Formación Profesional en CePETel 2023

Desde la Secretaria Técnica del Sindicato CePETel convocamos a participar del siguiente curso de formación profesional:

Seguridad en informática

Clases: 8 de 3hs c/u de 18:00 a 21:00 hs.
Días que se cursa: los días lunes 22, y 29 de mayo; 5, 12, 19 y 26 de junio; 3, y 10 de julio.
Modalidad: a distancia (requiere conectarse a la plataforma Zoom en los días y horarios indicados precedentemente).
Docente: Carlos Cagnani

La capacitación es:

- **Sin cargo para afiliados y su grupo familiar directo.**
- **Sin cargo para encuadrados con convenio CePETel.**
- **Con cargo al universo no contemplado en los anteriores.**

Informes: enviar correo a tecnico@cepetel.org.ar

Inscripción (hasta el 19 de mayo 12:00 hs): ingresar al formulario (se recomienda realizar el registro por medio de una cuenta de correo personal y ***no utilizar dispositivos de la empresa para acceder al link***).

https://forms.gle/8TVbL6HojaNxoEmx7

Temario:

Clase 1: Capas OSI, Redes, Accesos, tipo de redes, topologías, direccionamiento, protocolos, VLANS

- Capa OSI breve descripción
- Conceptos de Redes
- Tipo de Acceso
- Clasificación por tipo Negocio
- Clasificación por injerencia geográfica
- Topologías
- Servicios
- Protocolos de red
- Protocolos de transporte
- Aplicaciones
- VLANs
- Protocolos de ruteo

Ing. Daniel Herrero – Secretario Técnico – CDC

- Servicios críticos
- Seguridad sobre redes
- Seguridad sobre servicios Criticos

Clase 2: Certificados y Firma Digital, DNIe, eAdministración y eComercio

- Conceptos básicos
- Simbología
- Firma digital
- Reglamentación de la Ley de Firma Digital
- Firma electrónica
- Certificado Digital
- PKI definición
- Paso a paso para firmar digitalmente un documento electrónico en Argentina
- Identificación electrónica de las personas
- Identificación de Administración Electrónica
- Identificación en las PYMES

Clases 3 y 4: Seguridad en Aplicaciones y Sistemas Virtuales, Hacking y Análisis Forense

- Seguridad en Sistemas
- Accesos
- Problemas de seguridad en el desarrollo de sistemas (antes durante y después)
- Seguridad en el Ciclo de Vida de una Aplicación
- Metodología
- Hacking
- Hacking Ético, tipos
- Pentesting
- SIM
- SEM
- SIEM
- Correlación de eventos
- Ingeniería Forense
- Informática Forense

Clases 5 y 6: Seguridad en Redes y Comunicaciones Virtuales. Seguridad Perimetral

- Tipo de Redes
- Seguridad en LAN, WAN, MAN, WIFI, etc.
- DMZ
- Accesos
- Firewalls
- IDS
- IPS
- WAF
- NGFW

- Virus
- Malwares
- Seguridad Perimetral

Clase 7: Ciberseguridad

- Delito cibernético
- Ciberataques
- Ciberterrorismo
- Seguridad en IoT
- Ataques
- Seguridad en la Red
- Seguridad en la Nube
- Seguridad física

Clase 8: Normativas, estándares nacionales, internacionales y buenas prácticas en Seguridad de la Información

- Conceptos básicos de seguridad de la información
- Entorno regulatorio de Seguridad de la Información
- Principales organismos de referencia Internacionales
- Principales normas y reglamentos Internacionales
- Principales organismos de referencia en Argentina
- Principales normas y reglamentos en Argentina
- Infoleg
- Ley Sarbanes – Oxley (SOX)
- Estándar COSO
- Consideraciones previas a la implementación de ISO / IEC 27001
- Estándares de la Serie 27000

Seguridad en Informática - Módulo 1

Docente: Carlos Cagnani

*Este documento fue realizado en concepto de capacitación en Formación Profesional y dictada para el **Sindicato CePETel** a contar del mes de mayo del año 2023.*

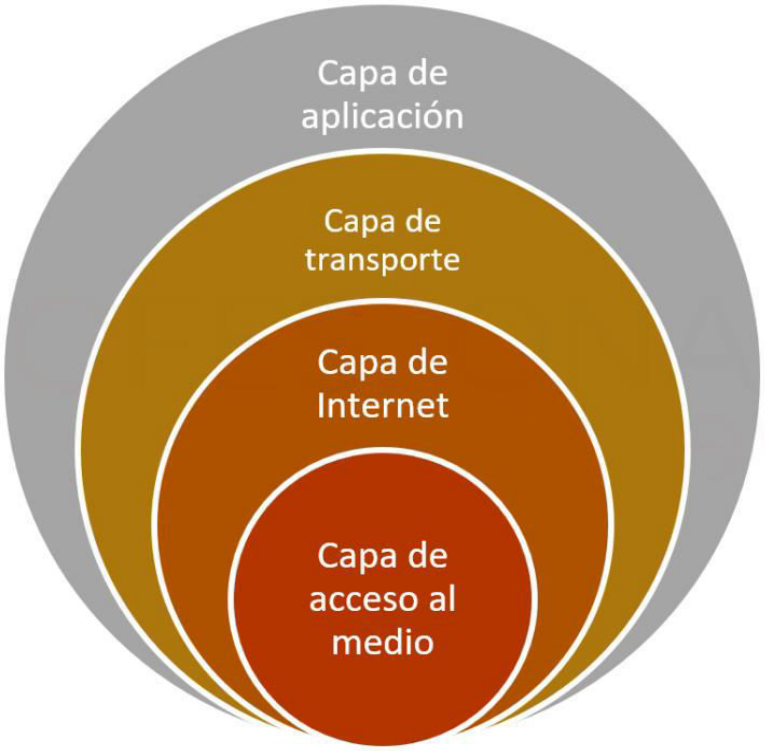
Redes Informáticas

CLASE 1 Modelo OSI,Redes, topologías

Índice de temas

1. Modelo OSI
2. Redes de Datos
3. Protocolo IP
4. Direcciones Físicas (MAC-Address)
5. Protocolo TCP
6. Protocolo UDP
7. Direccionamiento IP
8. VLANs
9. Protocolos de ruteo

Protocolos


Capa de aplicación
Capa de transporte
Capa de Internet
Capa de acceso al medio

Modelo OSI

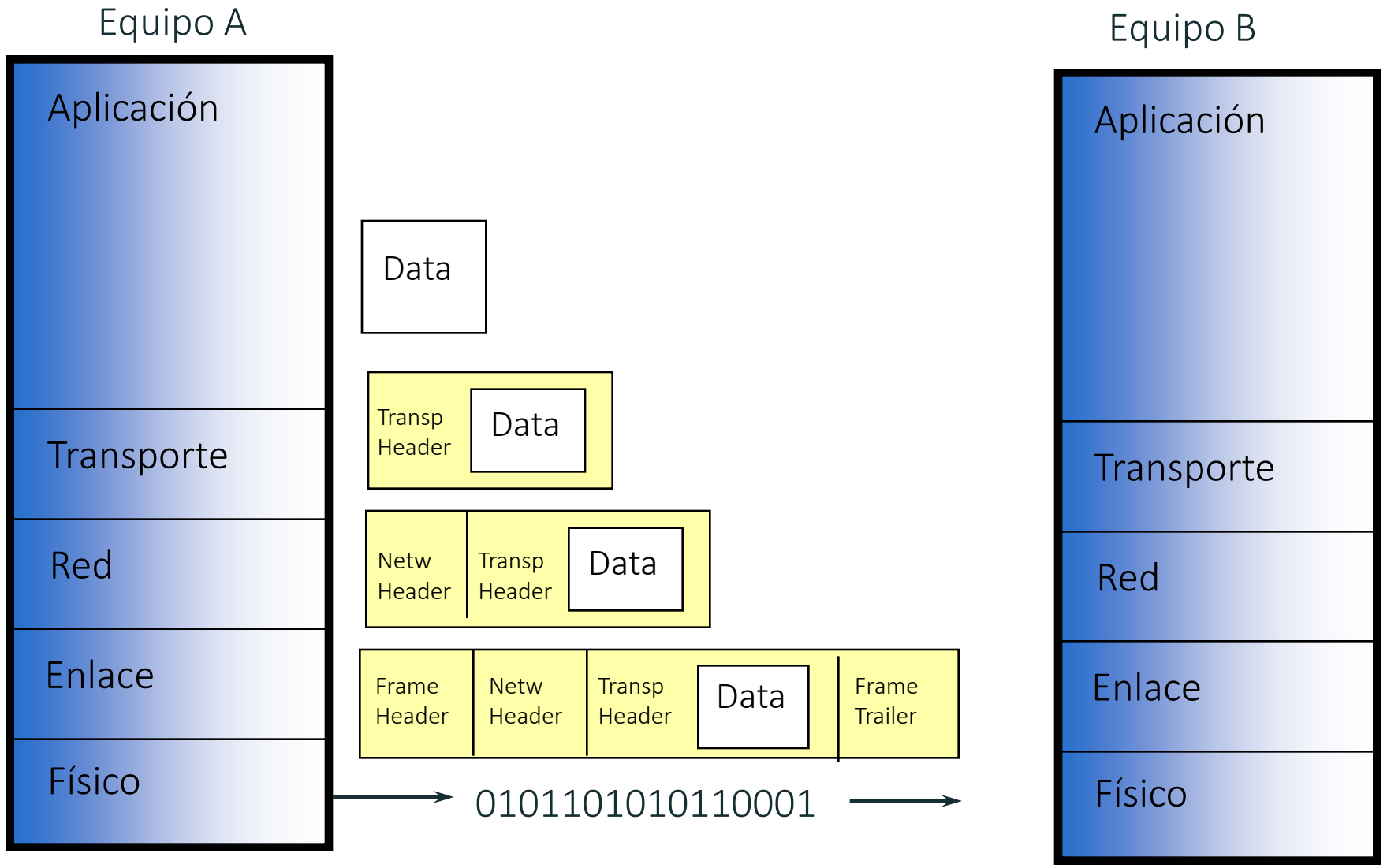
Modelo OSI

- Es la aplicación en sí misma que utiliza los servicios de la red.
- Provee formatos y códigos para la presentación e interpretación de la información entre los distintos sistemas.
- Soporta y administra las sesiones entre distintas aplicaciones (apertura, mantenimiento y cierre).
- Provee servicios seguros de transferencia de datos entre equipos. Secuenciamiento, corrección de errores.
- Se encarga que la información alcance cualquier destino dentro de la red. Provee direccionamiento lógico.
- Organización y transmisión libre de errores de datos entre equipos directamente conectados. Entramado, detección de errores y direccionamiento físico.
- Provee transmisión física de datos en los medios de telecomunicaciones. Define características eléctricas y mecánicas (conectores, interfases, velocidad de transmisión, niveles eléctricos, etc.)

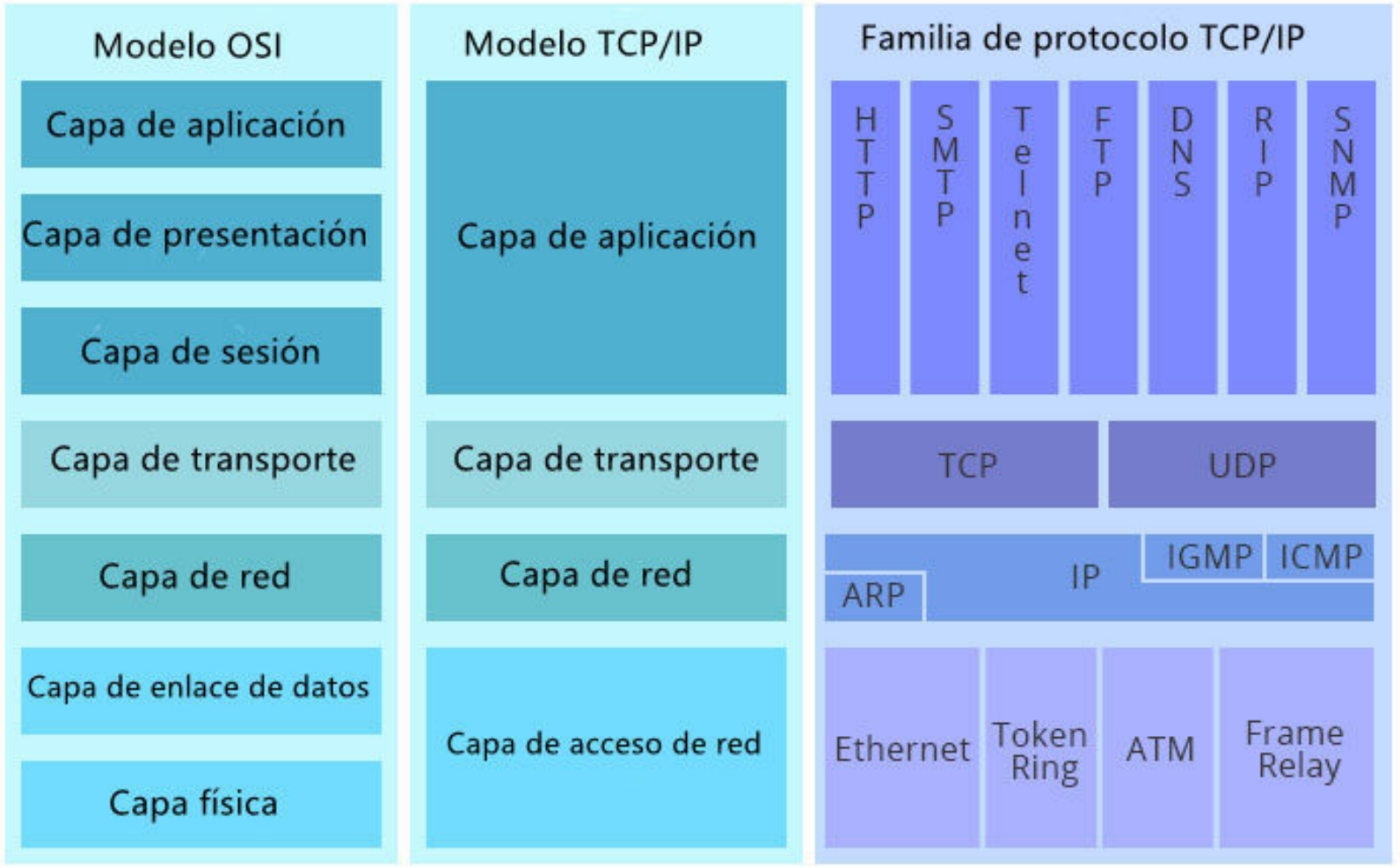
Modelo OSI

- 7- DNS, FTP, HTTP, IMAP, IRC, LDAP, MGCP, NTP, POP, SIP, SMTP, SNMP, SSH, Telnet.
- 6- EBCDIC-coded Vs. ASCII-coded text file. Encripción.
- 5- H.245 (Call Control Protocol), NetBIOS (Network Basic Input Output System), RPC (Remote Procedure Call Protocol), SDP (Sockets Direct Protocol).
- 4- TCP, UDP, SCTP, RSVP, SPX.
- 3- IPv4, IPv6, IGMP, IPsec, IPX, X.25 PLP
- 2- PPP, Ethernet, DSL, ISDN, FDDI, LAPB, SDLC, L2TP
- 1- RS-232, V.35, RJ45, UTP Cat.6, etc.

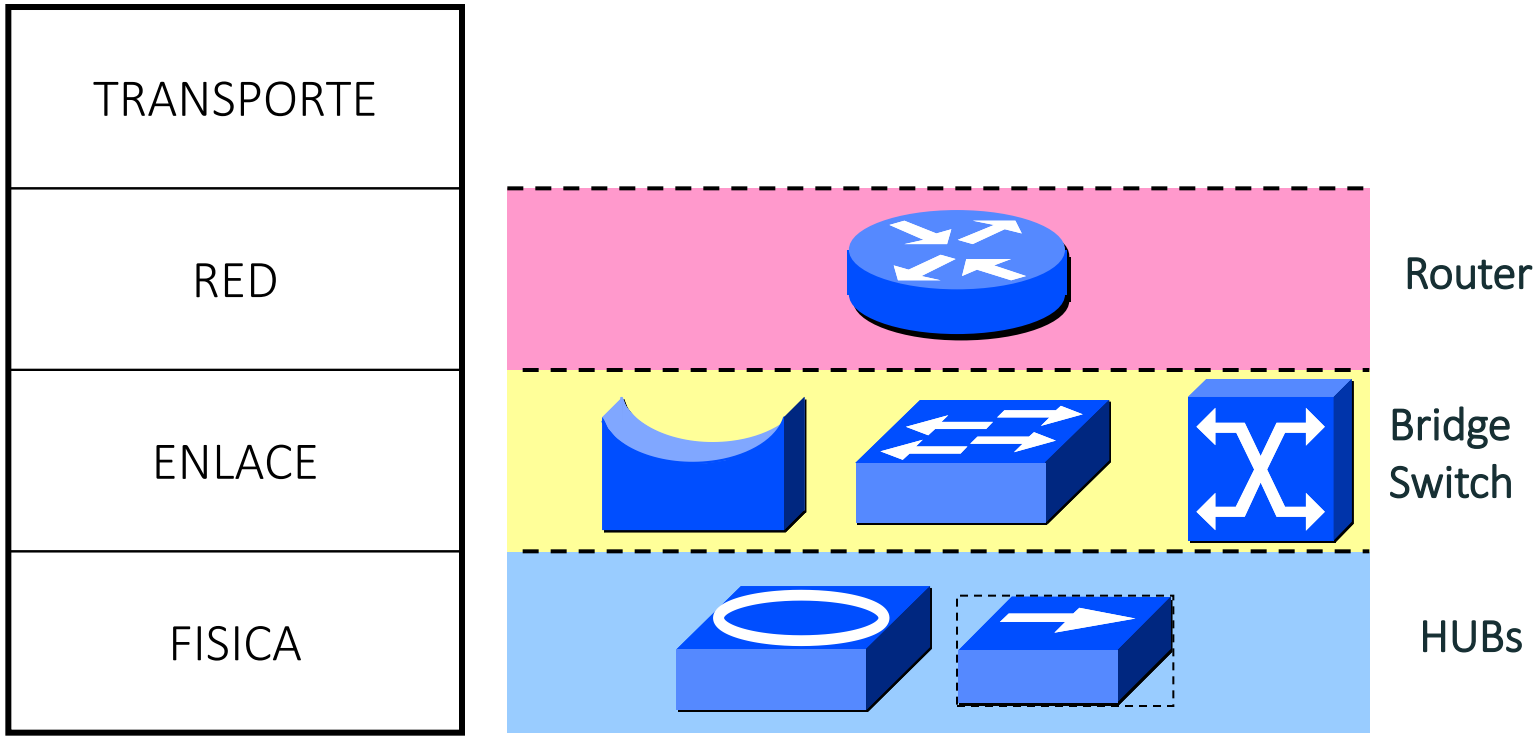
Encapsulado de Datos



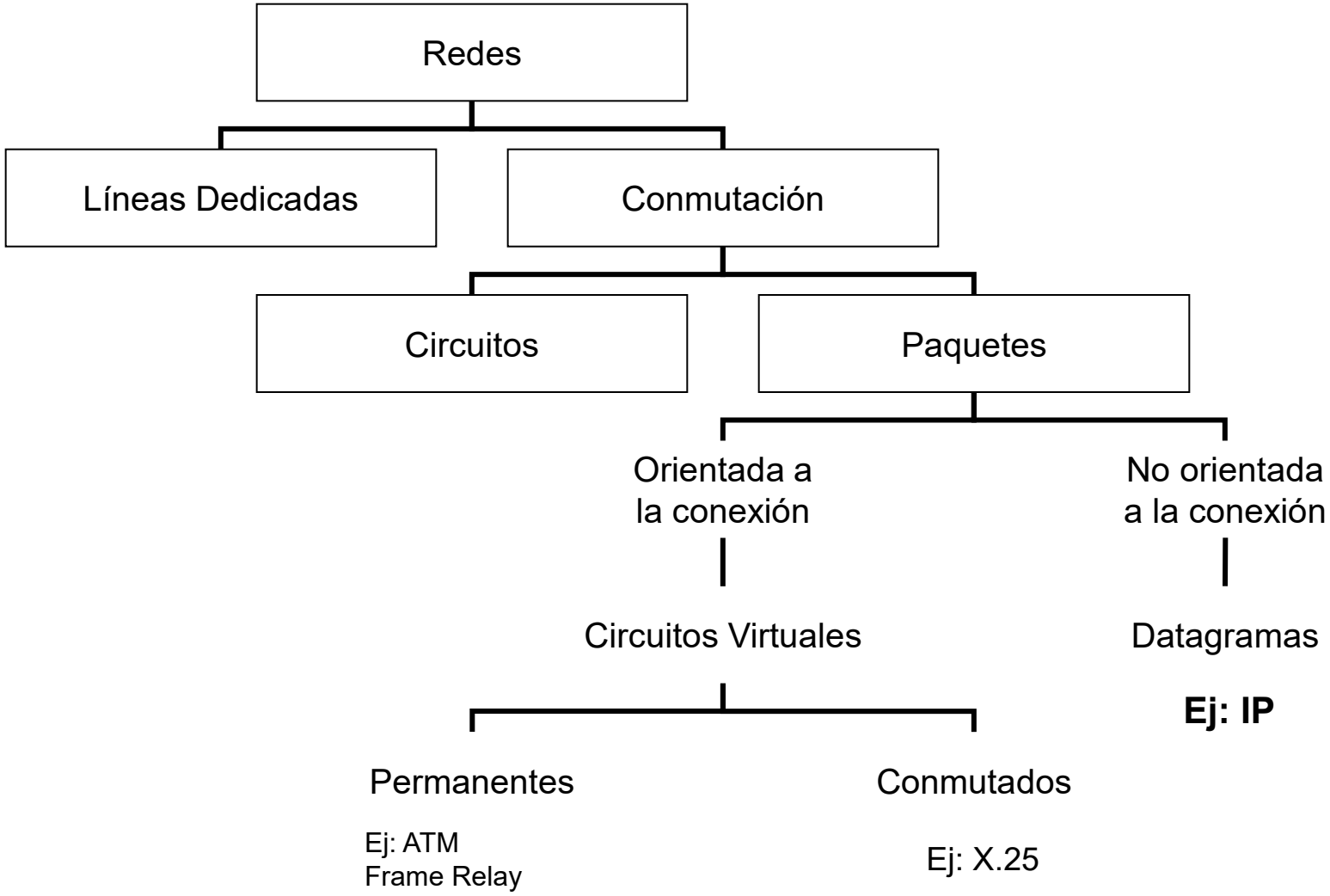
OSI vs TCP


Modelo OSI
Capa de aplicación
Capa de presentación
Capa de sesión
Capa de transporte
Capa de red
Capa de enlace de datos
Capa física
Modelo TCP/IP
Capa de aplicación
Capa de transporte
Capa de red
Capa de acceso de red
Familia de protocolo TCP/IP
HTTP
SMTP
Telnet
FTP
DNS
RIP
SNMP
TCP
UDP
ARP
IP
IGMP
ICMP
Ethernet
Token Ring
ATM
Frame Relay

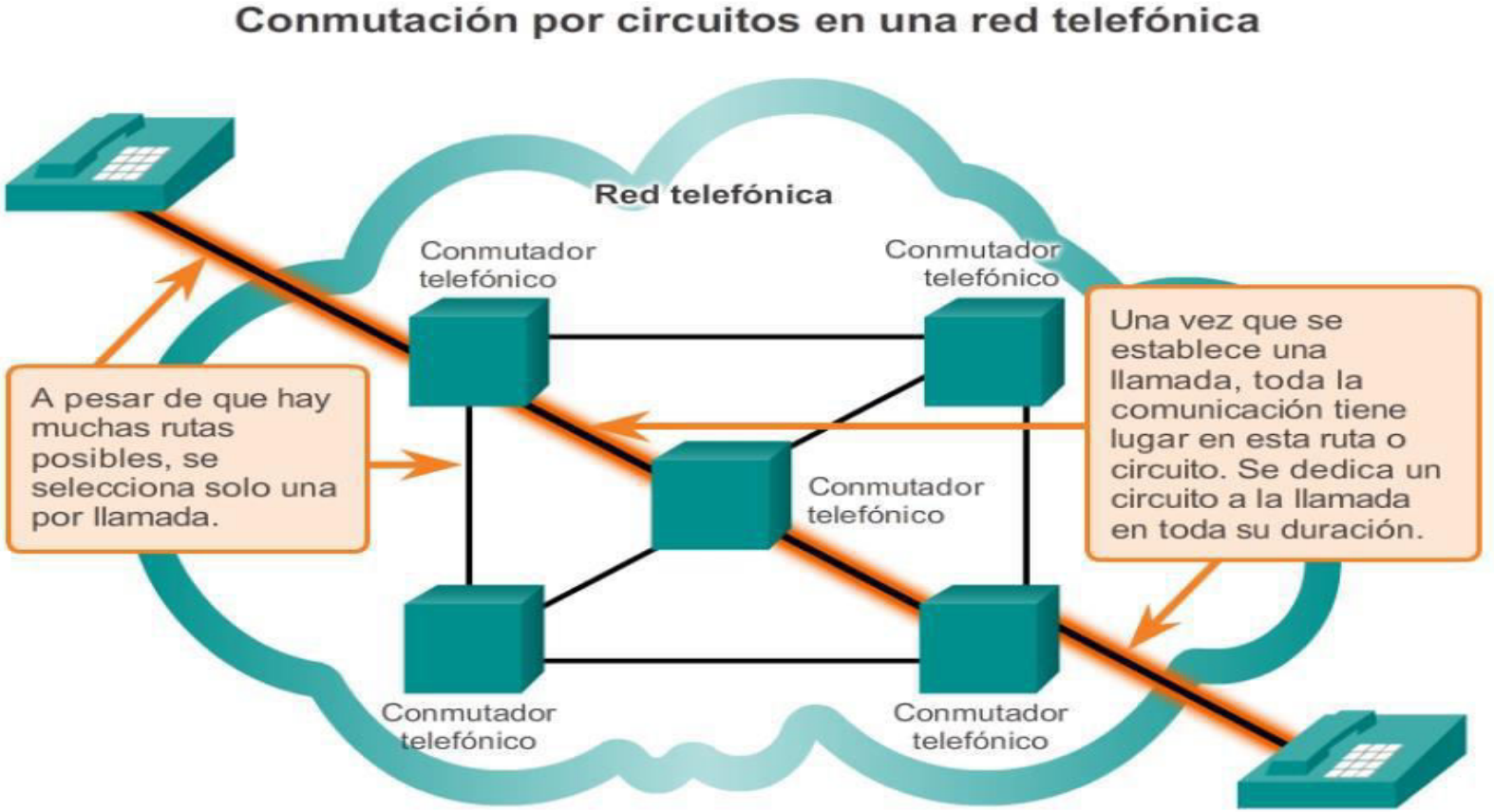
Dispositivos de Red por capa



Tipos de redes

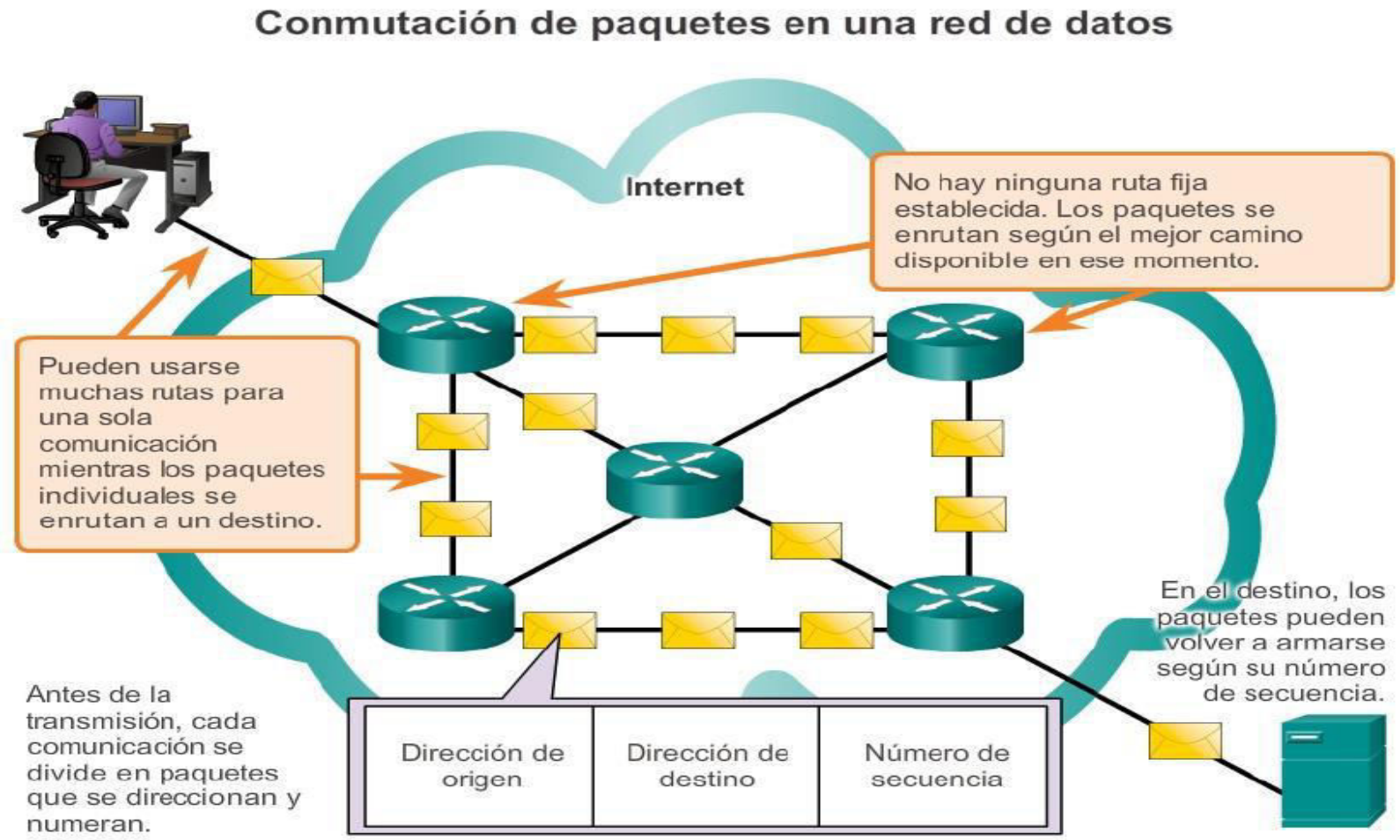


Tipos de redes
Conmutación por circuitos



Existen muchísimos circuitos, pero son una cantidad finita. Durante los períodos de demanda pico, es posible que se denieguen algunas llamadas.

Tipos de redes
Conmutación por paquetes



Redes de Datos

Red de datos
Definición

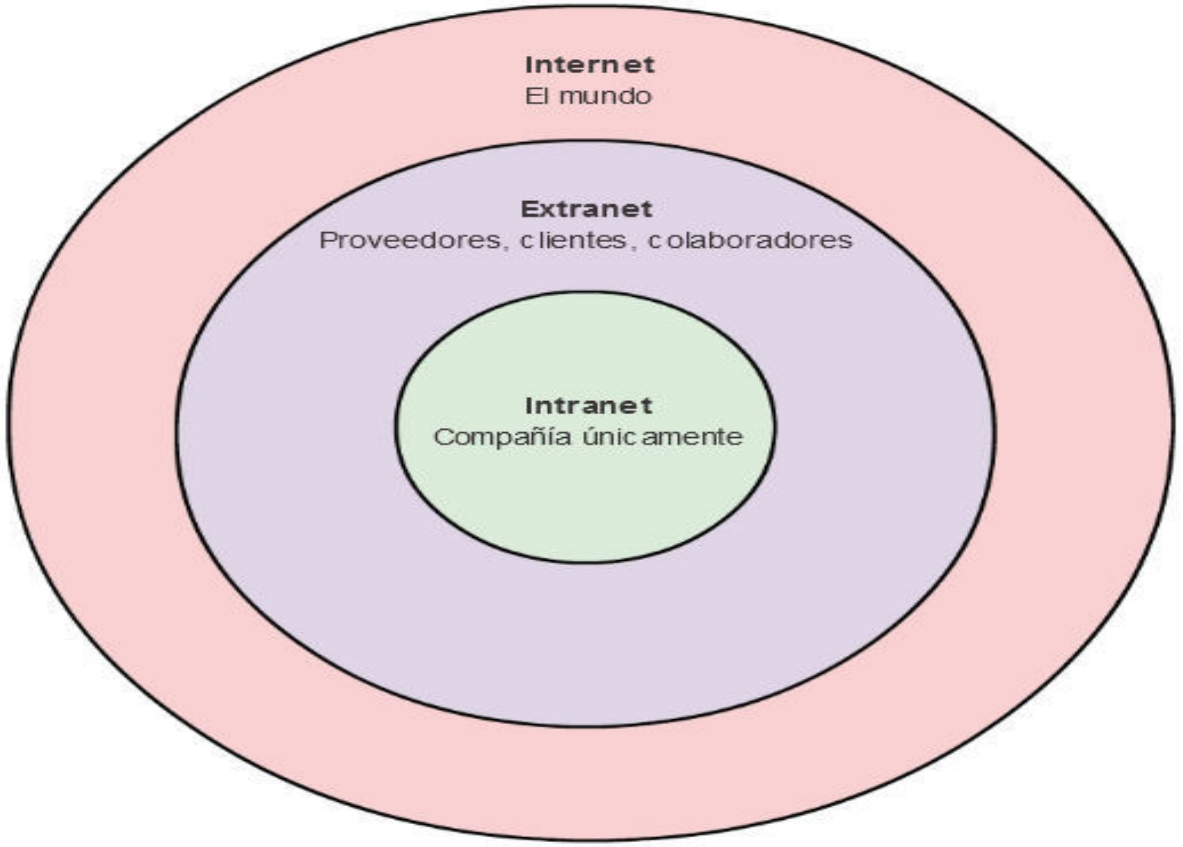
Es un conjunto de dispositivos interconectados físicamente(ya sea vía cableada o vía inalámbrica) que emplean los impulsos eléctricos, ondas electromagnéticas o cualquier otra tecnología para el transporte de datos; con la finalidad de compartir recursos (hardware y Software), información y servicios.

Y que se comunican entre sí a través de reglas (protocolos) de comunicación

Redes de datos
Definición

La comunicación a través de redes de datos desempeña un rol vital en nuestra vida cotidiana.

Red de datos
Clasificación por el Negocio

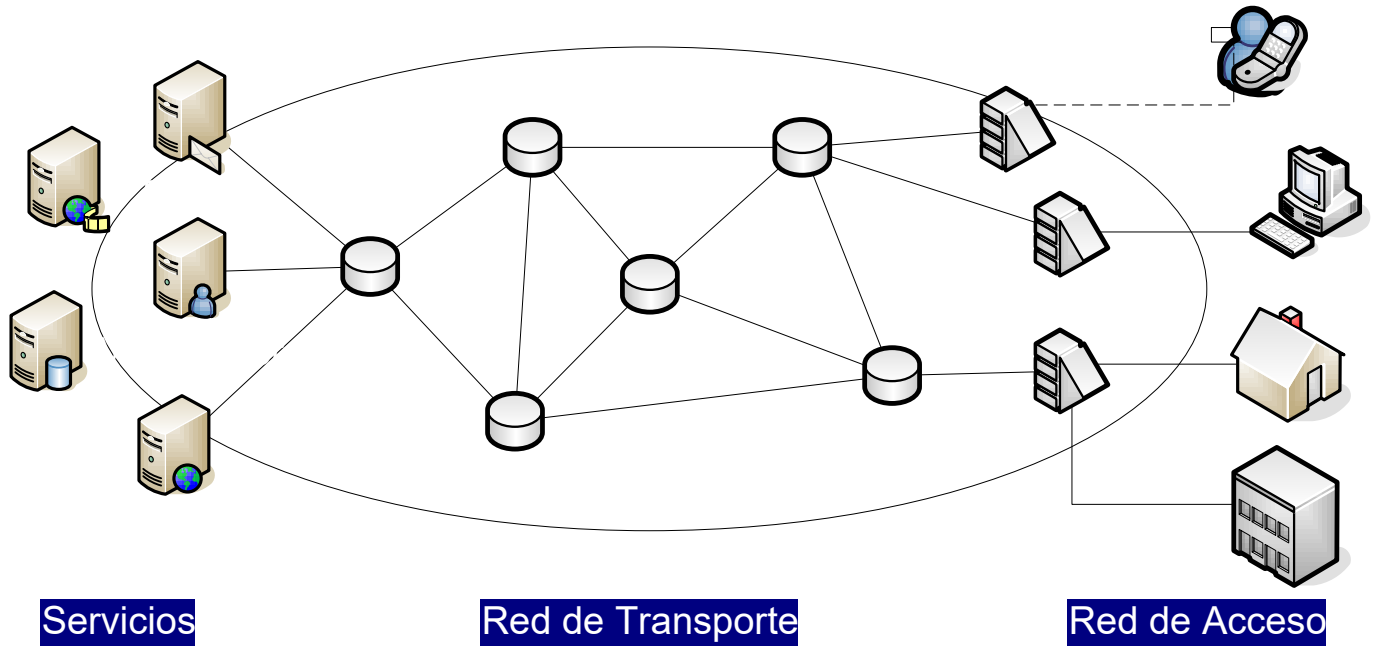


Redes de Datos
Componentes

Red de Acceso: parte de la red que se encuentra en la cercanía del cliente

Red Transporte: soporta la conexión entre los diversos nodos

Soporte Servicios: Provee los servicios que la red ofrece. Usualmente se encuentran distribuidos



Red de Acceso
Dispositivos terminales

-Son los llamados endpoints que tienen contenidos reales.

-Son los verdaderos receptores y emisores de los mensajes.

-Se identifican en la red por lo que se conoce como **dirección IP**.

Dispositivos del usuario final	
PC 	Impresora 
MAC 	Servidor de archivos 
Computadora portátil 	Mainframe IBM 

Red de Transporte
Dispositivos Intermediarios

Son los nodos centrales de una red

Se conectan entre sí y a su vez a los dispositivos terminales.

Algunas funcionalidades:

- Se encargan de direccionar o rutear los diálogos entre endpoints
- Volver a generar y transmitir las señales de datos.
- Conservar información acerca de las rutas que existen a través de la red.
- Notificar a otros dispositivos los errores de y las fallas de comunicación.
- Dirigir los datos a lo largo de rutas alternativas cuando hay una falla en el enlace.
- Clasificar y dirigir mensajes de acuerdo a las prioridades.
- Permitir de denegar flujo de datos de acuerdo a los parámetros de seguridad.

Red de Transporte
Dispositivos Intermediarios

Router inalámbrico

Switch LAN

Router

Switch de multicapa

Dispositivos de firewall

Red de Servicios

Red de Servicios

- World Wide Web.
- Correo electrónico.
- Grupos de Noticias (News, Boletines de noticias)
- Listas de distribución.
- Foros web.
- Weblogs, blogs o bitácoras.
- Transferencia de archivos FTP (File Transmision Protocol)
- Intercambio de archivo P2P.
- Telefonía
- Cloud Computing
- PaaS, IaaS y SaaS

Redes de datos
Por su ubicación geográfica

Desde el punto de vista de su alcance, las redes se clasifican en **LAN, MAN y WAN**

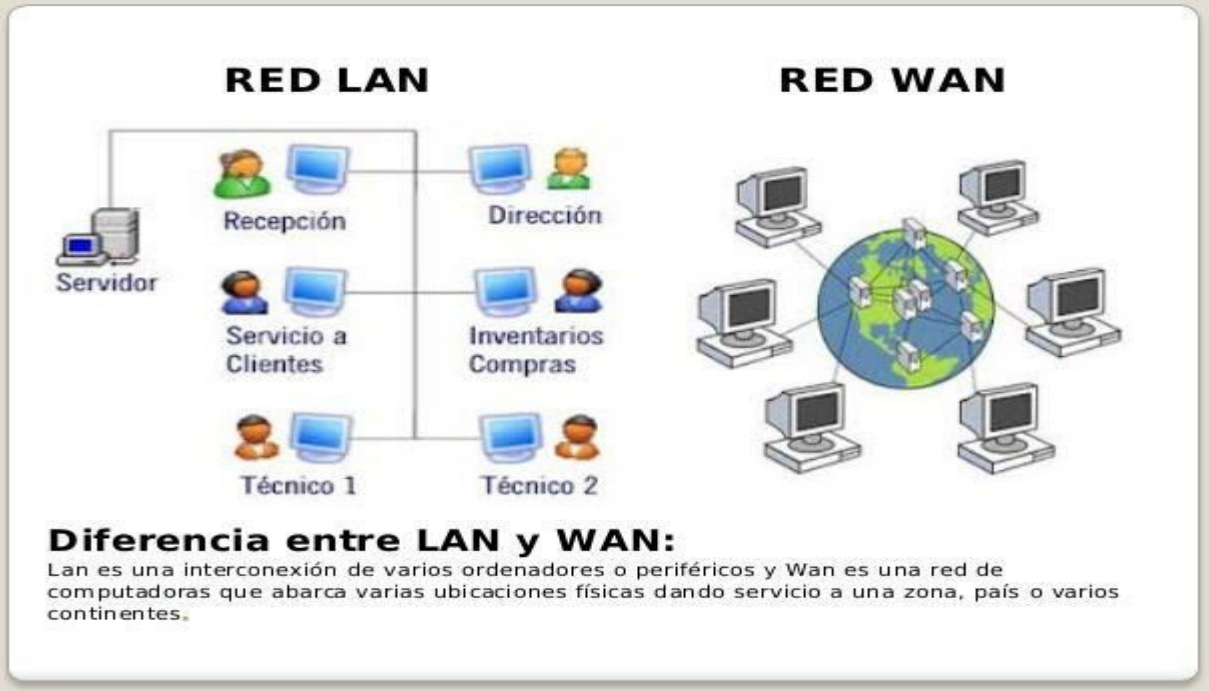
Características:

- Tasa de transmisión
- Tasa de error
- Retardo (latencia)
- Costo
- Propiedades

Red de datos
Clasificación por ubicación geográfica

Red LAN :

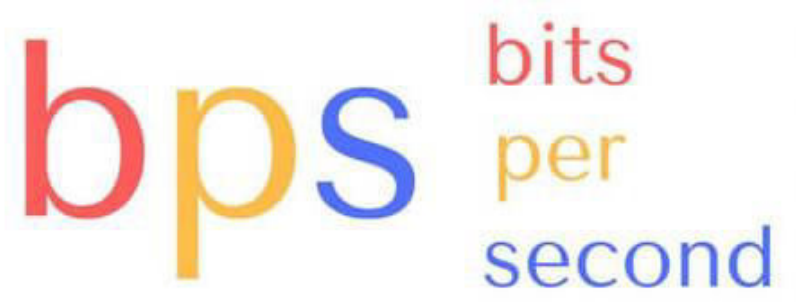
Red WAN:



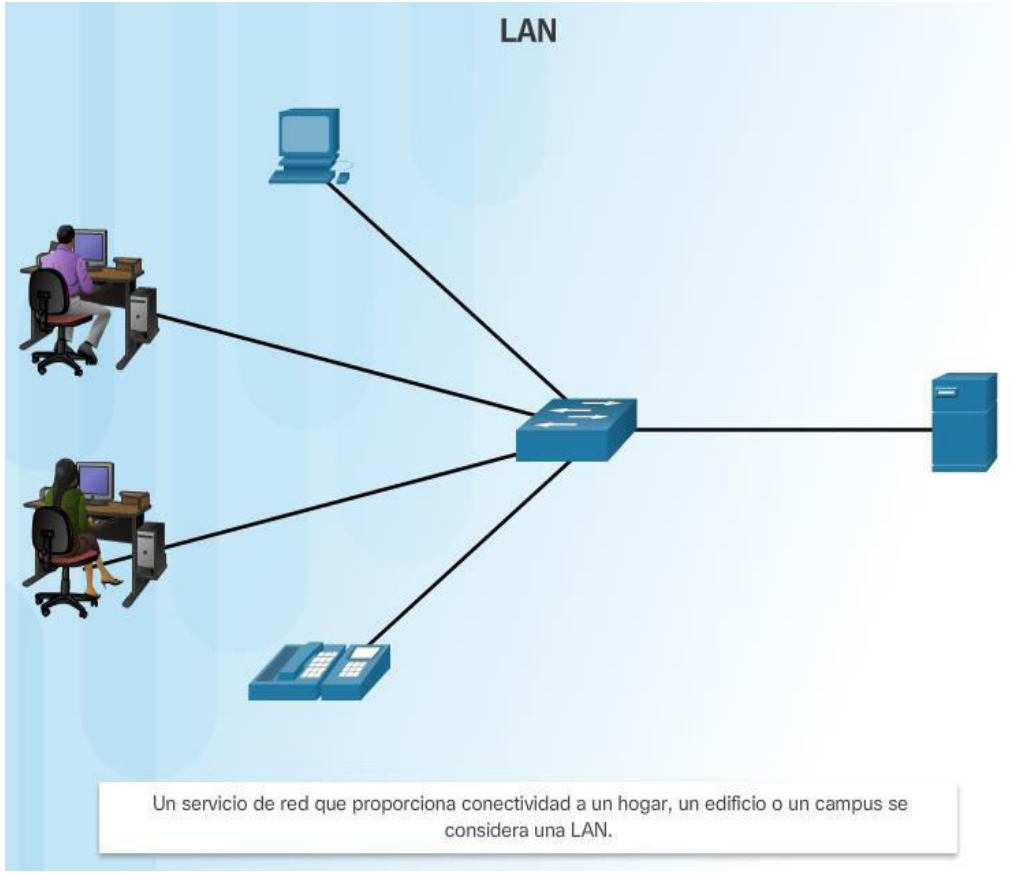
Velocidad de Transmisión

En comunicaciones, la velocidad de transmisión se mide siempre en bits por segundo.

También llamada tasa de transmisión o ancho de banda digital

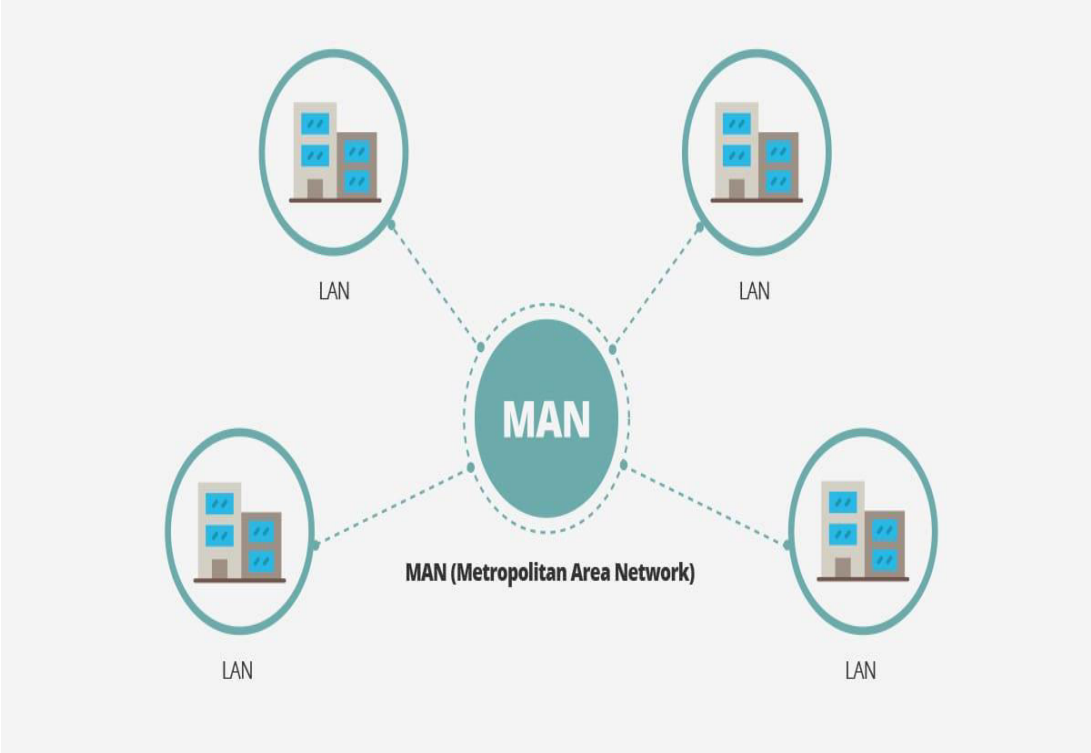


Tipos de Redes
Red LAN **L**ocal **A**rea **N**etwork



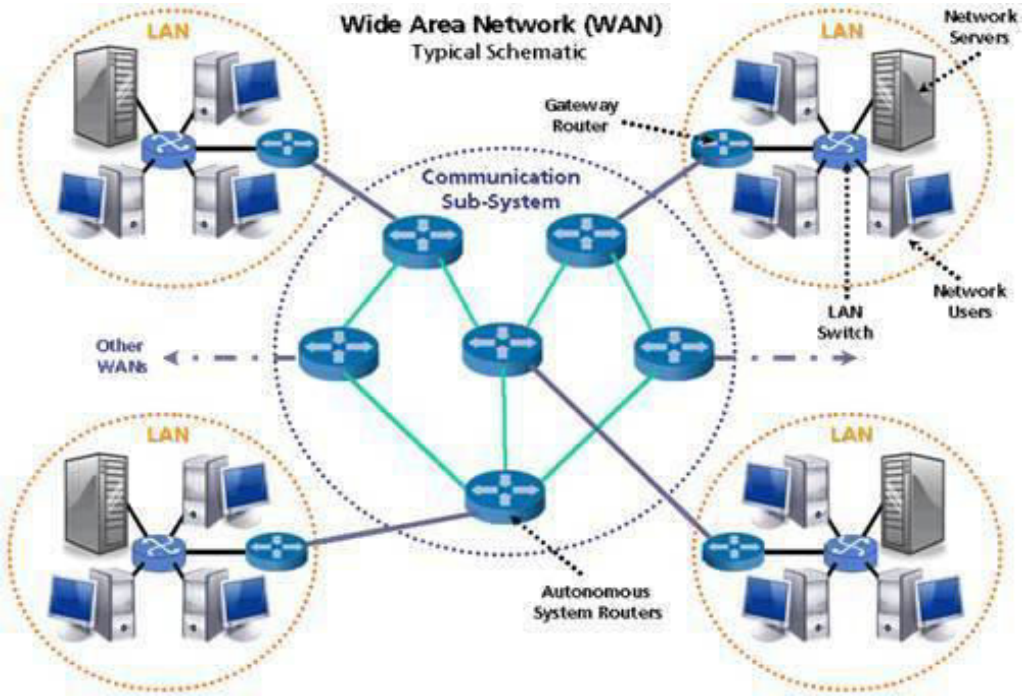
Se conoce como red LAN (siglas del inglés: *Local Área Network*, que traduce Red de Área Local) a una red informática **cuyo alcance se limita a un espacio físico reducido**, como una casa, un departamento o a lo sumo un edificio.
Fuente: https://concepto.de/red-lan/#ixzz71lnV0AdY

Tipos de Redes
Red MAN **M**etropolitan **A**rea **N**etwork



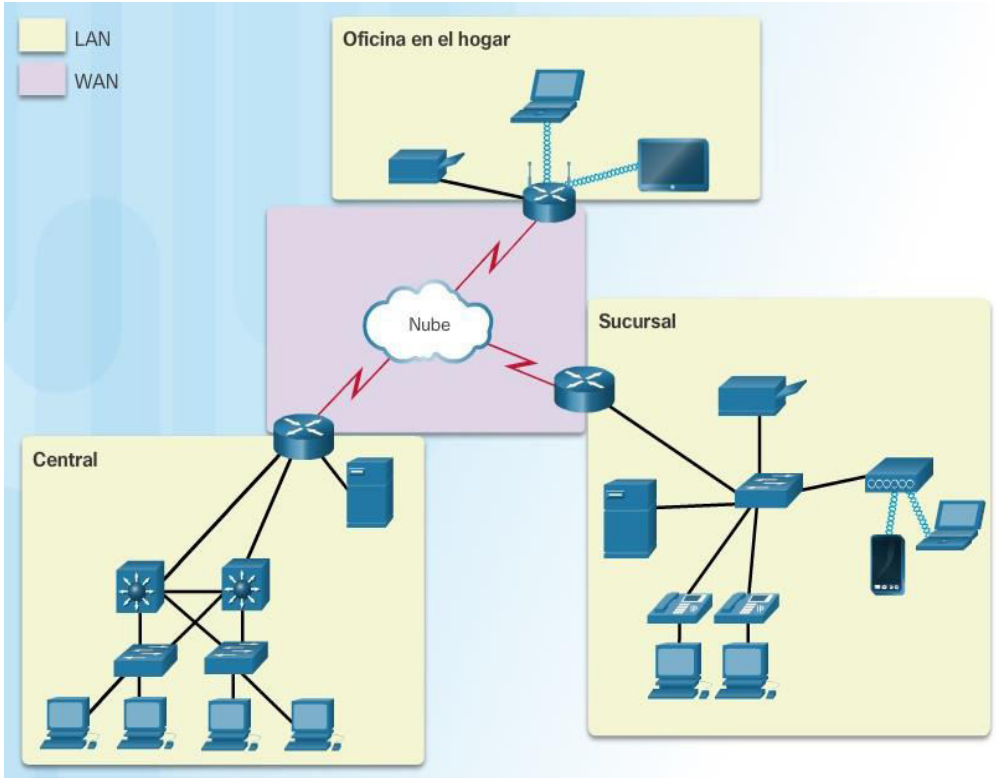
MAN es la sigla de **Metropolitan Area Network**, que puede traducirse como **Red de Área Metropolitana**. Una **red MAN** es aquella que, a través de una conexión de alta velocidad, ofrece cobertura en una zona geográfica extensa (como una **ciudad** o un municipio).

Tipos de Redes
Red WAN **W**ide **A**rea **N**etwork



WAN es la abreviatura de Wide Area Network. Estas redes se extienden por grandes áreas geográficas y conectan **redes más pequeñas** como redes LAN (Local Area Networks) o MAN (Metropolitan Area Networks). Por esto, solo se utilizan en el sector profesional.

Tipos de Redes
Red LAN/WAN en Pandemia

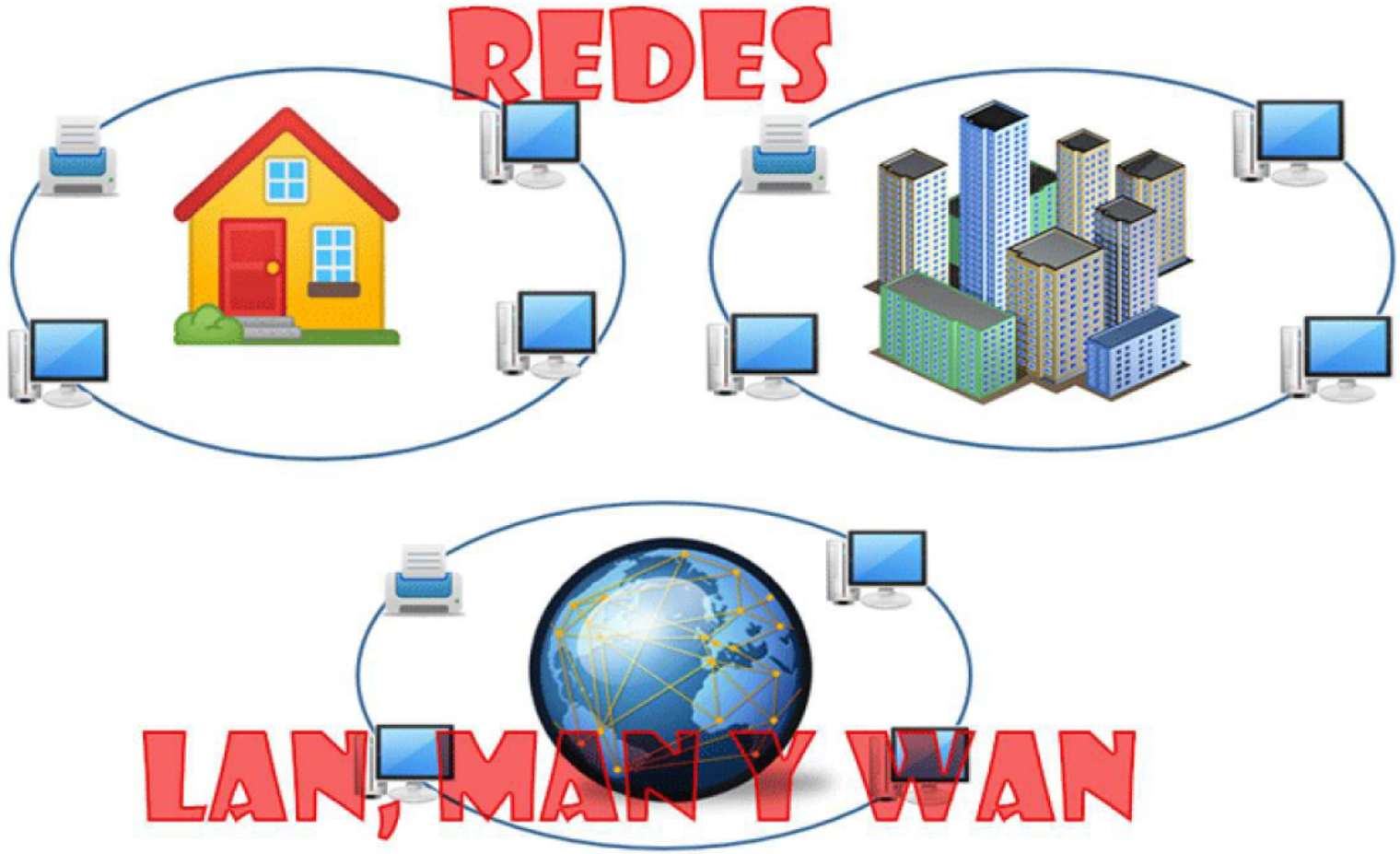


Este es un modelo de cómo se está trabajando actualmente en la mayoría de las empresas.

- La oficina de hogar se conecta a través de VPN al Sitio central

- Se puede acceder a la sucursal a través de Casa Central

Tipos de Redes
Red LAN/MAN/WAN



Tipos de Redes
Comparación de Redes

	Dispersión geográfica	Tasa de transmisión	Tasa de error	Retardo	Costo	Propiedad
LAN	Edificio Campus <1Km	↑↑↑	↓↓	⌛	$	Privadas
MAN	Ciudad 10Km	↑	↓	⌛	$$	Públicas
WAN	País Continente >100Km	↓	↑	⌛⌛⌛	$$$	Públicas

Tipos de redes
Características

- Tolerancia a fallas
- Escalabilidad
- Calidad de servicio (QoS)
- Seguridad

Pregunta Escalabilidad

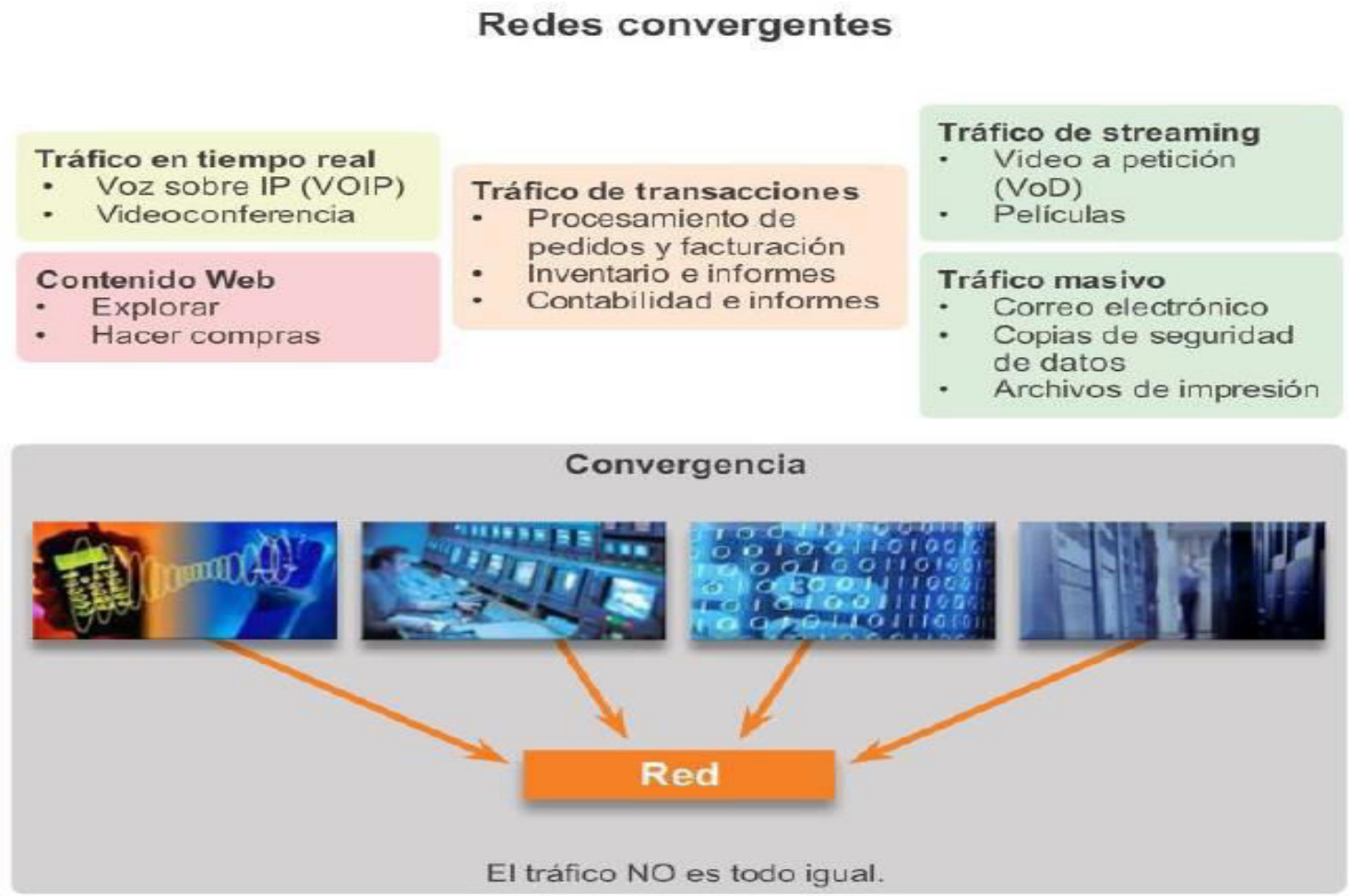
¿Quién/Qué limita el crecimiento de Internet?

Tipos de redes
Calidad de Servicio (QoS)

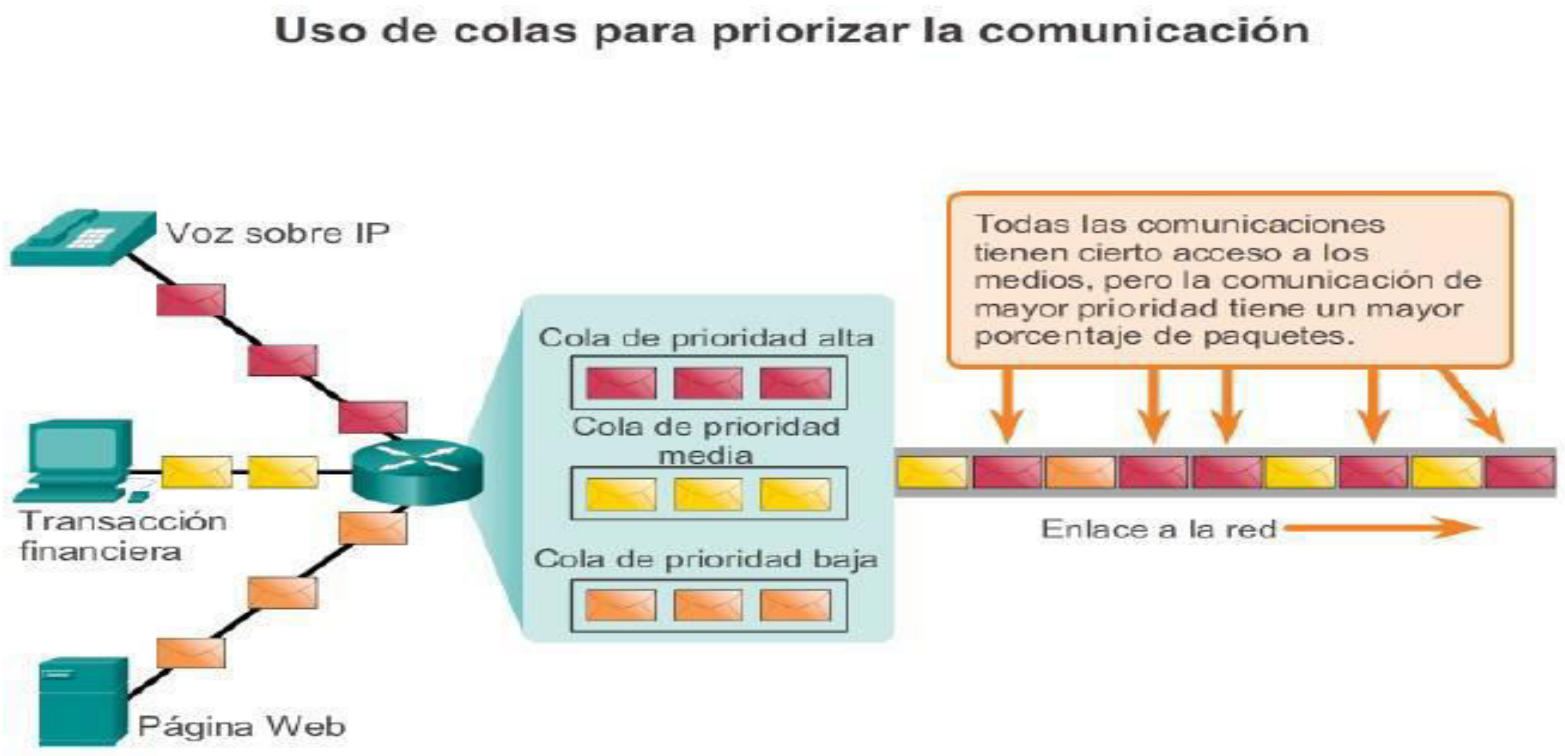
Internet NO tiene en cuenta la Calidad de Servicio.

- La calidad de servicio (QoS, Quality of Service) también es un requisito cada vez más importante para las redes hoy en día.
- Las nuevas aplicaciones disponibles para los usuarios en internetworks, como las transmisiones de voz y de video en vivo, generan expectativas más altas sobre la calidad de los servicios que se proporcionan.
- El ancho de banda de la red es la medida de la cantidad de bits que se pueden transmitir en un segundo, es decir, bits por segundo (bps).
- El secreto para ofrecer una solución de calidad de aplicación de extremo a extremo exitosa es lograr la QoS necesaria mediante la administración de los parámetros de retraso y de pérdida de paquetes en una red.
- Una de las formas en que esto se puede lograr es mediante la clasificación

Tipos de redes
Calidad de Servicios (QoS) cont.



Tipos de redes
Calidad de Servicios (QoS) cont.



La puesta en cola según los tipos de datos permite que los datos de voz tengan prioridad sobre los datos de transacción, los que a su vez tienen prioridad sobre los datos Web.

Pregunta QoS

¿Como se podría garantizar ?

Tipos de redes
Seguridad

La infraestructura de red, los servicios y los datos contenidos en los dispositivos conectados a la red son activos comerciales y personales muy importantes. Si se pone en peligro la integridad de esos recursos, esto podría traer consecuencias graves, como las siguientes:

- **Interrupciones** de la red que impidan la comunicación y la realización de transacciones, lo que puede provocar pérdidas de negocios.
- **Robo** de propiedad intelectual (ideas de investigación, patentes y diseños) y uso por parte de la competencia.
- Información personal o privada que se pone en riesgo o se hace pública sin el consentimiento de los usuarios.
- **Pérdida** de datos importantes cuyo reemplazo requiere un gran trabajo o que son irreemplazables.

Existen dos tipos de problemas de seguridad de red que se deben tratar: la seguridad de la infraestructura de red y la seguridad de la información.

Tipos de redes
Seguridad cont.

La seguridad es importante para la forma en que utilizamos una red

Transacciones no autorizadas

El uso no autorizado de nuestros datos de comunicaciones puede tener consecuencias graves.

Tipos de redes
Seguridad cont.

Disponibilidad: la disponibilidad se relaciona con tener la seguridad de que los usuarios autorizados contarán con acceso a los servicios de datos en forma confiable y oportuna.

- Los dispositivos de firewall de red, junto con el software antivirus de los equipos de escritorio y de los servidores pueden asegurar la confiabilidad y la solidez del sistema para detectar, repeler y resolver esos ataques.

Integridad de la comunicación: la integridad de los datos se relaciona con tener la seguridad de que la información **no se alteró** durante la transmisión desde el origen hasta el destino.

- Se puede asegurar la integridad de los datos mediante la solicitud de validación del emisor así como por medio del uso de mecanismos para validar que el paquete no se modificó durante la transmisión.

Confidencialidad: la confidencialidad de los datos se refiere a que solamente los destinatarios deseados y autorizados (personas, procesos o dispositivos) pueden acceder a los datos y leerlos.

- Esto se logra mediante la implementación de un sistema sólido de autenticación de usuarios

Tipos de redes
Seguridad cont.

Las comunicaciones y la información que deseamos mantener privadas están protegidas de quienes las utilizarían sin autorización.

Pregunta de Seguridad

¿Como se puede garantizar la seguridad total?

Protocolo IP

PROTOCOLO IP

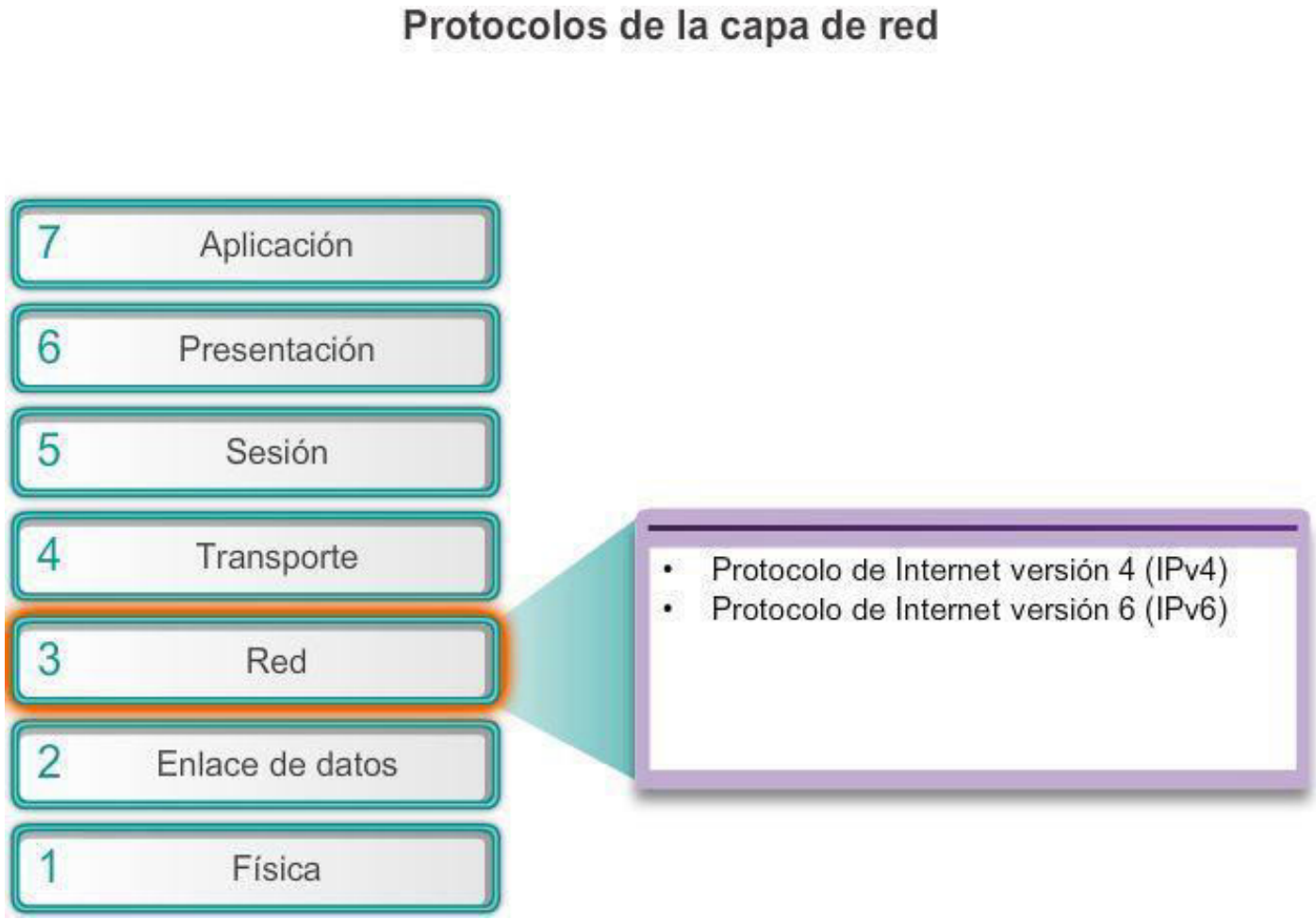
Existen varios protocolos de capa de red; sin embargo, solo los dos que se incluyen a continuación se implementan con frecuencia, como se muestra en la ilustración:

- Protocolo de Internet versión 4 (IPv4)
- Protocolo de Internet versión 6 (IPv6)

Otros protocolos de capa de red antiguos que no tienen un uso muy difundido incluyen los siguientes:

- Intercambio Novell de paquetes de internetwork (IPX)
- AppleTalk
- Servicio de red sin conexión (CLNS/DECNet)

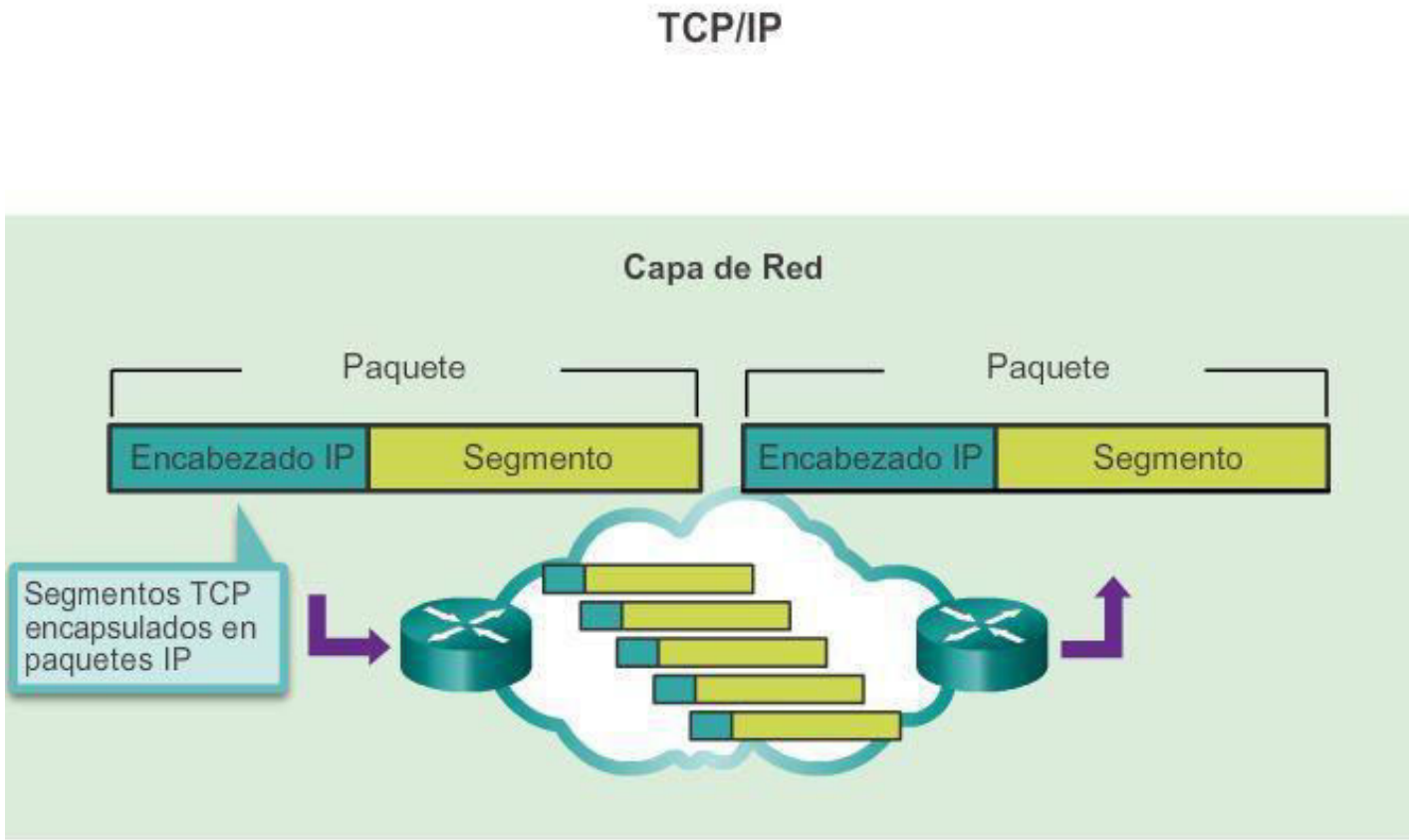
PROTOCOLO IP



PROTOCOLO IP
CARACTERISTICAS

- **Sin conexión**: no se establece ninguna conexión con el destino antes de enviar los paquetes de datos.
- **Máximo esfuerzo** (no confiable): la entrega de paquetes no está garantizada.
- **Independiente de los medios**: la operación es independiente del medio que transporta los datos.

PROTOCOLO IP
CARACTERISTICAS



Los paquetes IP fluyen a través de la internetwork.

PROTOCOLO IP
Sin Conexión

- La función de la capa de red es transportar paquetes entre los hosts colocando la menor carga posible en la red.
- La capa de red no se ocupa ni está al tanto del tipo de comunicación contenida dentro de un paquete.
- IP es un protocolo sin conexión, lo que significa que no se crea ninguna conexión dedicada de extremo a extremo antes de enviar los datos.
- Conceptualmente, la comunicación sin conexión es similar a enviar una carta a alguien sin notificar al destinatario con anticipación.
- Como se muestra en la figura, el servicio postal utiliza la información en una carta para entregarla a un destinatario.
- La dirección en el sobre no proporciona datos que indiquen si el receptor está presente, si la carta llegará a destino o si el receptor puede leerla.
- De hecho, el servicio postal no está al tanto de la información contenida dentro del paquete que entrega y, por lo tanto, no puede proporcionar ningún mecanismo de corrección de errores.

PROTOCOLO IP
Sin Conexión cont.

El emisor no sabe:

- Si el receptor está presente
- Si la carta llegó
- Si el receptor puede leer la carta

El receptor no sabe:

- Cuándo llegará

PROTOCOLO IP
Sin Conexión cont.

- Las comunicaciones de datos sin conexión funcionan según el mismo principio.
- IP es un protocolo sin conexión y, por lo tanto, NO requiere ningún intercambio inicial de información de control para establecer una conexión de extremo a extremo antes de reenviar los paquetes.
- Además, tampoco requiere campos adicionales en el encabezado de la unidad de datos del protocolo (PDU Protocol Data Unit) para mantener una conexión establecida.
- Este proceso reduce en gran medida la sobrecarga del IP.
- Sin embargo, sin una conexión de extremo a extremo preestablecida, los emisores no saben si los dispositivos de destino están presentes y en condiciones de funcionamiento cuando envían los paquetes, y tampoco saben si el destino recibe el paquete o si puede acceder al paquete y leerlo.

PROTOCOLO IP
Sin Conexión cont.

El emisor no sabe:

- Si el receptor está presente
- Si el paquete llegó
- Si el receptor puede leer el paquete

El receptor no sabe:

- Cuándo llegará

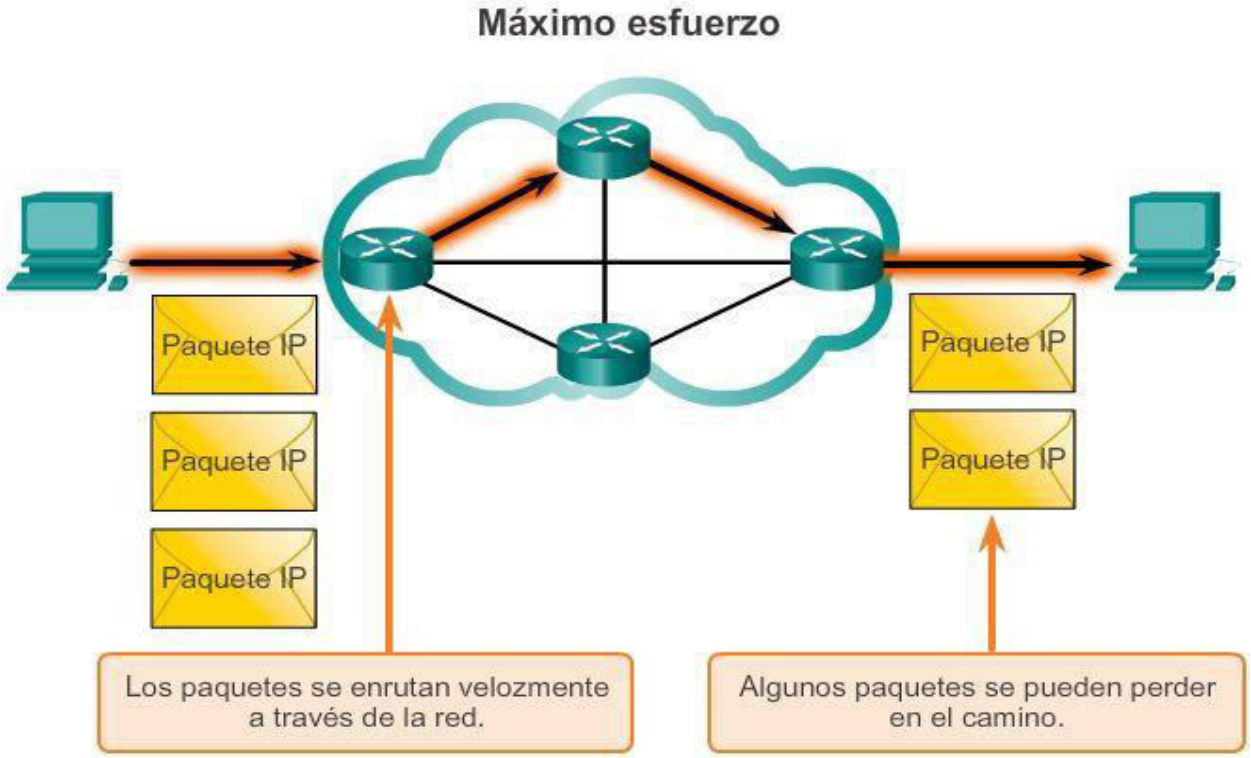
PROTOCOLO IP
Máximo esfuerzo de entrega

- A menudo, el protocolo IP se describe como un protocolo no confiable o de máximo esfuerzo de entrega.
- Esto no significa que IP a veces funcione bien y a veces funcione mal, ni que sea un protocolo de comunicación de datos deficiente.
- “No confiable” significa simplemente que IP no tiene la capacidad de administrar paquetes no entregados o dañados ni de recuperar datos de estos.
- Esto se debe a que los paquetes IP se envían con información sobre la ubicación de entrega, pero no contienen información que se pueda procesar para informar al emisor si la entrega se realizó correctamente.
- No se incluyen datos de sincronización en el encabezado del paquete para realizar un seguimiento del orden de entrega de los paquetes.
- Con el protocolo IP, tampoco hay acuses de recibo de la entrega de los paquetes ni datos de control de errores que permitan realizar un seguimiento de si los paquetes se entregaron sin daños.
- Los paquetes pueden llegar al destino dañado o fuera de secuencia, o pueden no llegar en absoluto.
- De acuerdo con la información proporcionada en el encabezado IP, no hay capacidad de retransmisión de paquetes si se producen errores como estos.

PROTOCOLO IP
Máximo esfuerzo de entrega cont.

- Si los paquetes faltantes o que no funcionan generan problemas para la aplicación que usa los datos, los servicios de las capas superiores, como TCP, deben resolver estos problemas.
- Esto permite que el protocolo IP funcione de forma muy eficaz. Si se incluyera la sobrecarga de confiabilidad en IP, las comunicaciones que no requieren conexión o confiabilidad se cargarían con el consumo de ancho de banda y la demora producidos por esta sobrecarga.
- En la suite TCP/IP, la capa de transporte puede utilizar el protocolo TCP o UDP, según la necesidad de confiabilidad en la comunicación.
- Dejar que la capa de transporte decida sobre la confiabilidad hace que el protocolo IP se adapte y se acomode mejor a los distintos tipos de comunicación.
- En la ilustración, se muestra un ejemplo de comunicaciones IP.
- Los protocolos orientados a la conexión, como TCP, requieren el intercambio de datos de control para establecer la conexión.
- Para mantener la información sobre la conexión, TCP también requiere campos adicionales en el encabezado de la PDU.

PROTOCOLO IP
Máximo esfuerzo de entrega cont.

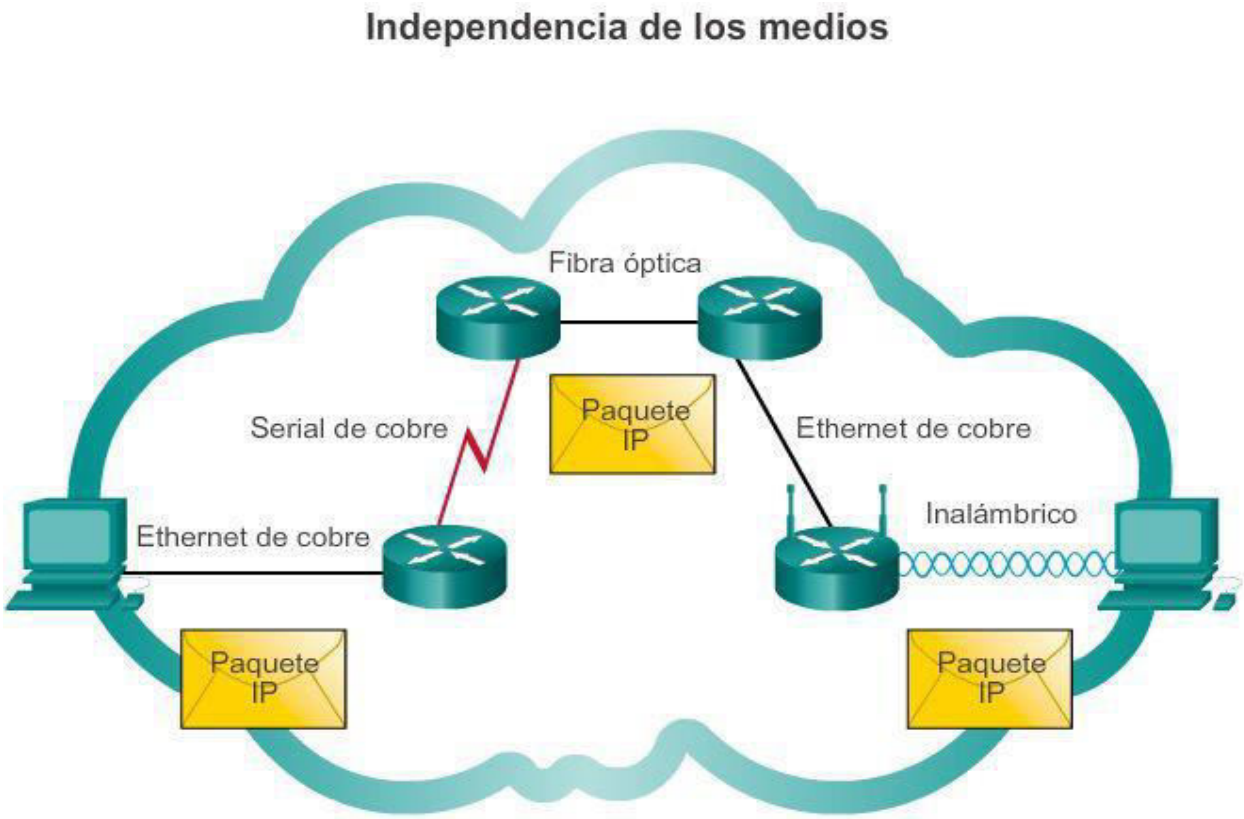


Dado que es un protocolo de capa de red no confiable, IP no garantiza que se reciban todos los paquetes enviados. Otros protocolos administran el proceso de seguimiento de paquetes y de aseguramiento de entrega.

PROTOCOLO IP
Independiente de los medios

- La capa de red tampoco tiene la carga de las características de los medios por los cuales se transportan los paquetes.
- IP funciona con independencia de los medios que transportan los datos en las capas inferiores del stack de protocolos.
- Como se muestra en la figura, cualquier paquete IP individual puede ser comunicado eléctricamente por cable, como señales ópticas por fibra, o sin cables como señales de radio.
- Es responsabilidad de la capa de enlace de datos del modelo OSI tomar un paquete IP y prepararlo para transmitirlo a través del medio de comunicación.
- Esto significa que el transporte de paquetes IP no está limitado a un medio en particular.

PROTOCOLO IP
Independiente de los medios cont.



Los paquetes IP pueden trasladarse a través de diferentes medios.

PROTOCOLO IP
Independiente de los medios cont.

Sin embargo, existe una característica importante de los medios que la capa de red tiene en cuenta: el tamaño máximo de la PDU que cada medio puede transportar.

Esta característica se denomina “unidad máxima de transmisión” (MTU).

Parte de la comunicación de control entre la capa de enlace de datos y la capa de red consiste en establecer el tamaño máximo para el paquete. La capa de enlace de datos pasa el valor de MTU a la capa de red.

A continuación, la capa de red determina cuán grandes pueden ser los paquetes.

En algunos casos, un dispositivo intermediario, generalmente un router, debe dividir un paquete cuando lo reenvía de un medio a otro con una MTU más pequeña.

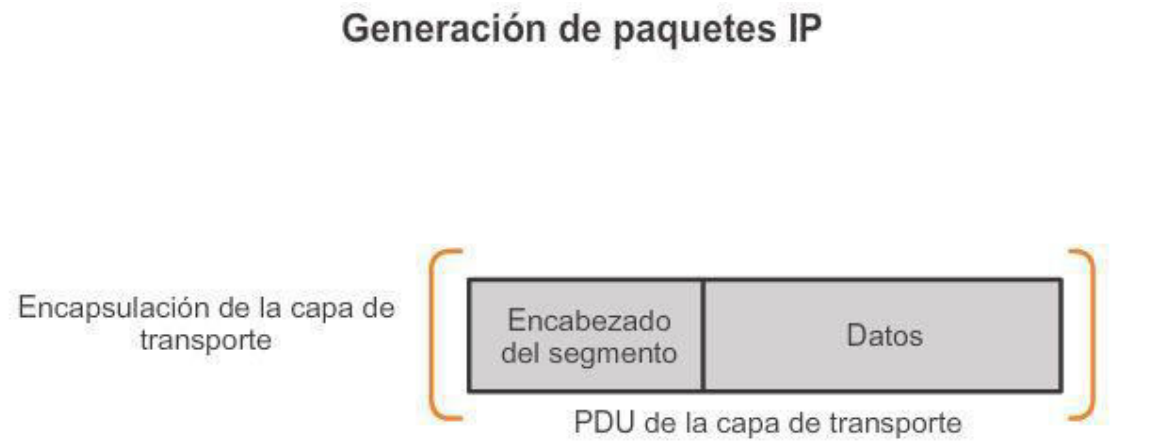
Este proceso se llama fragmentación de paquetes o solamente fragmentación

PROTOCOLO IP
Encapsulación de IP

- El protocolo IP encapsula o empaqueta el segmento de la capa de transporte agregando un encabezado IP.
- Este encabezado se utiliza para entregar el paquete al host de destino. El encabezado IP permanece en su lugar desde el momento en que el paquete abandona la capa de red del host de origen hasta que llega a la capa de red del host de destino.
- El proceso de encapsulación de datos capa por capa permite el desarrollo y el escalamiento de los servicios de las diferentes capas sin afectar otras capas.
- Esto significa que el protocolo IPv4 o IPv6, o cualquier protocolo nuevo que se desarrolle en el futuro, pueden empaquetar fácilmente los segmentos de la capa de transporte.
- Los routers pueden implementar estos diferentes protocolos de capa de red para operar al mismo tiempo en una red desde y hacia el mismo host o hosts diferentes.
- El enrutamiento que realizan estos dispositivos intermediarios solo tiene en cuenta el contenido del encabezado del paquete que encapsula el segmento.
- En todos los casos, la porción de datos del paquete, es decir, la PDU de la capa de transporte encapsulada, no se modifica durante los procesos de la capa de red.

PROTOCOLO IP
Encapsulación de IP

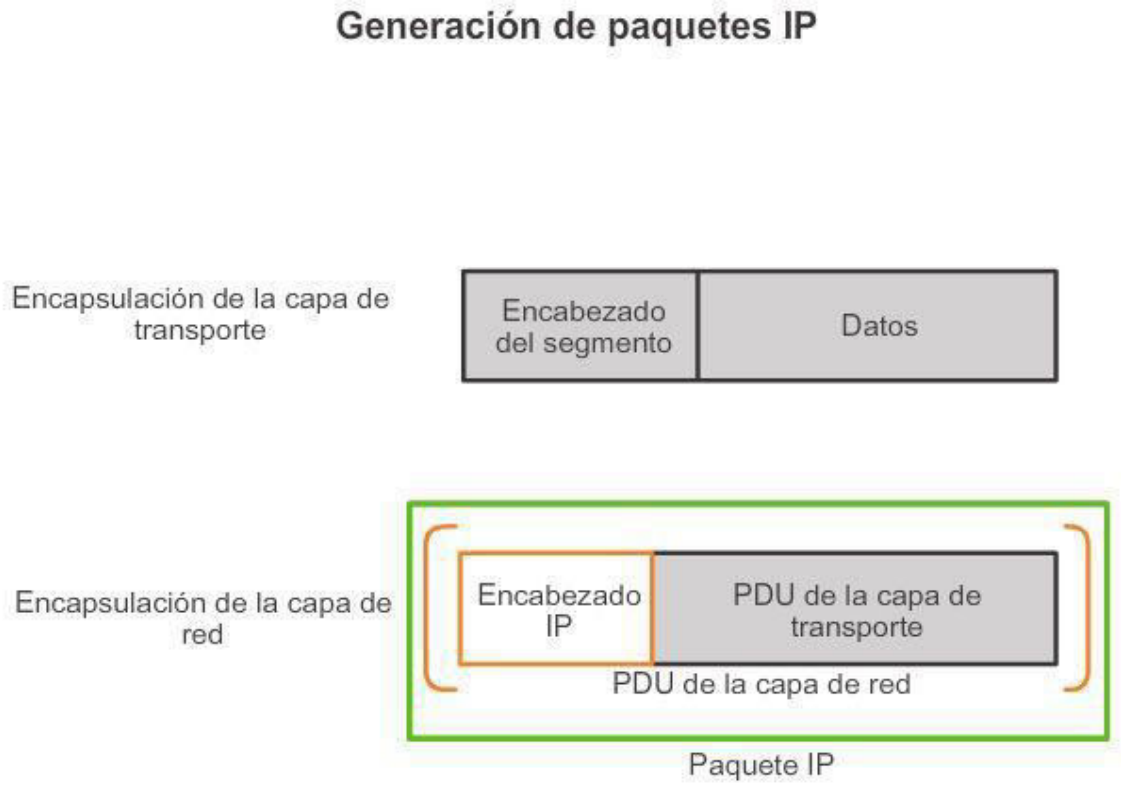
Proceso de creación de la PDU de la capa de transporte.



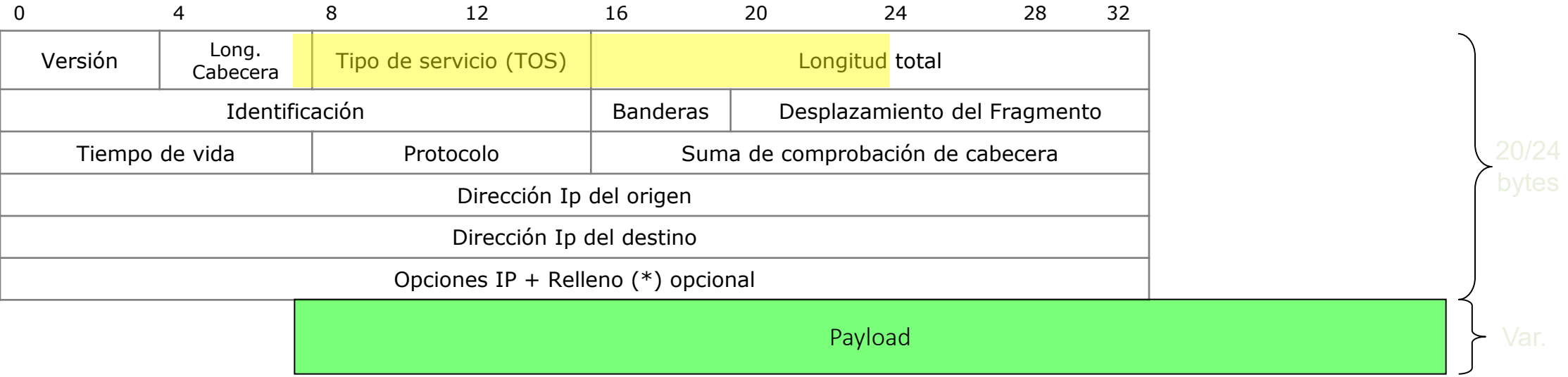
La capa de transporte agrega un encabezado para que los segmentos puedan volver a armarse en el destino.

PROTOCOLO IP
Encapsulación de IP

Proceso subsiguiente de creación de la PDU de la capa de red.



PROTOCOLO IP
CABECERA



Versión: es la versión del protocolo con la cual se creo el datagrama. La versión actual es la 4.

Long. Cabecera: indica la longitud de la cabecera o header en cantidad de palabras de 32 bits. Comunmente es de 5.

Tipo de servicio (TOS): A través de este campo se solicita determinado tratamiento del datagrama. Luego lo veremos en detalle.

Herramientas

Wireshark http://www.wireshark.org

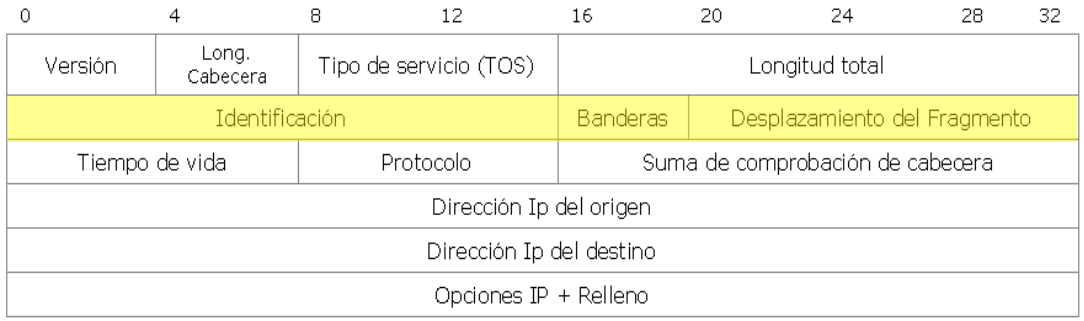
Nmap https://nmap.org/download.html

PROTOCOLO IP
CABECERA (CONT)

https://www.iana.org/assignments/protocol-numbers/protocol-numbers.xhtml

Decimal	Keyword	Protocol	IPv6 Extension Header	Reference
0	HOPOPT	IPv6 Hop-by-Hop Option	Y	[RFC8200]
1	ICMP	Internet Control Message		[RFC792]
2	IGMP	Internet Group Management		[RFC1112]
3	GGP	Gateway-to-Gateway		[RFC823]
4	IPv4	IPv4 encapsulation		[RFC2003]
5	ST	Stream		[RFC1190][RFC1819]
6	TCP	Transmission Control		[RFC793]
7	CBT	CBT		[Tony_Ballardie]
8	EGP	Exterior Gateway Protocol		[RFC888][David_Mills]
9	IGP	any private interior gateway (used by Cisco for their IGRP)		[Internet_Assigned_Numbe
10	BBN-RCC-MON	BBN RCC Monitoring		[Steve_Chipman]
11	NVP-II	Network Voice Protocol		[RFC741][Steve_Casner]
12	PUP	PUP		[Boggs, D., J. Shoch, E. T [[XEROX]]
13	ARGUS (deprecated)	ARGUS		[Robert_W_Scheifler]
14	EMCON	EMCON		[<mystery contact>]
15	XNET	Cross Net Debugger		[Haverty, J., "XNET Format
16	CHAOS	Chaos		[J_Noel_Chiappa]
17	UDP	User Datagram		[RFC768][Jon_Postel]

PROTOCOLO IP
FRAGMENTACION



IP puede fragmentar los paquetes para adecuarse a las **MTU** (Maximun Transmission Unit) de la capa de enlace.

Identificación: Se utiliza para identificar a los fragmentos de un mismo paquete.

Banderas: consta de tres bits, uno no utilizado:

Bit DF = 1 => no fragmentar

Bit MF = 1 => mas fragmentos

Desplazamiento: Indica la posicion relativa del fragmento dentro del paquete original, en unidades de 8 bytes.

Direcciones Físicas

Mac Address

MAC Address

Existen dos direcciones principales asignadas a un dispositivo host:

Dirección física (dirección MAC)

Dirección lógica (dirección IP)

Tanto la **dirección MAC** como la dirección IP operan juntas para identificar un dispositivo en la red. El proceso de utilizar la dirección MAC y la dirección IP para encontrar una PC es similar al proceso de utilizar el nombre y la dirección de una persona para enviarle una carta.

- El nombre de una persona generalmente no cambia.
- Por otro lado, la dirección de una persona indica dónde vive esa persona y puede cambiar.
- La dirección MAC en un host, como los nombres de las personas, no cambia; se asigna físicamente a la NIC del host y se conoce como “dirección física”.
- La dirección física es siempre la misma, independientemente del lugar en donde se encuentre el host.

MAC Address
La sintaxis de la dirección MAC

Las direcciones MAC en redes LAN o WLAN constan de 6 bytes (48 bits) y están escritas en notación hexadecimal.

El uso de separadores como guiones o dos puntos entre dos bytes facilita la lectura.

El siguiente ejemplo muestra la dirección MAC de un ordenador en representación binaria y hexadecimal:

Binario: 00110101 01101000 10110100 00000010 00010011 10011000

Hexa: AC-16-2D-02-C8-19

MAC Address

La sintaxis de la dirección MAC

La secuencia de bits de cada dirección MAC se divide en 4 áreas, cada una de las cuales codifica información diferente.

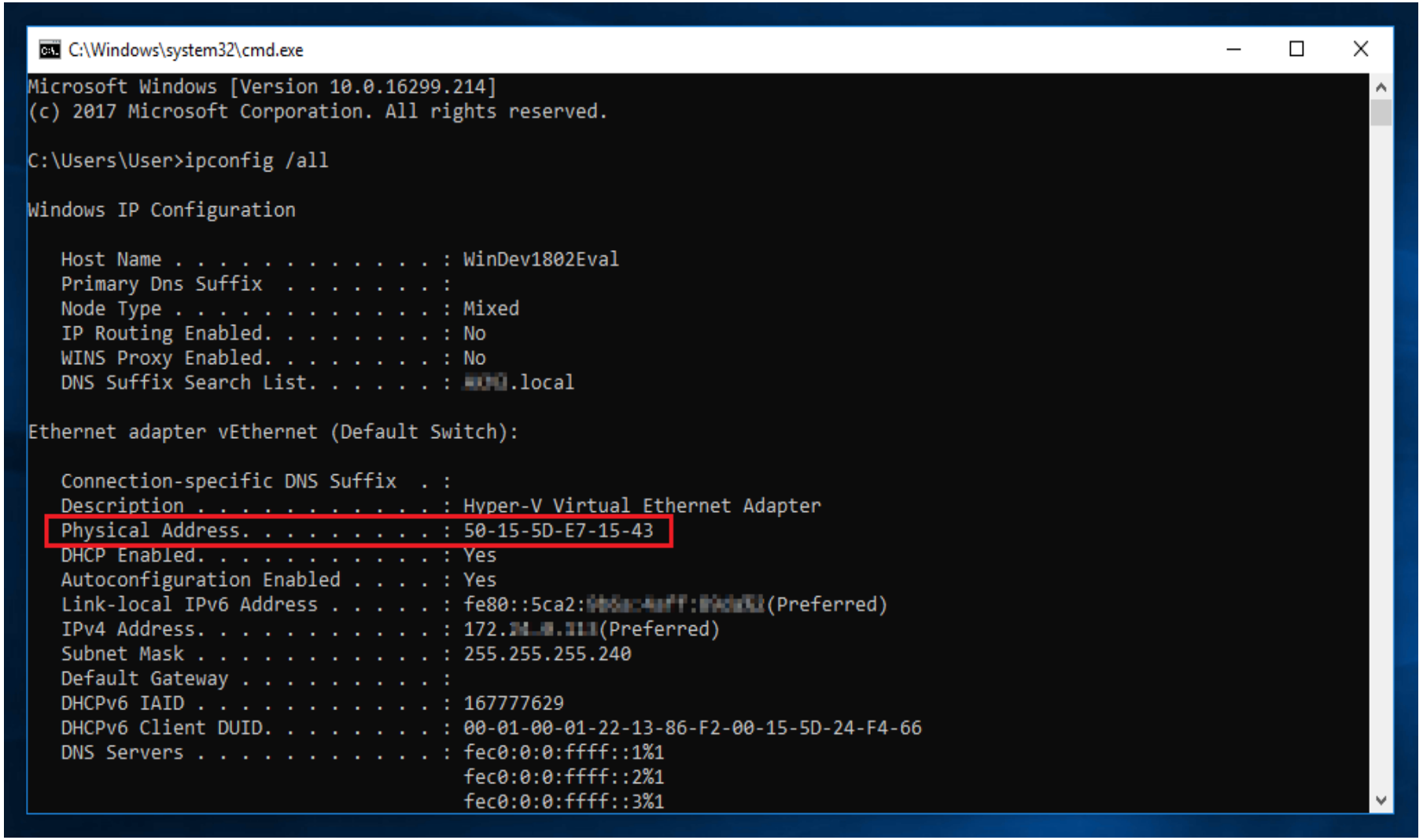
- **Bit 1 (destinatarios):** el primer bit de la dirección MAC indica si se trata de una dirección individual o de grupo. Este bit se llama I/G (abreviatura de Individual/Group). Si I/G = 0, es una dirección unicast para un solo adaptador de red. Las direcciones multidifusión se identifican con I/G = 1 y se dirigen a varios destinatarios.

- **Bit 2 (oficina de emisión):** el segundo bit de la dirección MAC indica si es una dirección con validez global (Universal) o si la dirección fue asignada localmente (Local). El bit se denomina U/L. Si U/L = 0, la dirección se considera una dirección de administración universal (UAA) válida en todo el mundo. Las direcciones que sólo son localmente únicas se denominan Dirección de administración local (LAA) y se marcan con U/L = 1.

- **Bits 3 - 24 (identificación del fabricante):** Los bits 3 a 24 codifican un identificador único de la organización (OUI), que es asignado exclusivamente a los fabricantes de hardware por la IEEE. La asignación de las OUI es generalmente pública y puede determinarse a través de bases de datos. La OUI de la dirección del ejemplo (AC-16-2D) fue asignada por el IEEE al fabricante de dispositivos estadounidense Hewlett Packard.

- **Bits 25 - 48 (identificación del adaptador de red):** Los bits 25 a 48 proporcionan 24 bits para que los fabricantes de dispositivos asignen un identificador de hardware único (Organizationally Unique Address, OUA). De este modo, se pueden asignar 2^{24} (= 16.777.216) OUAs únicas por OUI.

MAC Address
La sintaxis de la dirección MAC



MAC Address

Dirección física (dirección MAC)

- Un dispositivo de origen envía un paquete sobre la base de una dirección IP.
- El servicio de nombres de dominios (DNS), en el que una dirección IP se asocia a un nombre de dominio, es una de las formas más comunes en que un dispositivo de origen determina la dirección IP de un dispositivo de destino.
- Por ejemplo, www.cisco.com equivale a 209.165.200.225. Esta dirección IP envía el paquete a la ubicación de red del dispositivo de destino.
- Los routers utilizan esta dirección IP para determinar el mejor camino para llegar a destino. Entonces, en resumen, el direccionamiento IP determina el comportamiento de extremo a extremo de un paquete IP.
- Sin embargo, en cada enlace de la ruta, se encapsula un paquete IP en una trama específica de la tecnología de enlace de datos particular relacionada con ese enlace, como Ethernet.
- Los dispositivos finales en una red Ethernet no aceptan ni procesan tramas según las direcciones IP. Por el contrario, las tramas se aceptan y procesan según las direcciones MAC.
- En las redes Ethernet, las direcciones MAC se utilizan para identificar, en un nivel inferior, los hosts de origen y destino.

MAC Address cont.

- En las redes Ethernet, las direcciones MAC se utilizan para identificar, en un nivel inferior, los hosts de origen y destino.
- Cuando un host de una red Ethernet se comunica, envía tramas que contienen su propia dirección MAC como origen y la dirección MAC del destinatario previsto como destino.
- Todos los hosts que reciben la trama leerán la dirección MAC de destino. El host procesa el mensaje solo si la dirección MAC de destino coincide con la dirección MAC configurada en su NIC.
- En la figura, se muestra cómo se encapsula un paquete de datos, que contiene información de la dirección IP, con el entramado de la capa de enlace de datos, que contiene información de la dirección MAC.

Un switch examina las direcciones MAC.

Un router examina las direcciones IP.

Protocolo TCP

Transmition Control Protocol

Protocolo TCP – RFC IETF 793

https://datatracker.ietf.org/doc/html/rfc793

Este es un protocolo, orientado a conexión que hace uso de diversas técnicas de control de flujo, para garantizar que los paquetes que salen desde un nodo de la red lleguen a su destino en perfecto estado. Asimismo, este protocolo a diferencia del protocolo UDP, es fiable, ya que, transporta paquetes sobre un servicio no fiable de la capa Internet.

- El protocolo TCP, esta formado por los siguientes elementos*:*
- *Saludo de tres vías (SYN).*
- *Ventanas deslizantes.*
- *Formato del segmento TCP.*

Las cuales se describen a continuación:

Protocolo TCP
3 way-handShake o saludo

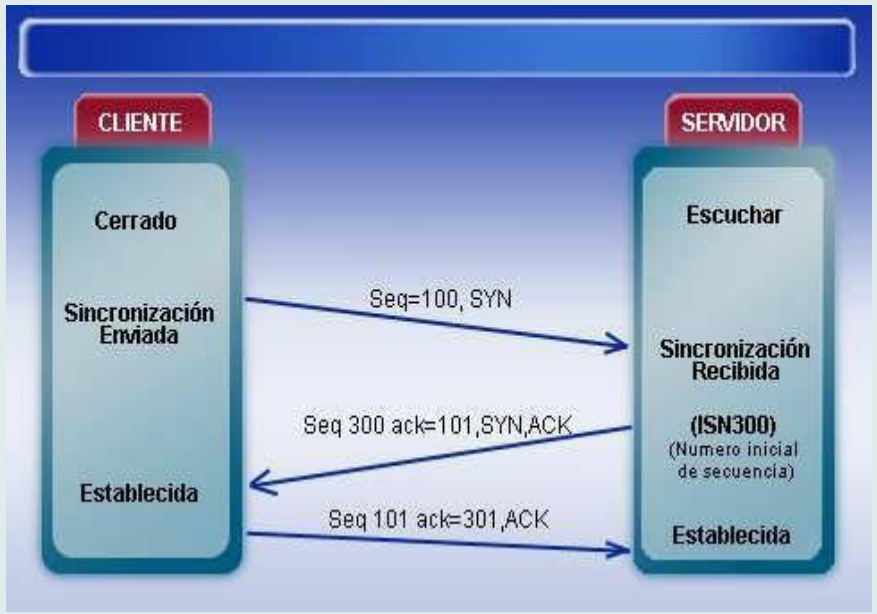
- El saludo de tres vías (*SYN*) es la sincronización de nodos emisores y receptores para que estén preparados para enviar y recibir datos, que darán lugar a la ***conexión bidireccional***, en caso contrario, el receptor desconocerá en que momento un nodo emisor empezó a enviarle información y puede concluir en la perdida de los paquetes de datos por parte del receptor, no se establece sesión.

- El mismo, se basa en la elección de un número que va a identificar de forma única cada intento de conexión de un emisor contra un receptor actuando como un PIN, de esta forma se minimiza el riesgo de aceptar como varios segmentos retrasados pudieran aparecer como resultado de conexiones anteriores.

- En el siguiente ejemplo veremos el proceso de sincronización entre ambos nodos.

Protocolo TCP
3 way-handShake o saludo

Sincronización entre ambos nodos.



1. El cliente elige para cada intento de conexión un PIN único. El número elegido lo incluye en la petición de conexión que envía al servidor.

2. El servidor, cuando recibe la petición, elige otro PIN único y envía una respuesta al cliente indicándoselo.

3. El cliente al recibir la respuesta considera establecida la conexión. A continuación envía un tercer mensaje en el que acusa recibo del anterior. El servidor considera establecida la conexión cuando el recibe este tercer mensaje.

Protocolo TCP
Formato Cabecera

El encabezado TCP

Campo TCP	Descripción
Puerto origen	Es el número de puerto de 16 bits del nodo origen
Puerto destino	El número de puerto de 16 bits del nodo destino
Número de secuencia	El número de secuencia del primer byte de datos del segmento. Si el byte de control SYN está a 1, el número de secuencia es el inicial(n) y el primer byte de datos será eln+1
Numero confirmación	Acuse de recibo
Offset de datos	Cabecera
Reservado	Debe ser cero
Flags	Banderas (URG, ACK, PSH, RST, SYN, FIN)
Ventana	Valor “n” de la ventana deslizante
Checksum	Suma de comprobación. Detección de errores
Urgent pointer	Apunta al primer octeto de datos que sigue a los datos importantes
Opciones	Opciones de datagramas IP

Protocolo UDP

User Datagram Protocol

Protocolo UDP – RFC IETF 768

https://datatracker.ietf.org/doc/html/rfc768

- Este protocolo no ofrece garantía de que el paquete de datos llegue a su destino porque no existe la verificación de software.

- Una de las ventajas de *UDP*, es su velocidad debido a que como no envía acuses de recibo no genera gran cantidad de tráfico a través de la red, lo que agiliza la transferencia.

- El mismo, está diseñado para aplicaciones que no necesitan ensamblar secuencias de segmentos, su uso principal es para protocolos como *DHCP*, *BOOTP*, *DNS*, *SMTP*, entre otros.

Protocolo UDP

- Proporciona un servicio de entrega sin conexión y no confiable, utiliza IP para transportar los mensajes en la capa de red, y agrega la capacidad de tener varios destinos dentro de una misma máquina.

- Al no proveer corrección de errores ni secuenciamiento, estas funciones deben estar contempladas en el desarrollo de la aplicación, la cual debe resolver la pérdida de paquetes, paquetes duplicados, la entrega en desordenada.

- Permite multiplexar la comunicación entre distintas aplicaciones a través de una dirección la cual se denomina puerto.

- Pregunta: ¿Un desarrollo sobre UDP que en una red LAN funciona correctamente es suficiente como para asegurar su performance en una WAN?

Protocolo UDP
Formato Cabecera

El encabezado UDP

Campo UDP	Descripción
Puerto origen	Es el número de puerto de 16 bits del nodo origen
Puerto destino	El número de puerto de 16 bits del nodo destino
Checksum	Suma de comprobación
Length	Longitud total del datagrama

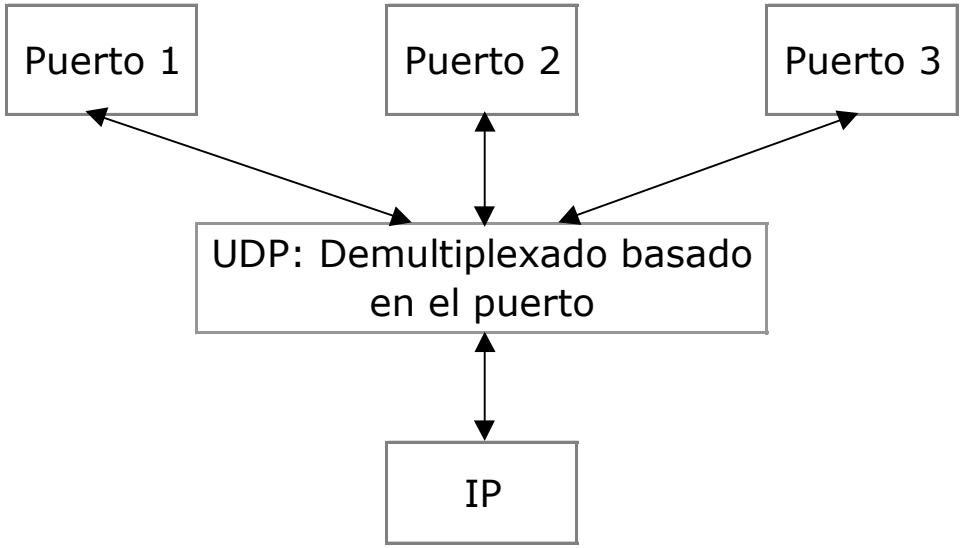
Puerto UDP origen y destino: Indica el número de puerto de los procesos involucrados. El origen puede ser cero.

Longitud: en cantidad de octetos incluyendo el encabezado.

PUERTOS

Puertos - Concepto

El multiplexado y demultiplexado de información con origen y/o destino distintos programa se realiza a través de los puertos UDP.



Puertos TCP / UDP

Port	Nombre	Tipo	Descripción	Port	Nombre	Tipo	Descripción
7	echo	tcp/udp	Echo	101	hostname	tcp	NIC Host Name Server
9	discard	tcp/udp	Discard	102	iso-tsap	tcp	ISO-TSAP
11	systat	tcp/udp	Active Users	107	rtelnet	tcp/udp	Remote Telnet Service
13	daytime	tcp/udp	Daytime	109	pop2	tcp	Post Office Protocol - Ver 2
17	qotd	tcp/udp	Quote of the Day	110	pop3	tcp	Post Office Protocol - Ver 3
19	chargen	tcp/udp	Character Generator	111	sunrpc	tcp/udp	SUN Remote Procedure Call
20	ftp-data	tcp	File Transfer [Default Data]	113	auth	tcp	Authentication Service
21	ftp	tcp	File Transfer [Control]	115	sftp	tcp/udp	Simple File Transfer Protocol
23	telnet	tcp	Telnet	119	nntp	tcp	Network News Transfer Prot
25	smtp	tcp	Simple Mail Transfer	123	ntp	udp	Network Time Protocol
37	time	tcp/udp	Time	129	pwdgen	tcp	Password Generator Protocol
42	nameserver	tcp/udp	Host Name Server	137	netbios-ns	tcp/udp	NETBIOS Name Service
43	nicname	tcp/udp	Who Is	138	netbios-dgm	tcp/udp	NETBIOS Datagram Service
53	domain	tcp/udp	Domain Name Server	139	netbios-ssn	tcp/udp	NETBIOS Session Service
67	bootps	udp/udp	Bootstrap Protocol Server	161	snmp	udp	SNMP
69	tftp	udp	Trivial File Transfer	162	snmptrap	udp	SNMPTRAP
70	gopher	tcp	Gopher	194	irc	tcp	Internet Relay Chat Protocol
79	finger	tcp	Finger	513	who	udp	Rwho daemon unix
80	www-http	tcp	World Wide Web HTTP	525	timed	tcp	Daemon de hora

Direccionamiento IP

Direccionamiento IP

Protocolo IP
Direccionamiento

- A cada host en la red le es asignado un número entero y único como dirección, llamado dirección IP o dirección lógica.
- No depende del hardware subyacente. No es una dirección física como la de ethernet.
- La dirección IP mide 32 bits
- Estructura jerárquica: todos los hosts de una red comparten una determinada cantidad de bits en común (dirección de red).

Protocolo IP
Direcciones Representación

Notación decimal con punto.

La direcciones IP se escriben como 4 enteros decimales separado por punto. Cada uno estos enteros corresponde a cada octeto de la dirección de 32 bits.

Ej. 10000000 00000000 00000001 00000010

en decimal es el 128.0.1.2

Protocolo IP

Direcciones IP - Clases

Clase A:

Net . Host . Host . Host $2^{24} - 2 > 16M$ hosts

Class B:

Net . Net . Host . Host $2^{16} - 2 = 65534$ hosts

Class C:

Net . Net . Net . Host $2^{8} – 2 = 254$ hosts

Protocolo IP

Direcciones - Regla del primer octeto

- Clase A: 1.0.0.0 a 126.0.0.0
  0xxxxxxx.xxxxxxxx.xxxxxxxx.xxxxxxxx

- Clase B: 128.0.0.0 a 191.0.0.0
  10xxxxxx.xxxxxxxx.xxxxxxxx.xxxxxxxx

- Clase C: 192.0.0.0 a 223.0.0.0
  110xxxxx.xxxxxxxx.xxxxxxxx.xxxxxxxx

- Clase D: 224.0.0.0 a 240.0.0.0
  Multicast

- Clase E: 241.0.0.0 a 248.0.0.0
  Está reservada para uso futuro

Protocolo IP
Direcciones Privadas

Direcciones privadas:

RFC 1918 **https://datatracker.ietf.org/doc/html/rfc1918**

son direcciones que no son enrutables en Internet, por lo tanto no deberían☺ ser “vistas”, fuera del contexto privado

- **Clase A:** **10.X.X.X/8**
- **Clases B:** **172.16.X.X/12**
- **Clases C:** **192.168.X.X/16**

Interface loopback:

- Permite a un cliente comunicarse con un servidor dentro de la misma máquina sin tener que usar una tarjeta de red.
- Se usa la clase A 127.0.0.0, de la que utilizamos la dirección 127.0.0.1 como dirección loopback.

Protocolo IP
Direcciones Reservadas

Bloques de direcciones especiales

Bloque de direcciones	Rango	Número de direcciones	Alcance	Descripción
0.0.0.0/8	0.0.0.0–0.255.255.255	16.777.216	Software	Red actual[3] (solo válido como dirección de origen).
10.0.0.0/8	10.0.0.0–10.255.255.255	16.777.216	Red privada	Utilizado para las comunicaciones locales dentro de una red privada.[4]
100.64.0.0/10	100.64.0.0–100.127.255.255	4.194.304	Red privada	Espacio de direcciones compartido[5] para las comunicaciones entre un proveedor de servicios y sus suscriptores cuando se utiliza un NAT de nivel de operador.
127.0.0.0/8	127.0.0.0–127.255.255.255	16.777.216	Host	Se utiliza para las direcciones de loopback.[3]
169.254.0.0/16	169.254.0.0–169.254.255.255	65.536	Subred	Se utiliza para las direcciones de enlace local[6] l entre dos hosts en un solo enlace cuando de otra manera no se especifica una dirección IP, como normalmente se habría recuperado de un servidor DHCP.
172.16.0.0/12	172.16.0.0–172.31.255.255	1.048.576	Red privada	Utilizado para las comunicaciones locales dentro de una red privada.[4]
192.0.0.0/24	192.0.0.0–192.0.0.255	256	Red privada	IETF Protocol Assignments.[3]
192.0.2.0/24	192.0.2.0–192.0.2.255	256	Documentación	Asignada como TEST-NET-1, para documentación y ejemplos.[7]
192.88.99.0/24	192.88.99.0–192.88.99.255	256	Internet	Reservada.[8] Previamente usado para *relay* IPv6 a IPv4.[9] (incluido el bloque de direcciones IPv6 2002::/16).
192.168.0.0/16	192.168.0.0–192.168.255.255	65.536	Red privada	Utilizado para las comunicaciones locales dentro de una red privada.[4]
198.18.0.0/15	198.18.0.0–198.19.255.255	131.072	Red privada	Se utiliza para pruebas de referencia de comunicaciones entre dos subredes separadas.[10]
198.51.100.0/24	198.51.100.0–198.51.100.255	256	Documentación	Asignado como TEST-NET-2, para documentación y ejemplos.[7]
203.0.113.0/24	203.0.113.0–203.0.113.255	256	Documentación	Asignado como TEST-NET-3, para documentación y ejemplos.[7]
224.0.0.0/4	224.0.0.0–239.255.255.255	268.435.456	Internet	Usado para Multicast IP.[11] (previamente una red clase D). (Experimental)
240.0.0.0/4	240.0.0.0–255.255.255.254	268.435.456	Internet	Reservada para usos futuros.[12] (anteriormente una red clase E). (Experimental)
255.255.255.255/32	255.255.255.255	1	Subred	Reservada para destinos multidifusión.[3] [13]

Protocolo IP

Direcciones Máscara/Classless

Para optimizar el espacio de direcciones se trabaja en ambientes classless (sin clases). Ej.: Internet.

La máscara indica la cantidad de bits que corresponden a la red (posiciones donde hay «unos»).

Las direcciones se dan en pares Address/Mask.

Ejemplo:

192.168.1.5

255.255.255.0

También se utiliza el formato IP/Nro bits de máscara:

192.168.1.5/24

La máscara permite crear «subredes», es decir subdividir una red en varias subredes que soporten menor cantidad de hosts cada una.

Protocolo IP
Direcciones VLSM y CIDR

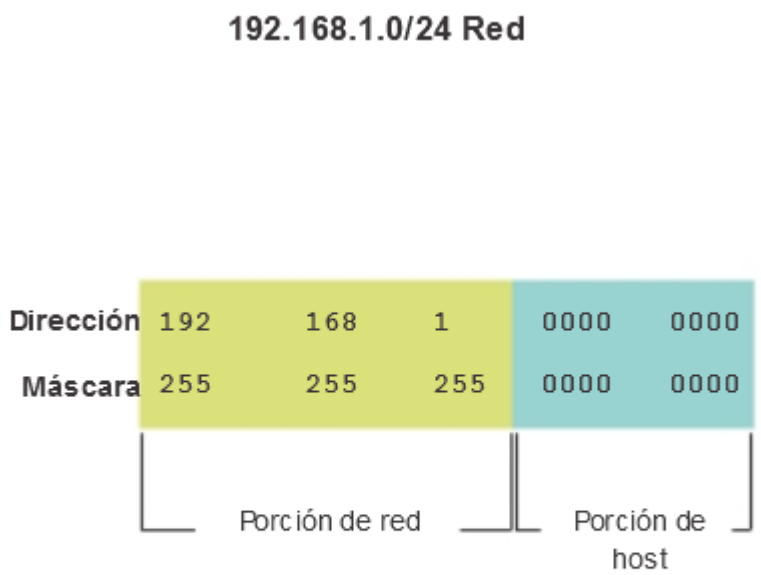
El subneteo con VLSM (Variable Length Subnet Mask), máscara de subred de longitud variable, es uno de los métodos que se implementó para evitar el agotamiento de direcciones IPv4 permitiendo un mejor aprovechamiento y optimización del uso de direcciones.

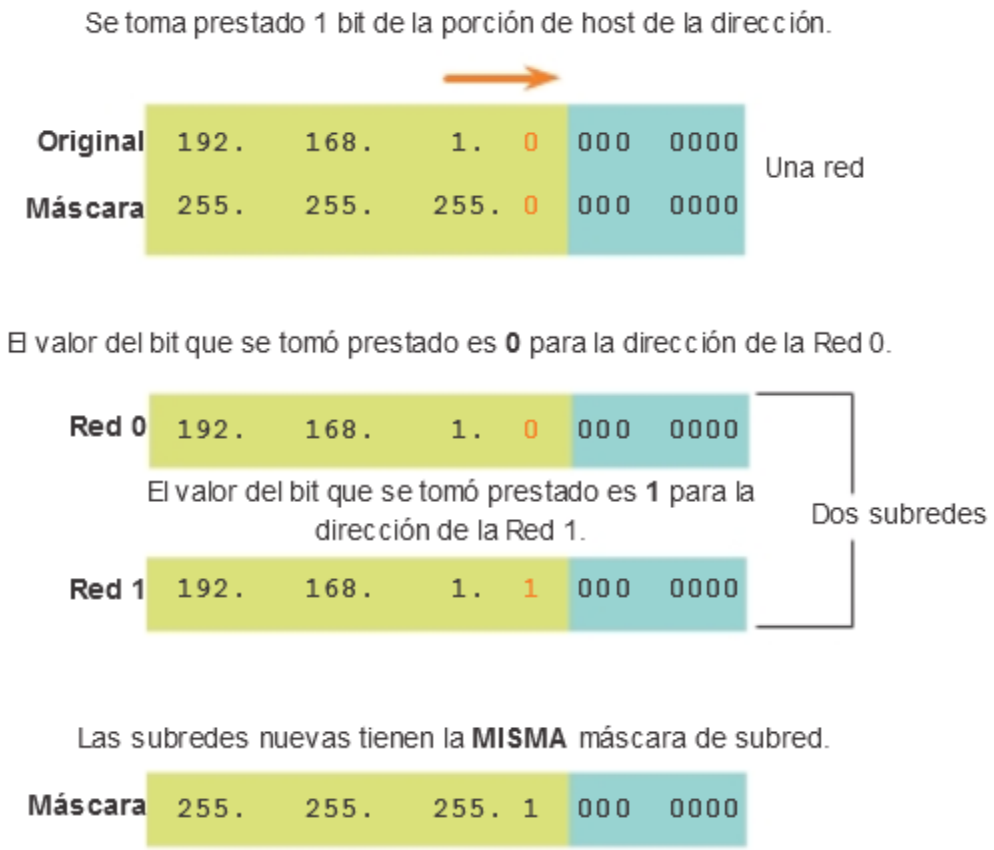
- **VLSM**: Es el resultado del proceso por el cual se divide una red o subred en subredes más pequeñas cuyas máscaras son diferentes según se adaptan a las necesidades de hosts por subred.
- **CIDR** (Classless Inter-Domain Routing - Enrutamiento Inter-Dominios sin Clases): es la capacidad que tienen los protocolos de enrutamiento de enviar actualizaciones a sus vecinos de redes con VLSM y de sumarizar esas direcciones en una sola dirección.

Protocolo IP
Sub redes

- Cada dirección de red tiene un rango válido de direcciones de host.
- Todos los dispositivos conectados a la misma red tendrán una dirección de host IPv4 para esa red y una máscara de subred o un prefijo de red común.
- El prefijo y la máscara de subred son diferentes formas de representar lo mismo, la porción de red de una dirección.
- Las subredes IPv4 se crean utilizando uno o más de los bits de host como bits de red.
- Esto se hace ampliando la máscara para tomar prestado algunos de los bits de la porción de host de la dirección, a fin de crear bits de red adicionales.
- Cuantos más bits de host se tomen prestados, mayor será la cantidad de subredes que puedan definirse.
- Por cada bit que se toma prestado, se duplica la cantidad de subredes disponibles.
- Por ejemplo, si se toma prestado 1 bit, se pueden crear 2 subredes. Si se toman prestados 2 bits, se crean 4 subredes; si se toman prestados 3 bits, se crean 8 subredes, y así sucesivamente.
- Sin embargo, con cada bit que se toma prestado, se dispone de menos direcciones de host por subred.
- Los bits solo se pueden tomar prestados de la porción de host de la dirección. El proveedor de servicios determina la porción de red de la dirección, la que no puede modificarse.

Protocolo IP
Sub redes

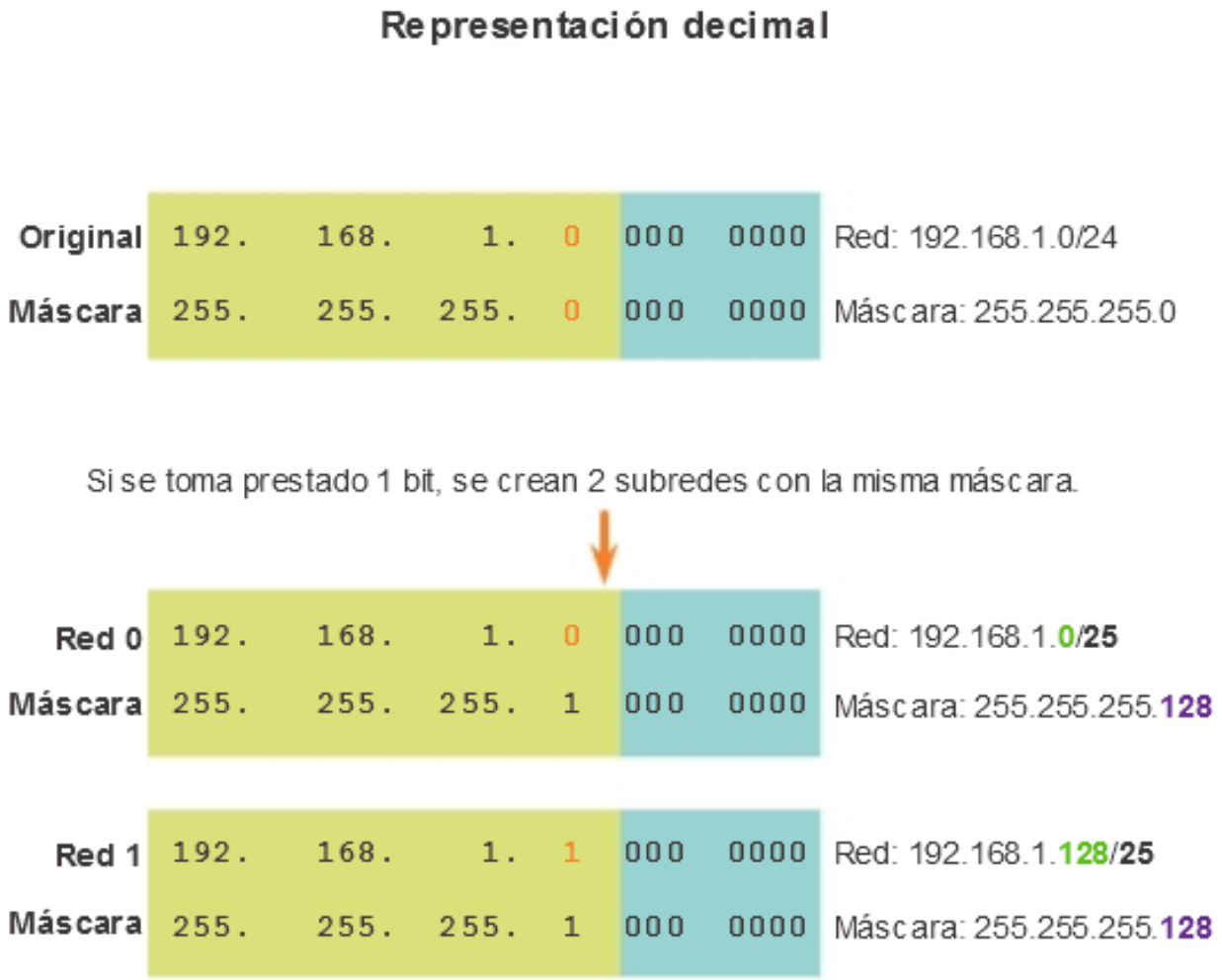




Protocolo IP
Sub redes

- La red 192.168.1.0/24 tiene 24 bits en la porción de red y 8 bits en la porción de host, lo que se indica con la máscara de subred 255.255.255.0 o la notación /24.
- Sin división en subredes, esta red admite una única interfaz LAN. Si se necesitara otra LAN, sería necesario dividir la red en subredes.
- Se toma prestado 1 bit del bit más significativo (el bit que se encuentra más a la izquierda) en la porción de host, lo que extiende la porción de red a 25 bits.
- Esto crea 2 subredes que se identifican mediante un 0 en el bit que se tomó prestado para la primera red y un 1 en el bit que se tomó prestado para la segunda red.
- La máscara de subred para ambas redes utiliza un 1 en la posición del bit que se tomó prestado para indicar que ahora este bit es parte de la porción de red.
- Cuando convertimos el octeto binario al sistema decimal, advertimos que la dirección de
  - La primera subred es: 192.168.1.0
  - La segunda subred es 192.168.1.128.
  - Dado que se tomó prestado un bit, la máscara de subred de cada subred es 255.255.255.128 o /25.

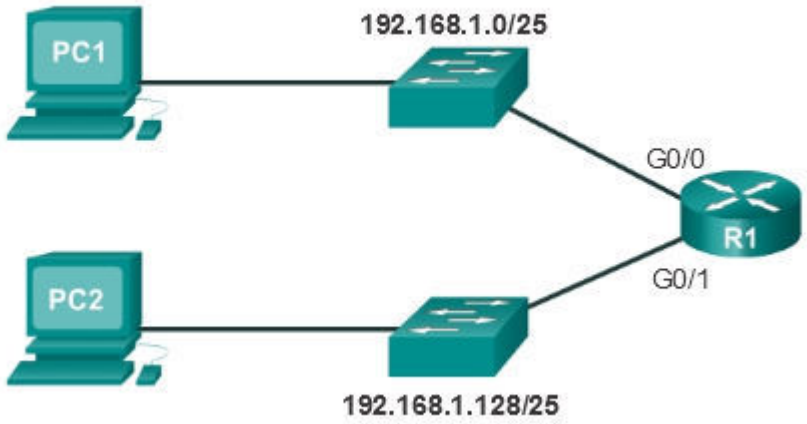
Protocolo IP
Sub redes



Protocolo IP
Sub redes

- En el ejemplo anterior, se dividió la red 192.168.1.0/24 para crear dos subredes:
  - 192.168.1.0/25
  - 192.168.1.128/25
- En la figura 1, observe que el router R1 tiene dos segmentos LAN conectados a sus interfaces GigabitEthernet. Para los segmentos conectados a estas interfaces, se utilizarán subredes.
- Para cumplir la función de gateway para los dispositivos en la LAN, a cada una de las interfaces del router se le debe asignar una dirección IP dentro del rango de direcciones válidas para la subred asignada.
- La primera subred, 192.168.1.0/25, se utiliza para la red conectada a GigabitEthernet 0/0, y la segunda subred, 192.168.1.128/25, se utiliza para la red conectada a GigabitEthernet 0/1.
- Para asignar una dirección IP para cada una de estas interfaces, se debe determinar el rango de direcciones IP válidas para cada subred.
- Las siguientes son pautas para cada una de las subredes:
  - **Dirección de red:** todos bits 0 en la porción de host de la dirección.
  - **Primera dirección de host:** todos bits 0 más un bit 1 (en la máxima posición a la derecha) en la porción de host de la dirección.
  - **Última dirección de host:** todos bits 1 más un bit 0 (en la máxima posición a la derecha) en la porción de host de la dirección.
  - **Dirección de broadcast:** todos bits 1 en la porción de host de la dirección.

Protocolo IP
Sub redes



Protocolo IP
Sub redes

- La primera dirección de host para la red 192.168.1.0/25 es 192.168.1.1
- La última dirección de host es 192.168.1.126.

Rango de direcciones para la subred 192.168.1.0/25

Protocolo IP
Sub redes

- La primera dirección de host para la red 192.168.1.128/25 es 192.168.1.129
- La última dirección de host es 192.168.1.254.

Rango de direcciones para la subred 192.168.1.128/25

Dirección de red

192. 168. 1. 1 000 0000 = 192.168.1.128

Primera dirección de host

192. 168. 1. 1 000 0001 = 192.168.1.129

Última dirección de host

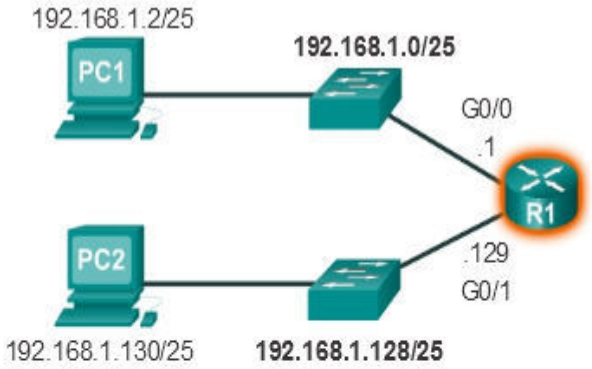
192. 168. 1. 1 111 1110 = 192.168.1.254

Dirección de broadcast

192. 168. 1. 1 111 1111 = 192.168.1.255

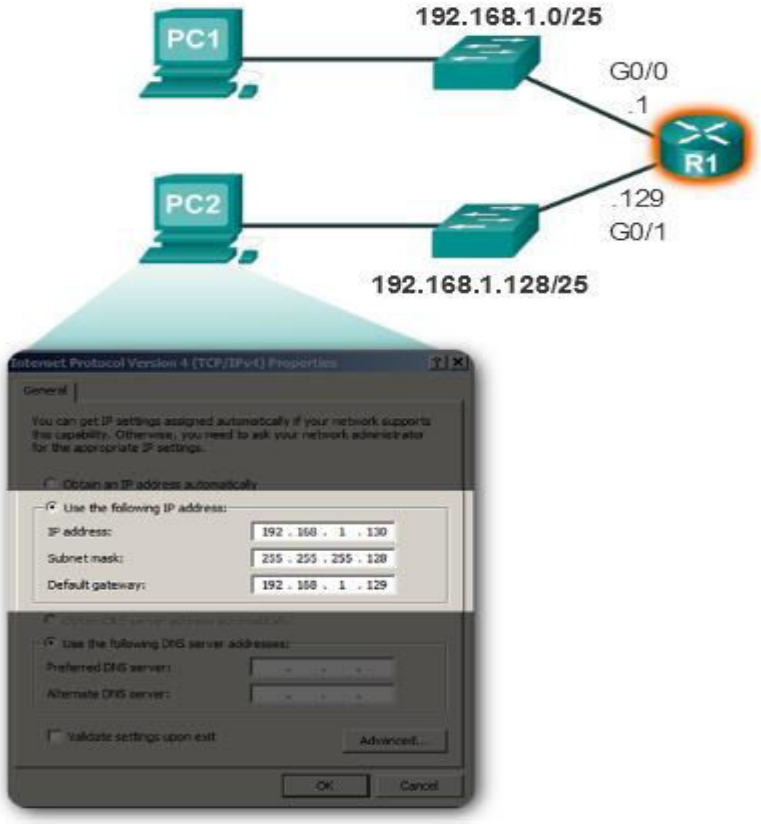
Protocolo IP
Sub redes

- Configuración en router Cisco




```
R1(config)# interface gigabitethernet 0/0
R1(config-if)# ip address 192.168.1.1 255.255.255.128
R1(config-if)# exit
R1(config)# interface gigabitethernet 0/1
R1(config-if)# ip address 192.168.1.129 255.255.255.128
```

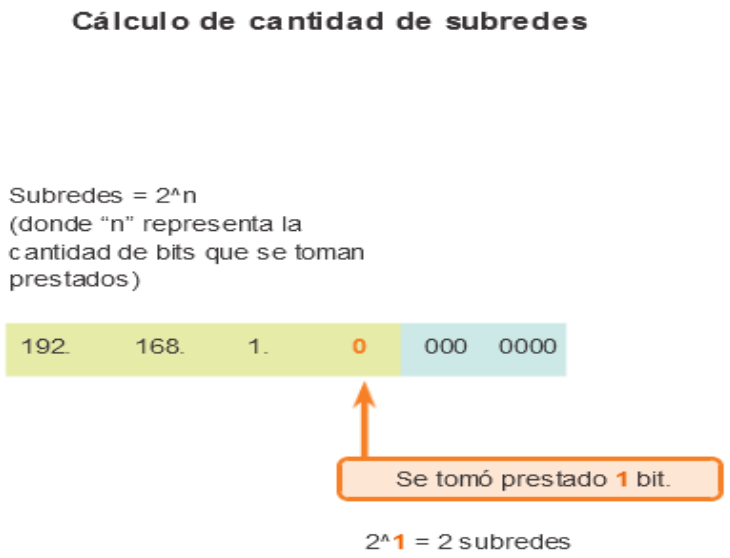
- Configuración en PC



Protocolo IP
Fórmula para calcular Sub redes

Cálculo de subredes

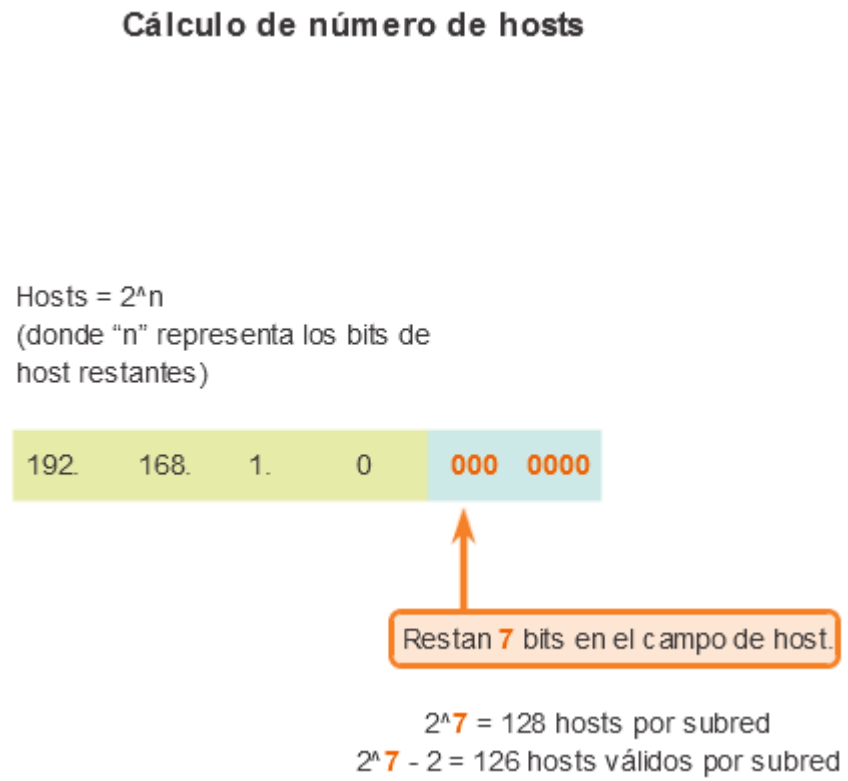
- Use esta fórmula para calcular la cantidad de subredes:
- 2^n (donde “n” representa la cantidad de bits que se toman prestados)
- Como se muestra en la figura 1, para el ejemplo 192.168.1.0/25, el cálculo es el siguiente:
- 2^1 = 2 subredes



Protocolo IP
Fórmula para calcular Sub redes

Cálculo de hosts

- 2^n (donde “n” representa la cantidad de bits restantes en el campo de host)
- Como se muestra en la figura 2, para el ejemplo 192.168.1.0/25, el cálculo es el siguiente:
- 2^7 = 128
- Debido a que los hosts no pueden utilizar la dirección de red o a la dirección de broadcast de una subred, dos de estas direcciones no son válidas para la asignación de hosts. Esto significa que cada una de las subredes tiene 126 (128-2) direcciones de host válidas.
- En este ejemplo, si se toma prestado 1 bit de host para la red, se crean 2 subredes, y cada subred puede tener un total de 126 hosts asignados.



Protocolo IP
Direcciones VLSM ejemplo

Ej: Con el rango 192.168.10.0/24 diseñar el plan de numeración LAN para 3 sitios con capacidad de 50 hosts por sitio.

Cant de bits para host: $2^6 = 64$

Cant de bits de mascara = 32 - 6 = 26 => Mask=255.255.255.192

Primera subred:

11111111.11111111.11111111.11	000000	MASK
11000000.10101000.00001010.00	000000	NETWORK
11000000.10101000.00001010.00	111111	BROADCAST

Netw1: 192.168.10.0

Broadcast1: 192.168.10.63

Hosts1:192.168.10.1 – 192.168.10.62

Protocolo IP

Direcciones VLSM ejemplo cont.

Segunda subred:

11111111.11111111.11111111.11 000000	MASK
11000000.10101000.00001010.01 000000	NETWORK
11000000.10101000.00001010.01 111111	BROADCAST

Netw2: 192.168.10.64

Broadcast2: 192.168.10.127

Hosts2:192.168.10.65 – 192.168.10.126

Protocolo IP

Direcciones VLSM ejemplo cont.

Tercera subred:

11111111.11111111.11111111.11 000000	MASK
11000000.10101000.00001010.10 000000	NETWORK
11000000.10101000.00001010.10 111111	BROADCAST

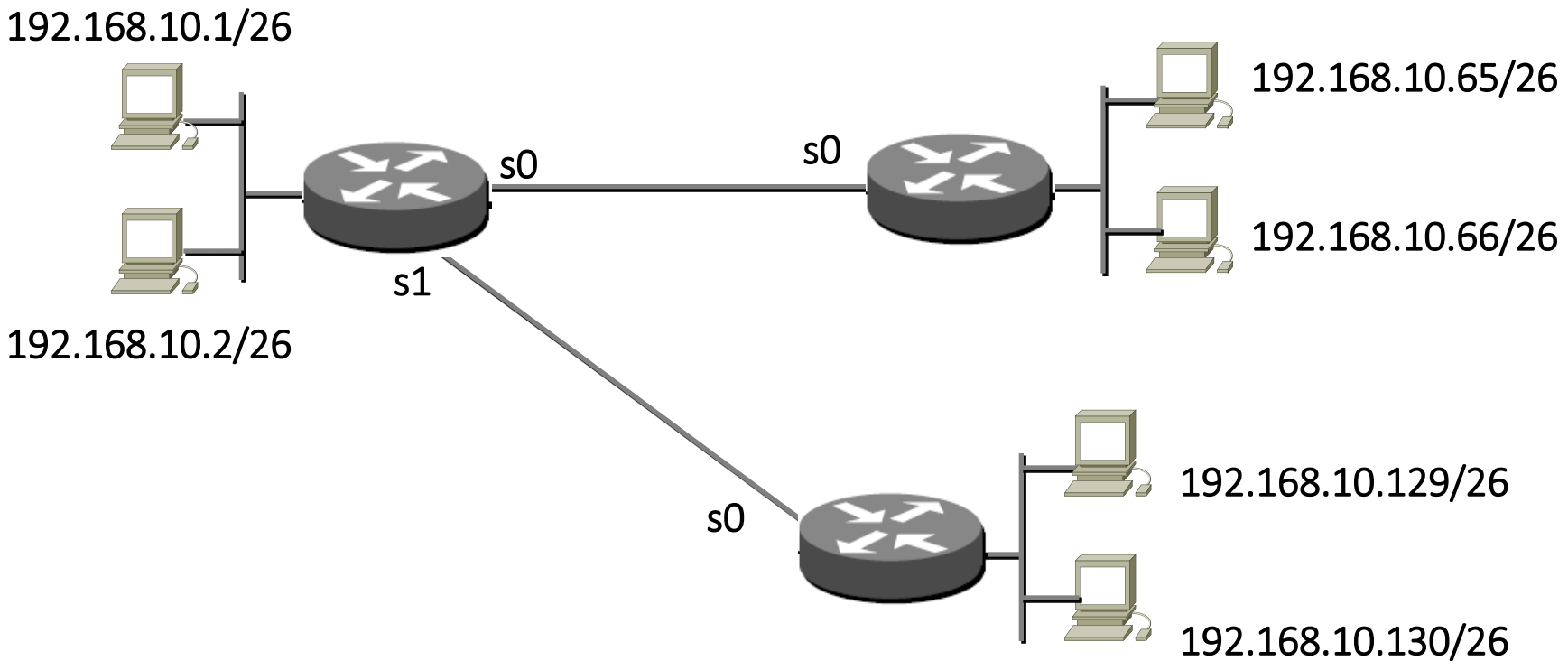
Netw3: 192.168.10.128

Broadcast3: 192.168.10.191

Hosts3:192.168.10.129 – 192.168.10.190

Protocolo IP

Direcciones VLSM ejemplo cont.



Protocolo IP
Transmisión de datos

En una red IPv4, los hosts pueden comunicarse de una de tres maneras:

Unicast: proceso por el cual se envía un paquete de un host a un host individual.

Broadcast: proceso por el cual se envía un paquete de un host a todos los hosts en la red.

Multicast: proceso por el cual se envía un paquete de un host a un grupo seleccionado de hosts, posiblemente en redes distintas.

Existe una cuarta forma

Anycast: es un unicast por ubicación geográfca

Protocolo IP
Transmisión **Unicast**

La comunicación unicast se usa para la comunicación normal de host a host, tanto en redes cliente/servidor como en redes punto a punto.

Los paquetes unicast utilizan las direcciones del dispositivo de destino como la dirección de destino y pueden enrutarse a través de una internetwork.

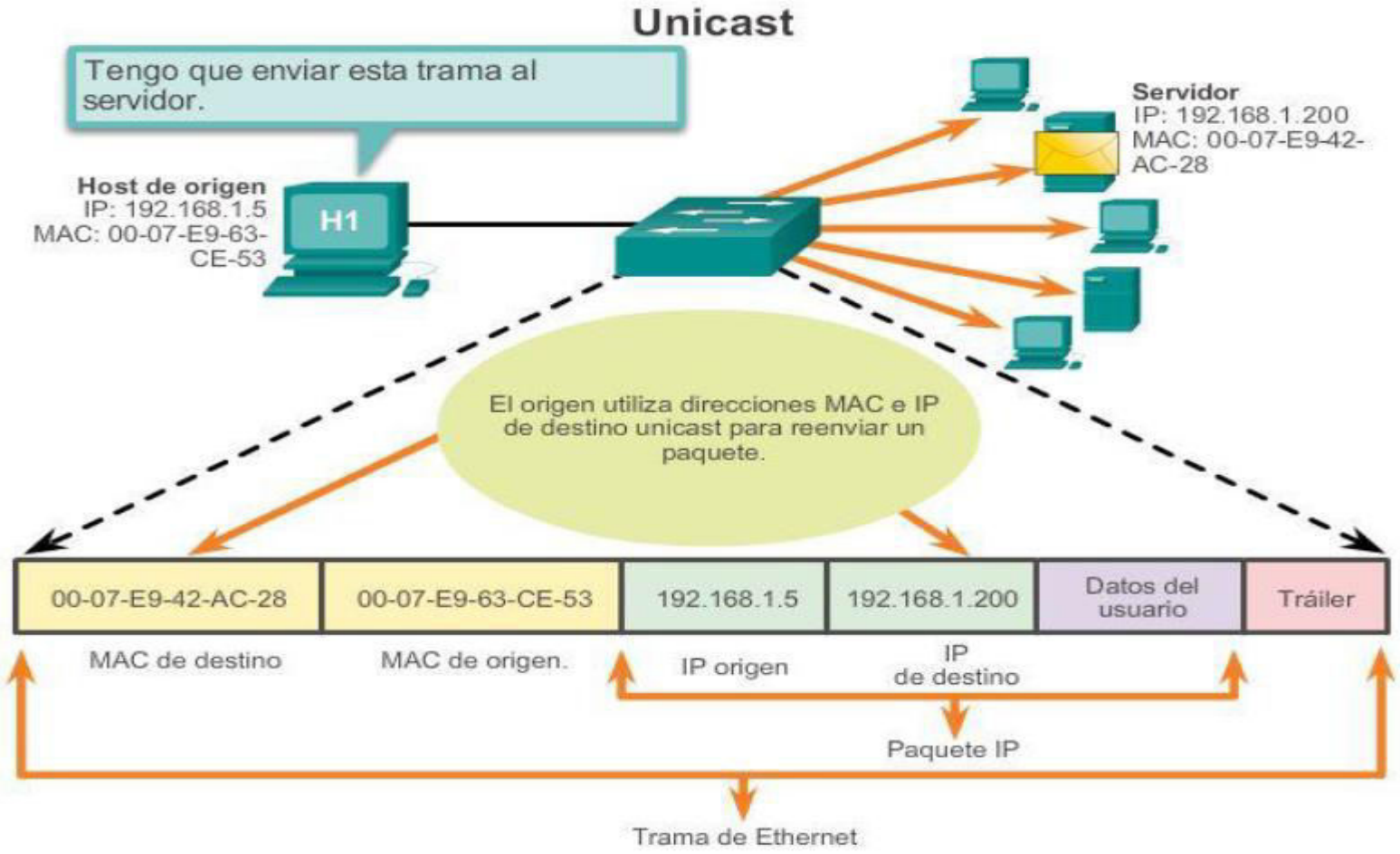
En una red IPv4, la dirección unicast aplicada a un dispositivo final se denomina “dirección de host”.

En la comunicación unicast, las direcciones asignadas a dos dispositivos finales se usan como las direcciones IPv4 de origen y de destino.

Durante el proceso de encapsulación, el host de origen coloca su dirección IPv4 en el encabezado del paquete unicast como la dirección de origen y la dirección IPv4 del host de destino en el encabezado del paquete como la dirección de destino.

Independientemente de si el destino especificado para un paquete es unicast, broadcast o multicast, la dirección de origen de cualquier paquete es siempre la dirección unicast del host de origen

Protocolo IP
Transmisión **Unicast** cont.



Protocolo IP
Transmisión **Broadcast**

El tráfico de broadcast se utiliza para enviar paquetes a todos los hosts en la red usando la dirección de broadcast para la red.

Para broadcast, el paquete contiene una dirección IP de destino con todos unos (1) en la porción de host.

Esto significa que todos los hosts de esa red local (dominio de broadcast) recibirán y verán el paquete.

Muchos protocolos de red, como DHCP, utilizan broadcasts.

Cuando un host recibe un paquete enviado a la dirección de broadcast de red, el host procesa el paquete de la misma manera en la que procesaría un paquete dirigido a su dirección unicast.

Protocolo IP
Transmisión **Broadcast** cont.

Algunos ejemplos para utilizar una transmisión de broadcast son:

- Asignar direcciones de capa superior a direcciones de capa inferior
- Solicitar una dirección
- A diferencia de unicast, donde los paquetes pueden ser enrutados por toda la internetwork, los paquetes de broadcast normalmente se restringen a la red local.

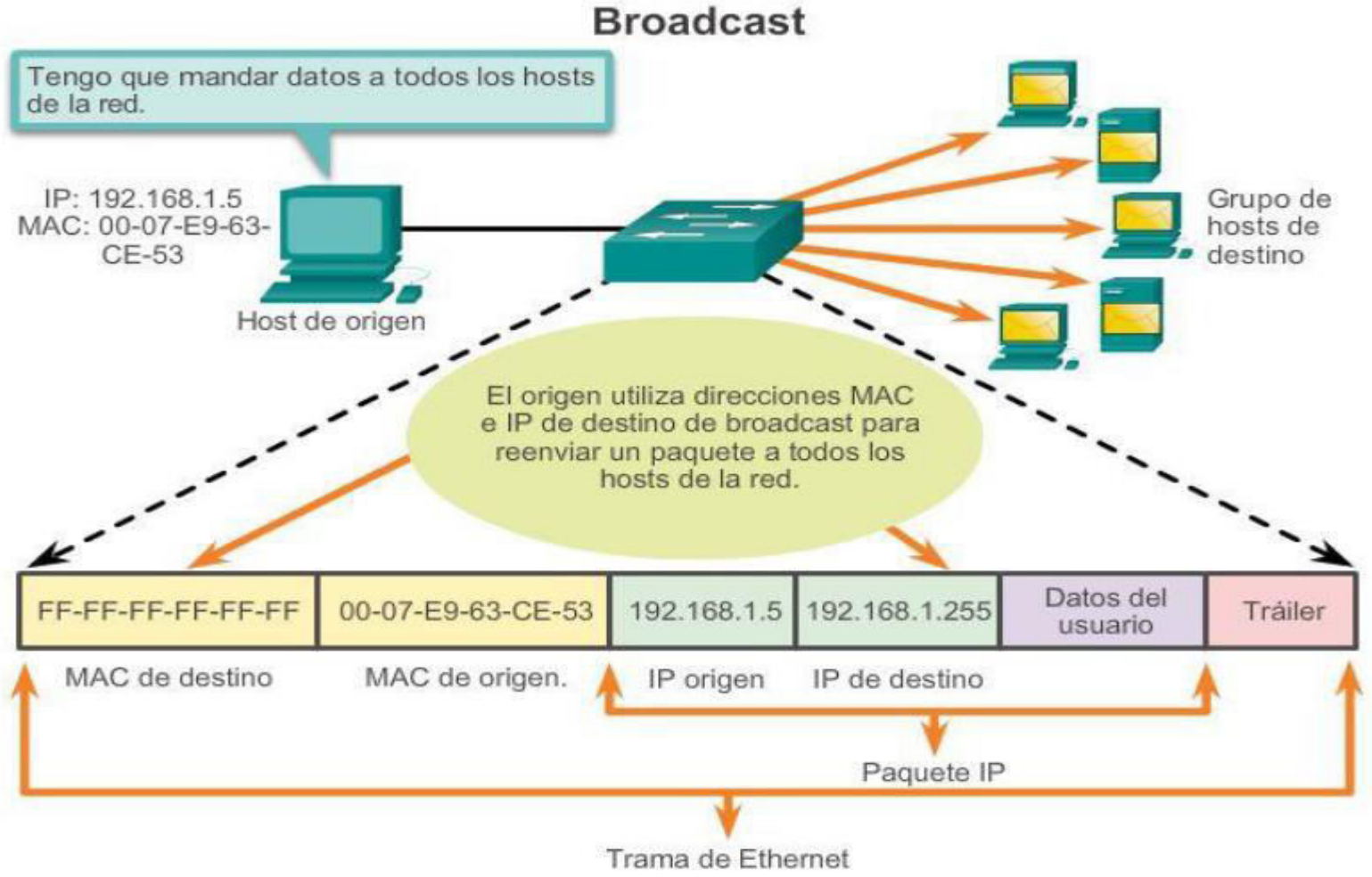
Broadcast dirigido

Un broadcast dirigido se envía a todos los hosts de una red específica.

Este tipo de broadcast es útil para enviar un broadcast a todos los hosts de una red local. Por ejemplo, para que un host fuera de la red 172.16.4.0/24 se comunique con todos los hosts dentro de esa red, la dirección de destino del paquete sería 172.16.4.255.

Aunque los routers no reenvían broadcasts dirigidos de manera predeterminada, se les puede configurar para que lo hagan.

Protocolo IP
Transmisión **Broadcast** cont.



Protocolo IP

Transmisión **Multicast**

- La transmisión de multicast está diseñada para conservar el ancho de banda de las redes IPv4.
- Reduce el tráfico al permitir que un host envíe un único paquete a un conjunto seleccionado de hosts que forman parte de un grupo multicast suscrito.
- Para alcanzar hosts de destino múltiples mediante la comunicación unicast, sería necesario que el host de origen envíe un paquete individual dirigido a cada host.
- Con multicast, el host de origen puede enviar un único paquete que llegue a miles de hosts de destino.
- La responsabilidad de la internetwork es reproducir los flujos multicast en un modo eficaz para que alcancen solamente a los destinatarios

Protocolo IP
Transmisión **Multicast** cont.

Algunos ejemplos de transmisión de multicast son:

- Transmisiones de video y de audio
- Intercambio de información de enrutamiento por medio de protocolos de enrutamiento
- Distribución de software
- Juegos remotes

Protocolo IP
Transmisión **Multicast** cont.

Direcciones multicast

- IPv4: 224.0.0.0 a 239.255.255.255.
- El rango de direcciones multicast está subdividido en distintos tipos de direcciones:

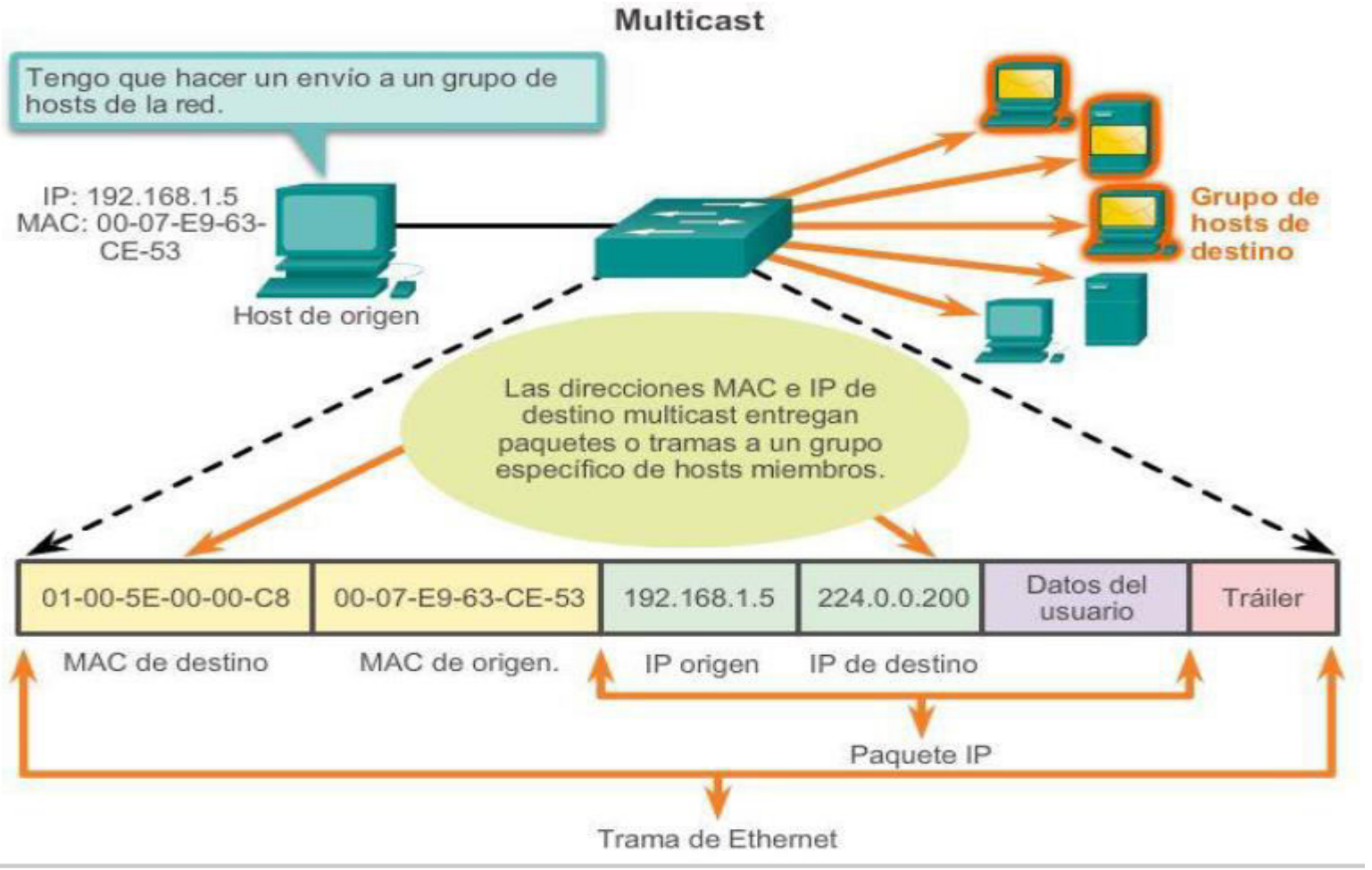
  - direcciones de enlace local reservadas

  - direcciones agrupadas globalmente.

  - Un tipo adicional de dirección multicast son las direcciones agrupadas administrativamente, también llamadas direcciones de agrupamiento limitado.

- **Enlace local reservadas**: 224.0.0.0 a 224.0.0.255. Estas direcciones se utilizarán con grupos multicast en una red local. Un uso común de las direcciones de link-local reservadas se da en los protocolos de enrutamiento usando transmisión multicast para intercambiar información de enrutamiento.
- **Direcciones agrupadas globalmente:** 224.0.1.0 a 238.255.255.255. Se les puede usar para transmitir datos en Internet mediante multicast. Por ejemplo, se reservó 224.0.1.1 para que el protocolo de hora de red (NTP) sincronice los relojes con la hora del día de los dispositivos de red.

Protocolo IP
Transmisión **Multicast** cont.



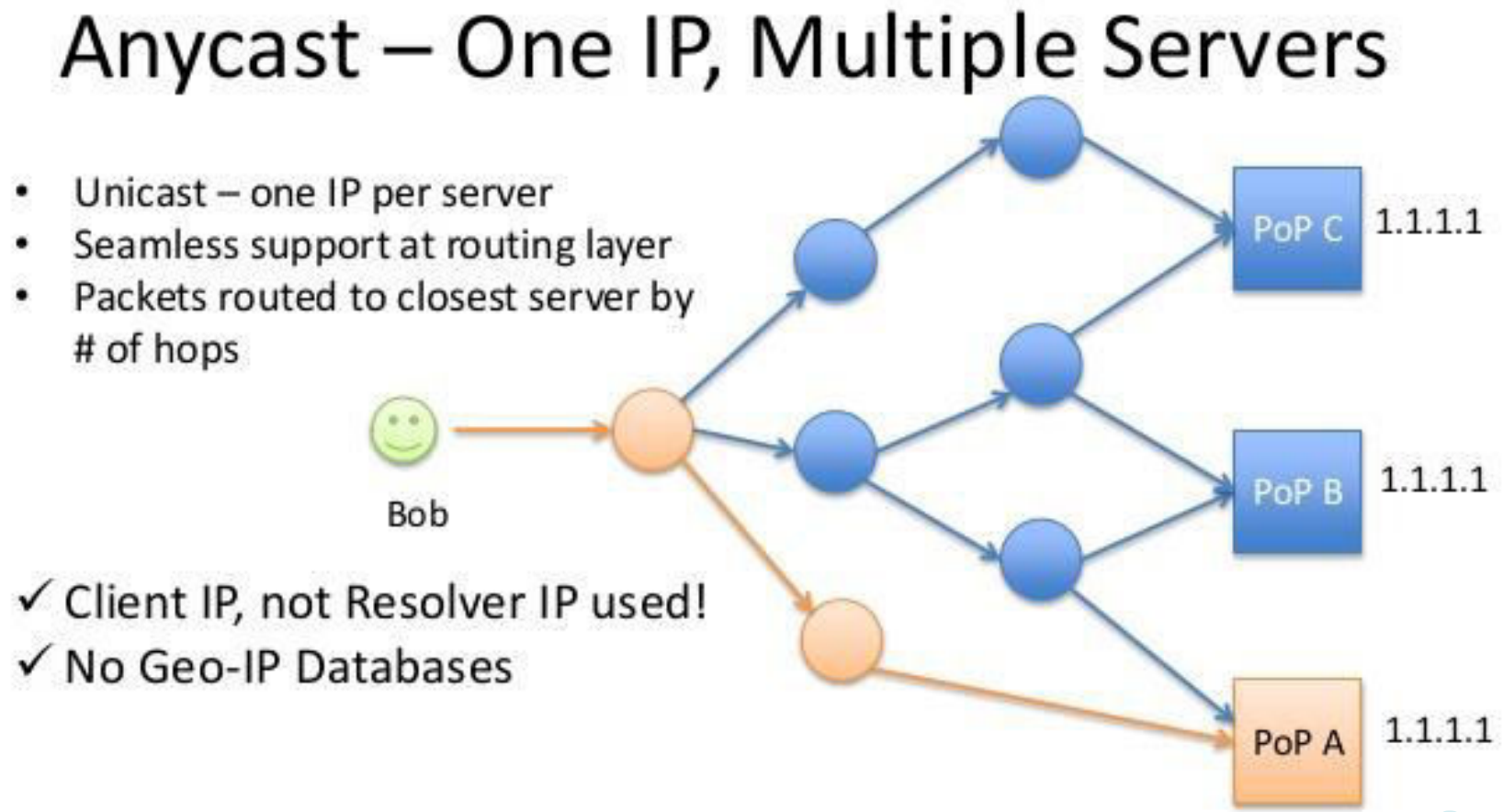
Protocolo IP
Transmisión **Anycast**

- Lo habitual es que cualquier dispositivo o servidor que se conecte directamente a Internet tenga una única dirección IP.
- La comunicación entre los dispositivos conectados a la red es de 1 a 1; cada comunicación fluye de un dispositivo específico al dispositivo objetivo al otro lado de la comunicación.
- En cambio, las redes Anycast permiten que múltiples servidores de la red utilicen la **misma dirección IP** o el mismo conjunto de direcciones IP.
- La comunicación con una red anycast es de 1 a muchos.

Protocolo IP
Transmisión **Anycast cont.**

- Una dirección IP suele funcionar como una dirección postal: especifica la ubicación específica a la que debe ir el mensaje.
- Pero pongámonos en el caso de que tenemos un amigo con muchas casas por todo el país, y que una carta dirigida a una de sus casas podría enviarse a cualquier de las otras en función de la cercanía con el remitente, a pesar de que la carta estaba remitida a una casa en otra ciudad.
- Así funciona el enrutamiento de anycast: una dirección IP se puede asociar a varias ubicaciones.
- Por ejemplo, cualquier centro de datos que opere Cloudflare puede responder a una solicitud a una dirección IP dentro del CDN de Cloudflare, en lugar de un servidor específico. Para más información sobre anycast y cómo puede usarlo una CDN, consulta

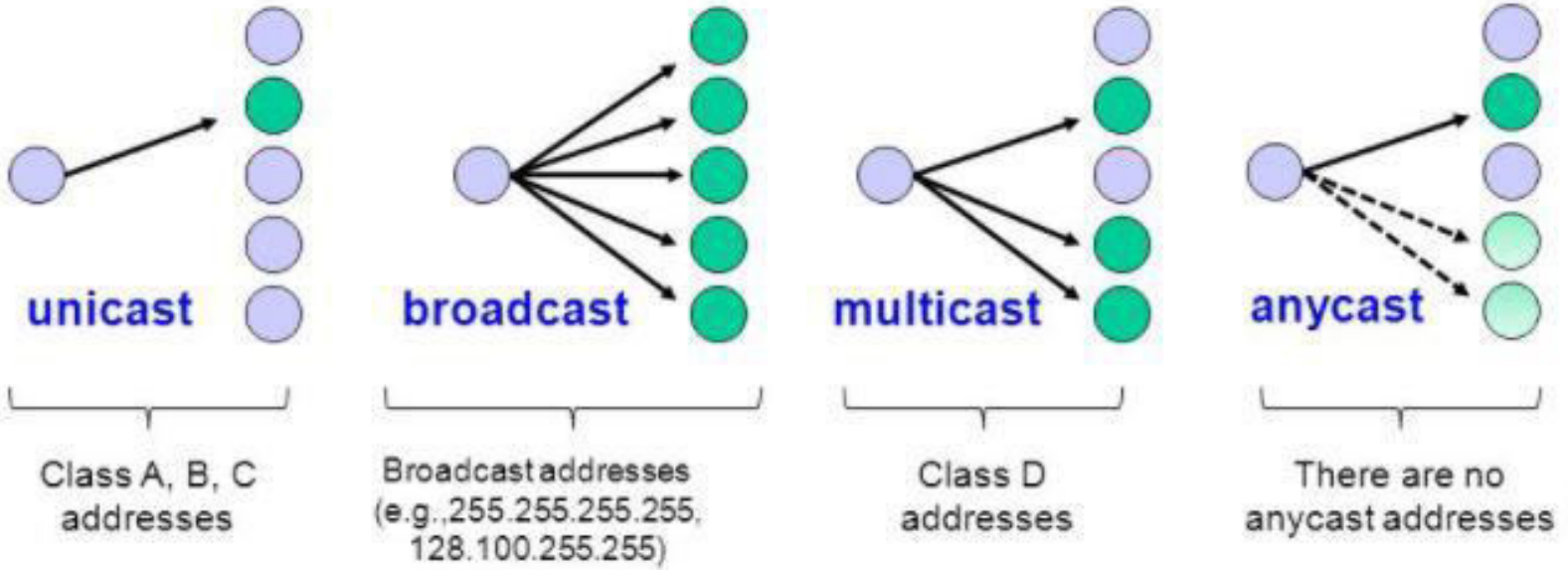
Transmisión **Anycast cont.**



Protocolo IP

Transmisión **Unicast,Broadcast,Multicast y Anycast cont.**

- Supported by IPv4
  - one-to-one (unicast)
  - one-to-all (broadcast)
  - one-to-many (multicast)
- Not supported by IPv4:
  - one-to-any (anycast)



VLANS

VLANS

VLAN
Definición

- Dentro de un entorno de internetwork conmutada, las VLAN proporcionan la segmentación y la flexibilidad organizativa.
- Las VLAN proporcionan una manera de agrupar dispositivos dentro de una LAN.
- Un grupo de dispositivos dentro de una VLAN se comunica como si estuvieran conectados al mismo cable. Las VLAN se basan en conexiones lógicas, en lugar de conexiones físicas.
- Las VLAN permiten que el administrador divida las redes en segmentos según factores como la función, el equipo del proyecto o la aplicación, sin tener en cuenta la ubicación física del usuario o del dispositivo.
- Los dispositivos dentro de una VLAN funcionan como si estuvieran en su propia red independiente, aunque compartan una misma infraestructura con otras VLAN.
- Cualquier puerto de switch puede pertenecer a una VLAN, y los paquetes de unidifusión, difusión y multidifusión se reenvían y saturan solo las estaciones terminales dentro de la VLAN donde se originan los paquetes.

VLAN
Definición

- Cada VLAN se considera una red lógica independiente, y los paquetes destinados a las estaciones que no pertenecen a la VLAN se deben reenviar a través de un dispositivo que admita el routing.
- Una VLAN crea un dominio de difusión lógico que puede abarcar varios segmentos LAN físicos.
- Las VLAN mejoran el rendimiento de la red mediante la división de grandes dominios de difusión en otros más pequeños.
- Si un dispositivo en una VLAN envía una trama de Ethernet de difusión, todos los dispositivos en la VLAN reciben la trama, pero los dispositivos en otras VLAN no la reciben.
- Las VLAN habilitan la implementación de las políticas de acceso y de seguridad según grupos específicos de usuarios.
- Cada puerto de switch se puede asignar a una sola VLAN (a excepción de un puerto conectado a un teléfono IP o a otro switch).

VLAN
Definición

- La VLAN (LAN virtual) es una partición lógica de una red de capa 2.
- Se pueden crear **varias particiones** para que coexistan varias VLAN.
- Cada VLAN es un dominio de difusión, que generalmente posee su propia red IP.
- Las VLAN se aíslan mutuamente y los paquetes pueden pasar entre ellas solamente mediante un **router**.
- La partición de la red de capa 2 se lleva a cabo dentro de un dispositivo de capa 2 (por lo general, un switch).
- Los **hosts** que se agrupan dentro de una VLAN **desconocen** la **existencia** de esta

VLAN
Beneficios

- Seguridad
- Reducción de costos
- Mejor rendimiento
- Reducción de dominios de difusión (broadcast)
- Mejora de la eficiencia del personal de TI
- Administración más simple de aplicaciones y proyectos

VLAN
Beneficios

Seguridad:

Los grupos que tienen datos sensibles se separan del resto de la red, lo que disminuye las posibilidades de que ocurran violaciones de información confidencial.

Como se muestra en la ilustración, las computadoras del cuerpo docente están en la VLAN 10 y separadas por completo del tráfico de datos de los estudiantes y los Invitados.

Reducción de costos:

El ahorro de costos se debe a la poca necesidad de actualizaciones de red costosas y al uso más eficaz de los enlaces y del ancho de banda existentes.

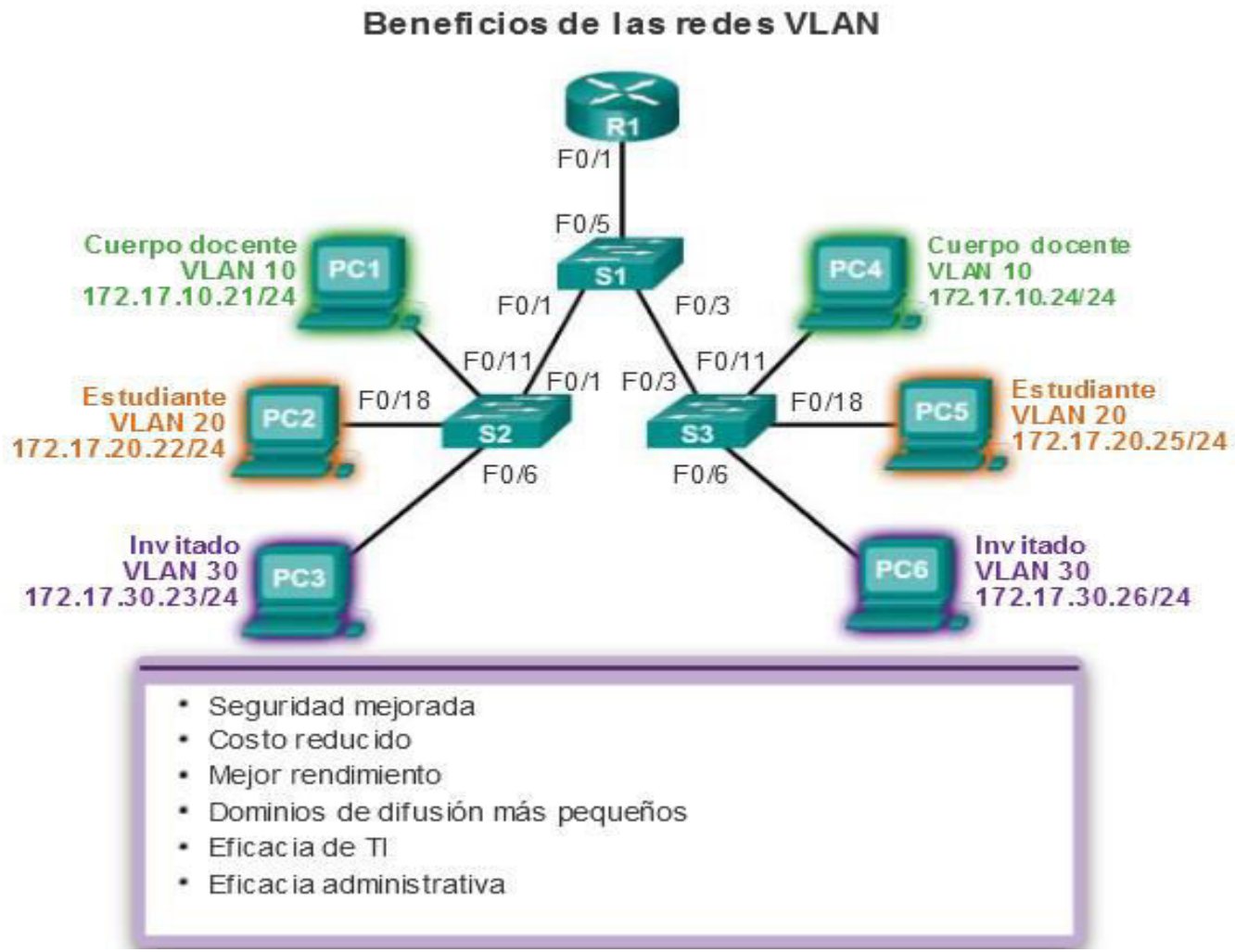
Mejor rendimiento:

La división de las redes planas de capa 2 en varios grupos de trabajo lógicos (dominios de difusión) reduce el tráfico innecesario en la red y mejora el rendimiento.

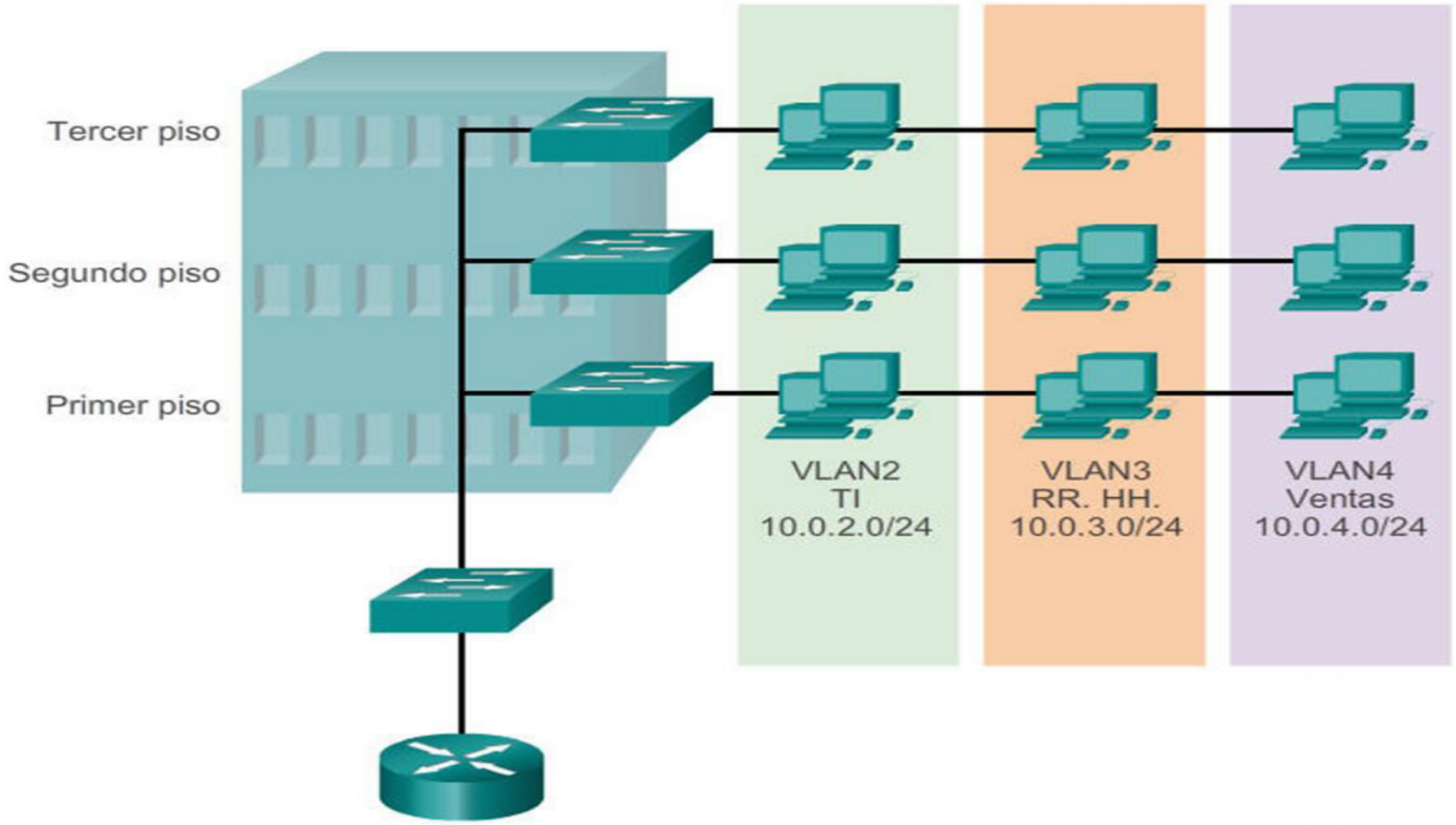
Reducción de dominios de difusión (broadcast):

La división de una red en redes VLAN reduce la cantidad de dispositivos en el dominio de difusión. Como se muestra en la ilustración, existen seis computadoras en esta red, pero hay tres dominios de difusión: Cuerpo docente, Estudiantes e Invitados.

VLAN
Beneficios



VLAN
Beneficios



VLAN
Tipos

Algunos tipos de VLAN se definen según las clases de tráfico. Otros tipos de VLAN se definen según la función específica que cumplen.

VLAN de datos

Una VLAN de datos es una VLAN configurada para transportar tráfico generado por usuarios.

Una VLAN que transporta tráfico de administración o de voz no sería una VLAN de datos.

Es una práctica común separar el tráfico de voz y de administración del tráfico de datos.

A veces a una VLAN de datos se la denomina VLAN de usuario.

Las VLAN de datos se usan para dividir la red en grupos de usuarios o dispositivos.

VLAN predeterminada

Todos los puertos de switch se vuelven parte de la VLAN predeterminada después del arranque inicial de un switch que carga la configuración predeterminada.

Los puertos de switch que participan en la VLAN predeterminada forman parte del mismo dominio de difusión.

Esto admite cualquier dispositivo conectado a cualquier puerto de switch para comunicarse con otros dispositivos en otros puertos de switch.

La VLAN predeterminada para los switches Cisco es la VLAN 1.

En la ilustración, se emitió el comando **show vlan brief** en un switch que ejecuta la configuración predeterminada. Observe que todos los puertos se asignan a la VLAN 1 de manera predeterminada.

La VLAN 1 tiene todas las características de cualquier VLAN, excepto que no se le puede cambiar el nombre ni se puede eliminar. Todo el tráfico de control de capa 2 se asocia a la VLAN 1 de manera predeterminada.

VLAN
Tipos

VLAN 1

```
Switch# show vlan brief

VLAN Name                 Status    Ports
---- -------------------- --------- -------------------------
1    default              active    Fa0/1,  Fa0/2,  Fa0/3,  Fa0/4
                                    Fa0/5,  Fa0/6,  Fa0/7,  Fa0/8
                                    Fa0/9,  Fa0/10, Fa0/11, Fa0/12
                                    Fa0/13, Fa0/14, Fa0/15, Fa0/16
                                    Fa0/17, Fa0/18, Fa0/19, Fa0/20
                                    Fa0/21, Fa0/22, Fa0/23, Fa0/24
                                    Gi0/1,  Gi0/2
1002 fddi-default         act/unsup
1003 token-ring-default   act/unsup
1004 fddinet-default      act/unsup
1005 trnet-default        act/unsup
```

- De manera predeterminada, todos los puertos están asignados a la VLAN 1 para reenviar datos.
- De manera predeterminada, la VLAN nativa es la VLAN 1.
- De manera predeterminada, la VLAN de administración es la VLAN 1.

VLAN nativa

Una VLAN nativa está asignada a un puerto troncal 802.1Q.

Los puertos de enlace troncal son los enlaces entre switches que admiten la transmisión de tráfico asociado a más de una VLAN.

Los puertos de enlace troncal 802.1Q admiten el tráfico proveniente de muchas VLAN (tráfico con etiquetas), así como el tráfico que no proviene de una VLAN (tráfico sin etiquetar).

El tráfico con etiquetas hace referencia al tráfico que tiene una etiqueta de 4 bytes insertada en el encabezado de la trama de Ethernet original, que especifica la VLAN a la que pertenece la trama.

El puerto de enlace troncal 802.1Q coloca el tráfico sin etiquetar en la VLAN nativa, que es la VLAN 1 de manera predeterminada.

Las VLAN nativas se definen en la especificación IEEE 802.1Q a fin de mantener la compatibilidad con el tráfico sin etiquetar de modelos anteriores común a las situaciones de LAN antiguas.

Una VLAN nativa funciona como identificador común en extremos opuestos de un enlace troncal.

Se recomienda configurar la VLAN nativa como VLAN sin utilizar, independiente de la VLAN 1 y de otras VLAN.

De hecho, es común utilizar una VLAN fija para que funcione como VLAN nativa para todos los puertos de enlace troncal en el dominio conmutado.

VLAN
Tipos

VLAN de administración

- Una VLAN de administración es cualquier VLAN que se configura para acceder a las capacidades de administración de un switch.
- La VLAN 1 es la VLAN de administración de manera predeterminada.
- Para crear la VLAN de administración, se asigna una dirección IP y una máscara de subred a la interfaz virtual de switch (SVI) de esa VLAN, lo que permite que el switch se administre mediante HTTP, Telnet, SSH o SNMP.
- Dado que en la configuración de fábrica de un switch Cisco la VLAN 1 se establece como VLAN predeterminada, la VLAN 1 no es una elección adecuada para la VLAN de administración.
- En la ilustración, actualmente todos los puertos están asignados a la VLAN 1 predeterminada. No hay ninguna VLAN nativa asignada explícitamente ni otras VLAN activas; por lo tanto, la VLAN nativa de la red que se diseñó es la VLAN de administración. Esto se considera un riesgo de seguridad.

VLAN
Tipos

VLAN de voz

Se necesita una VLAN separada para admitir la tecnología de voz sobre IP (VoIP).

El tráfico de VoIP requiere:

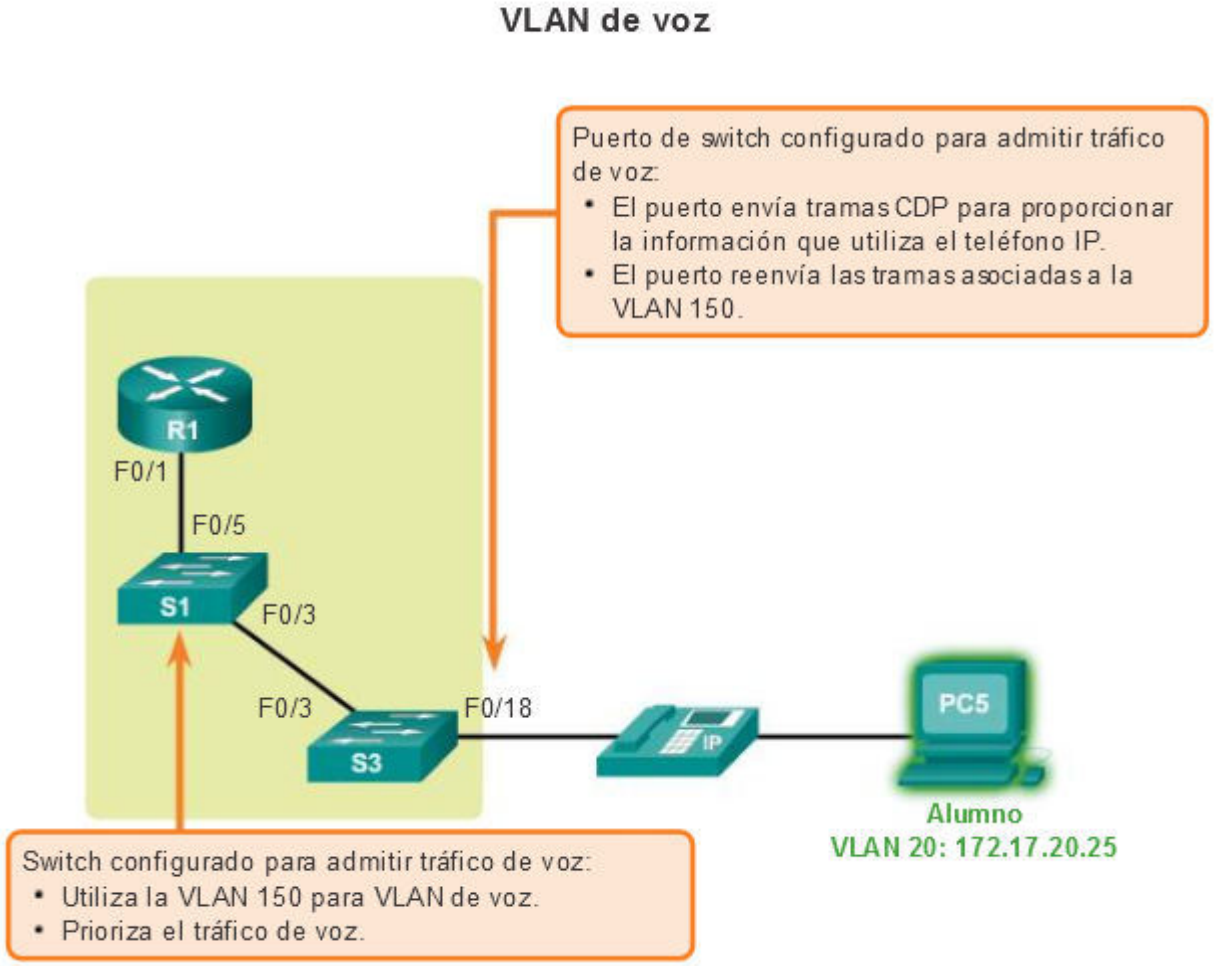
- Ancho de banda garantizado para asegurar la calidad de la voz.
- Prioridad de la transmisión sobre los tipos de tráfico de la red
- Capacidad para ser enrutado en áreas congestionadas de la red
- Una demora inferior a 150 ms a través de la red

Para cumplir estos requerimientos, se debe diseñar la red completa para que admita VoIP.

Los detalles sobre cómo configurar una red para que admita VoIP exceden el ámbito de este curso, pero es útil resumir cómo funciona una VLAN de voz entre un switch, un teléfono IP Cisco y una computadora.

En la figura, la VLAN 150 se diseña para enviar tráfico de voz. La computadora del estudiante PC5 está conectada al teléfono IP de Cisco y el teléfono está conectado al switch S3. La PC5 está en la VLAN 20 que se utiliza para los datos de los estudiantes.

VLAN
Tipos


VLAN de voz
Puerto de switch configurado para admitir tráfico de voz:
• El puerto envía tramas CDP para proporcionar la información que utiliza el teléfono IP.
• El puerto reenvía las tramas asociadas a la VLAN 150.
R1
F0/1
F0/5
S1
F0/3
F0/3
F0/18
S3
IP
PC5
Alumno
VLAN 20: 172.17.20.25
Switch configurado para admitir tráfico de voz:
• Utiliza la VLAN 150 para VLAN de voz.
• Prioriza el tráfico de voz.

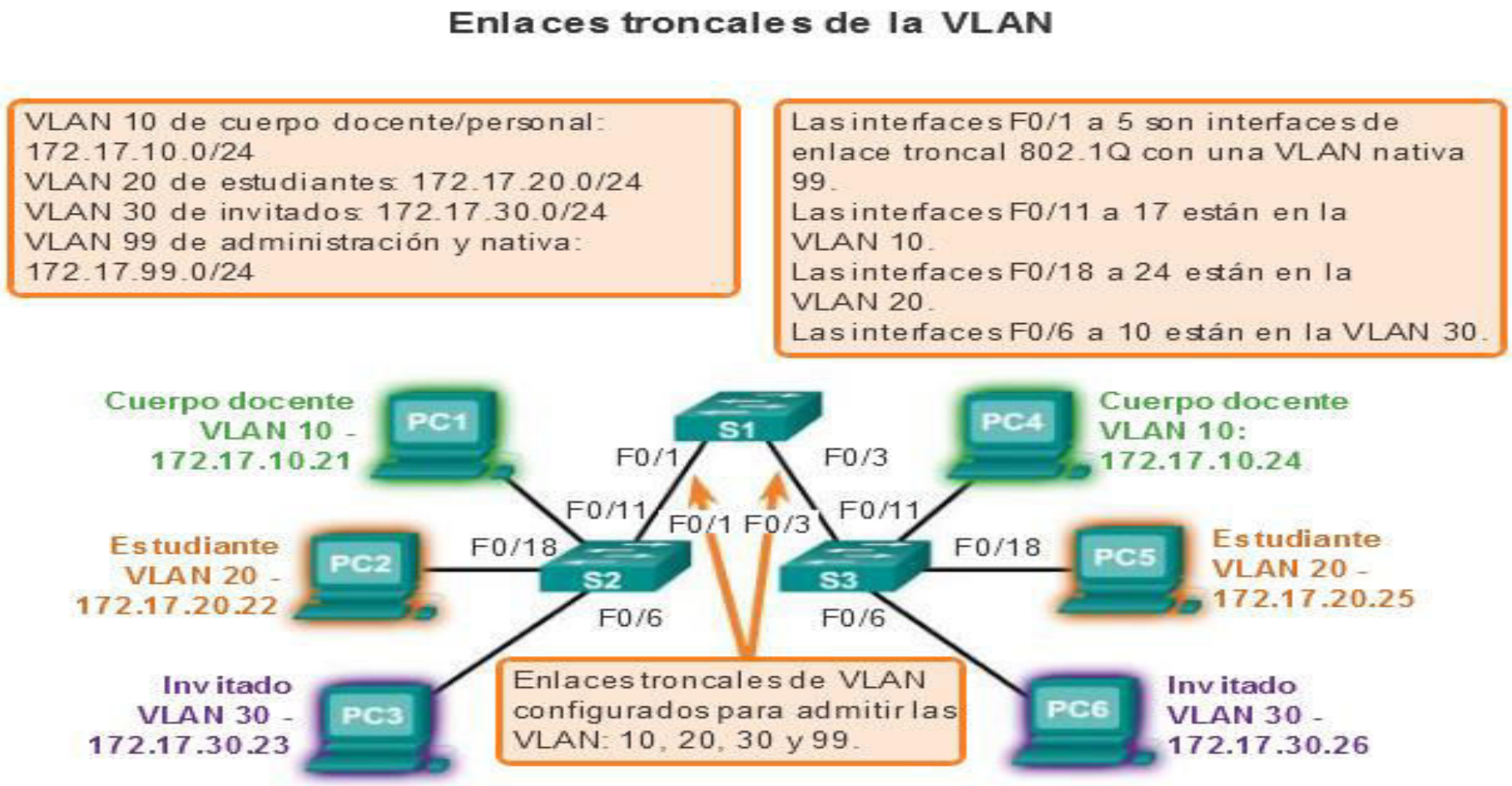
VLAN
Enlaces Troncales (Trunks)

- Un enlace troncal es un enlace punto a punto entre dos dispositivos de red que lleva más de una VLAN.
- Un enlace troncal de VLAN amplía las VLAN a través de toda la red.
- Cisco admite IEEE 802.1Q para coordinar enlaces troncales en las interfaces Fast Ethernet, Gigabit Ethernet y 10-Gigabit Ethernet.
- Las VLAN no serían muy útiles sin los enlaces troncales de VLAN.
- Los enlaces troncales de VLAN permiten que se propague todo el tráfico de VLAN entre los switches, de modo que los dispositivos que están en la misma VLAN pero conectados a distintos switches se puedan comunicar sin la intervención de un router.
- Un enlace troncal de VLAN no pertenece a una VLAN específica, sino que es un conducto para varias VLAN entre switches y routers.
- También se puede utilizar un enlace troncal entre un dispositivo de red y un servidor u otro dispositivo que cuente con una NIC con capacidad 802.1Q.
- En los switches Cisco Catalyst, se admiten todas las VLAN en un puerto de enlace troncal de manera predeterminada.

VLAN
Enlaces Troncales (Trunks)

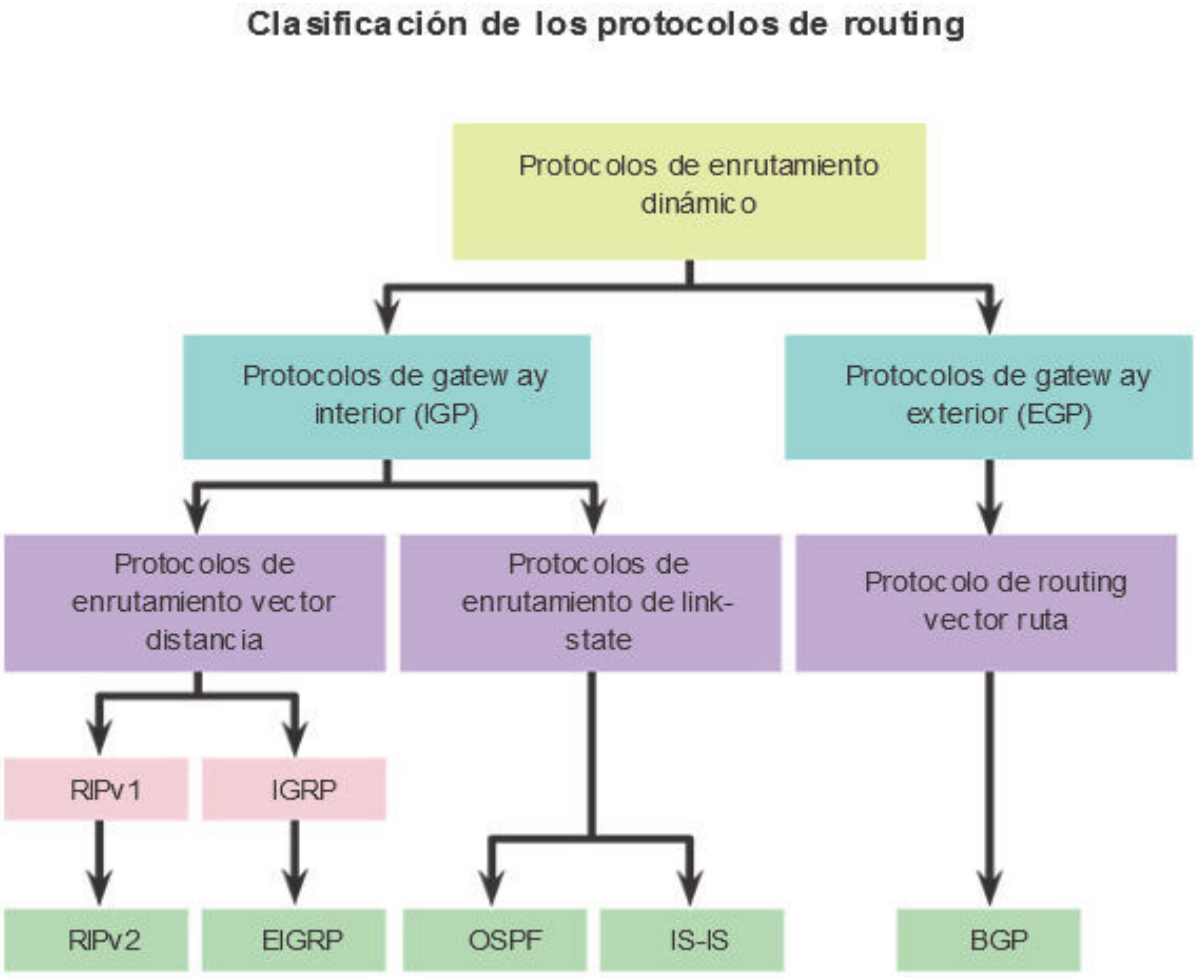
- Un enlace troncal de VLAN **transporta más de una VLAN**.
- Generalmente, se establece entre los switches para que los dispositivos de una misma VLAN se puedan comunicar incluso si están conectados físicamente a switches diferentes.
- Un enlace troncal de VLAN no está relacionado con ninguna VLAN. Tampoco lo están los puertos de enlace troncal que se utilizan para establecer el enlace troncal.
- **IEEE802.1q**, es un protocolo usado de enlace troncal de VLAN.
- En la ilustración, los enlaces entre los switches S1 y S2, y S1 y S3 se configuraron para transmitir el tráfico proveniente de las VLAN 10, 20, 30 y 99 a través de la red.
- Esta red no podría funcionar sin los enlaces troncales de VLAN.

VLAN
Enlaces Troncales



Protocolo de Ruteo

Proceso de enrutamiento
Dinámico Clasificación



Protocolo de ruteo Estático

Proceso de enrutamiento
Estático

Enrutamiento estático

- El enrutamiento es el proceso usado por el router para enviar paquetes a la red de destino.
- Un router toma decisiones en función de la dirección de IP de destino de los paquetes de datos.
- Todos los dispositivos intermedios usan la dirección de IP de destino para guiar el paquete hacia la dirección correcta, de modo que llegue finalmente a su destino.
- A fin de tomar decisiones correctas, los routers deben aprender la ruta hacia las redes remotas.
- Cuando los routers usan enrutamiento dinámico, esta información se obtiene de otros routers.
- Cuando se usa enrutamiento estático, el administrador de la red configura manualmente la información acerca de las redes remotas.

Proceso de enrutamiento
Estático

Enrutamiento estático

- Debido a que las rutas estáticas deben configurarse manualmente, cualquier cambio en la topología de la red requiere que el administrador agregue o elimine las rutas estáticas afectadas por dichos cambios.
- En una red de gran tamaño, el mantenimiento manual de las tablas de enrutamiento puede requerir de una enorme cantidad de tiempo de administración.
- En redes pequeñas, con pocos cambios, las rutas estáticas requieren muy poco mantenimiento.
- Debido a los requisitos de administración adicionales, el enrutamiento estático no tiene la escalabilidad o capacidad de adaptarse al crecimiento del enrutamiento dinámico.
- Aun en redes de gran tamaño, a menudo se configuran rutas estáticas, cuyo objetivo es satisfacer requerimientos específicos, junto con un protocolo de enrutamiento dinámico.

Proceso de enrutamiento
Estático

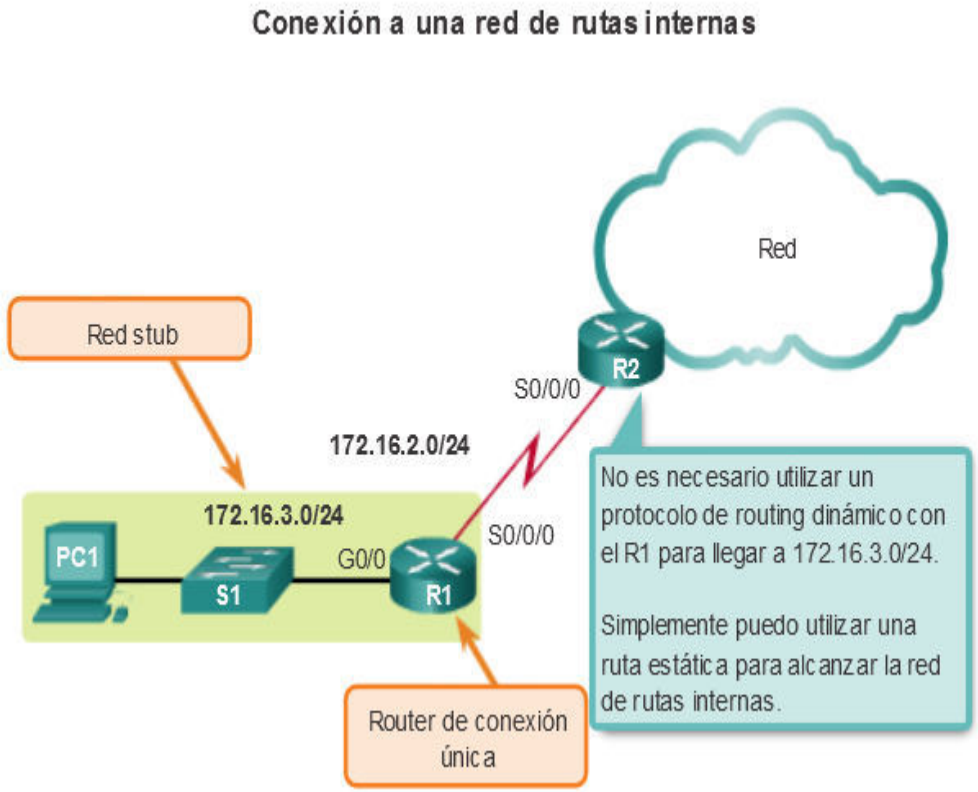
- El administrador de la red **configura manualmente** la información acerca de las redes remotas.
- Cualquier cambio en la topología de la red requiere intervención del administrador.
- La **tabla de ruteo** se genera manualmente.
- Poco recomendable en una red de gran tamaño, el mantenimiento es costoso.
- Se usa en redes pequeñas con pocos cambios.
- **No tiene la escalabilidad o capacidad de adaptarse al crecimiento.**
- Igualmente en redes de gran tamaño, se configuran rutas estáticas, cuyo objetivo es satisfacer requerimientos específicos.

Proceso de enrutamiento
Estático Clasificación

Tipos de rutas

- Ruta estática estándar
- Ruta estática predeterminada
- Ruta estática resumida
- Ruta estática flotante

Proceso de enrutamiento
Estático estándar

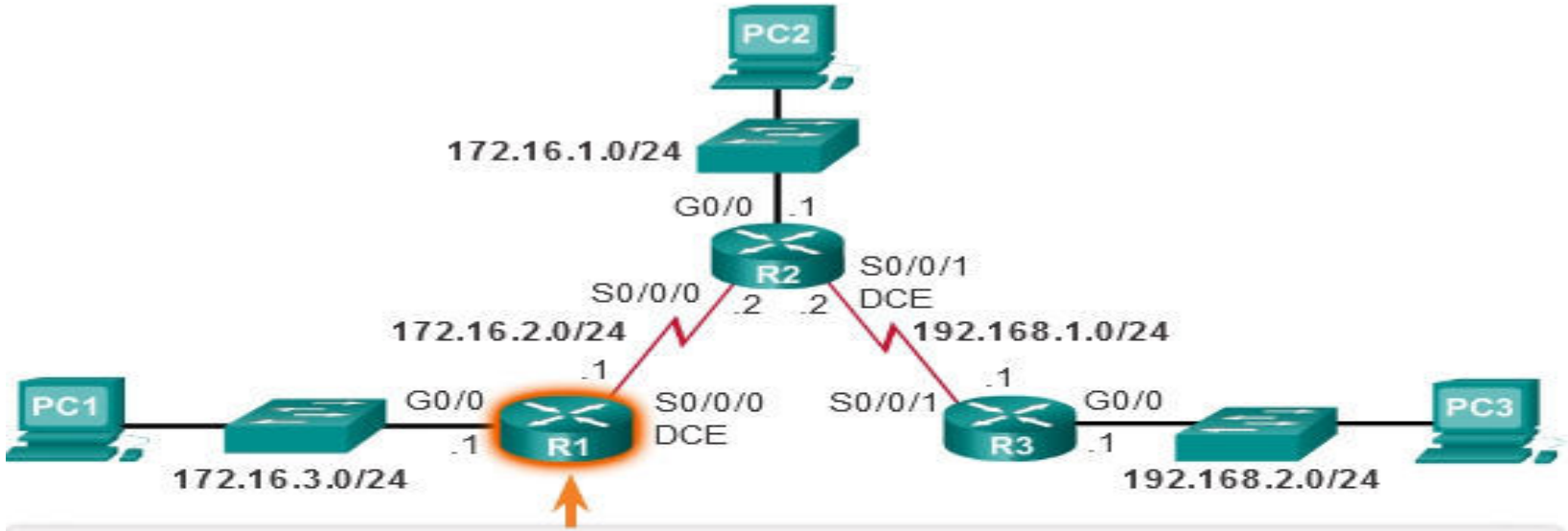


Las rutas estáticas son útiles para conectarse a una red remota específica.

En R2 se puede configurar con una ruta estática para alcanzar la red de rutas internas 172.16.3.0/24.

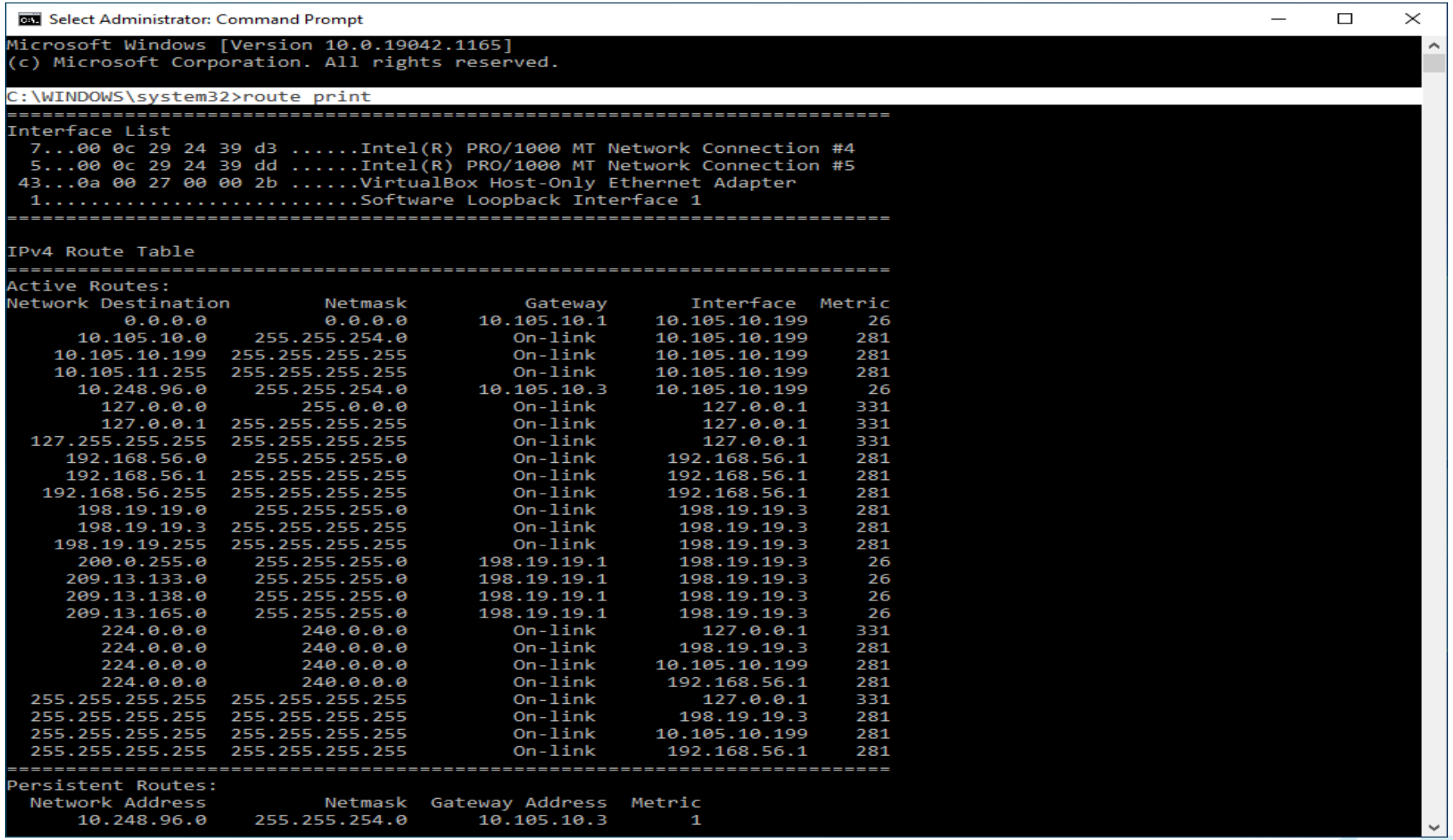
Proceso de enrutamiento
Estático estándar en Cisco

Configuración de rutas estáticas de siguiente salto en el R1

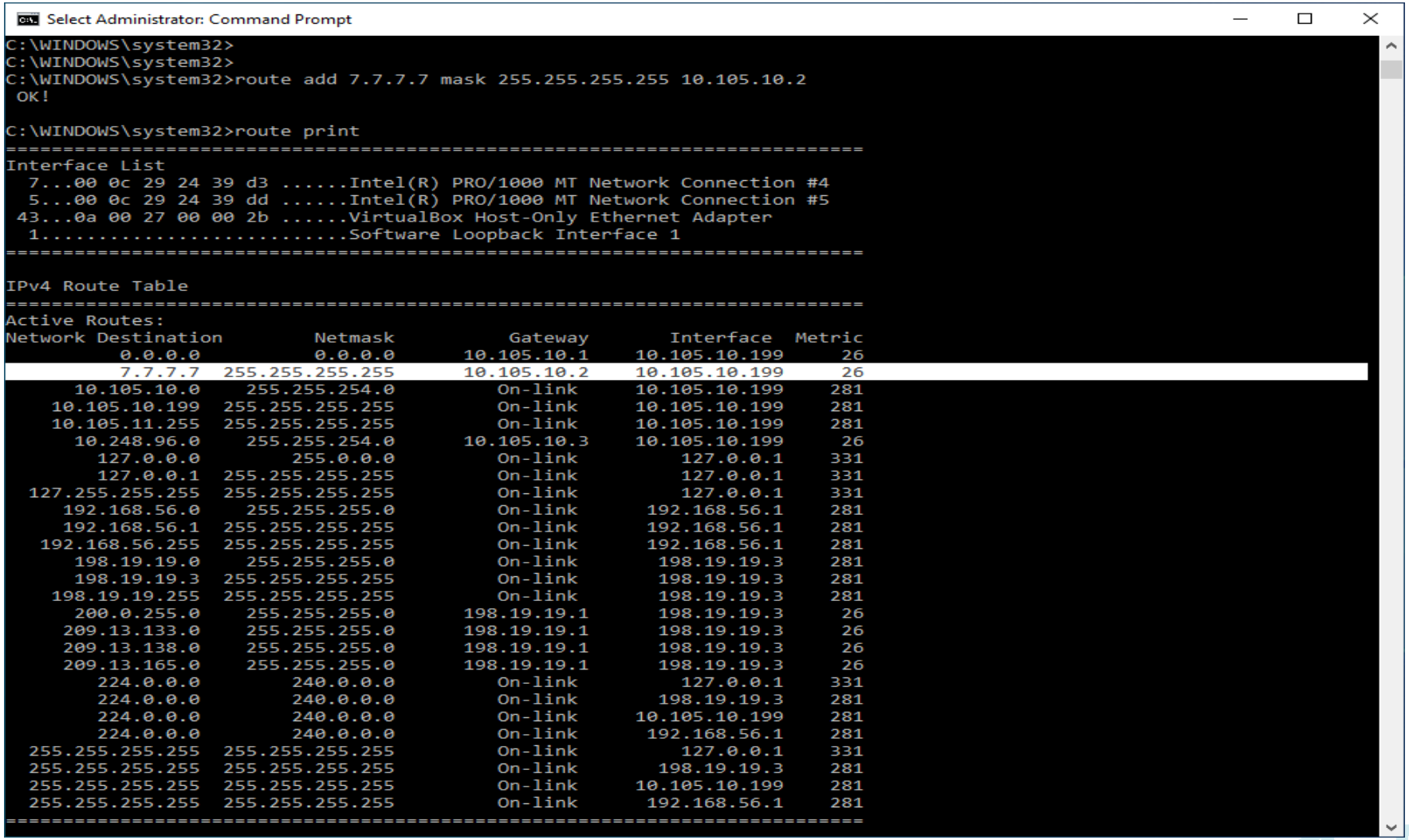



```
R1(config)# ip route 172.16.1.0 255.255.255.0 172.16.2.2
R1(config)# ip route 192.168.1.0 255.255.255.0 172.16.2.2
R1(config)# ip route 192.168.2.0 255.255.255.0 172.16.2.2
R1(config)#
```

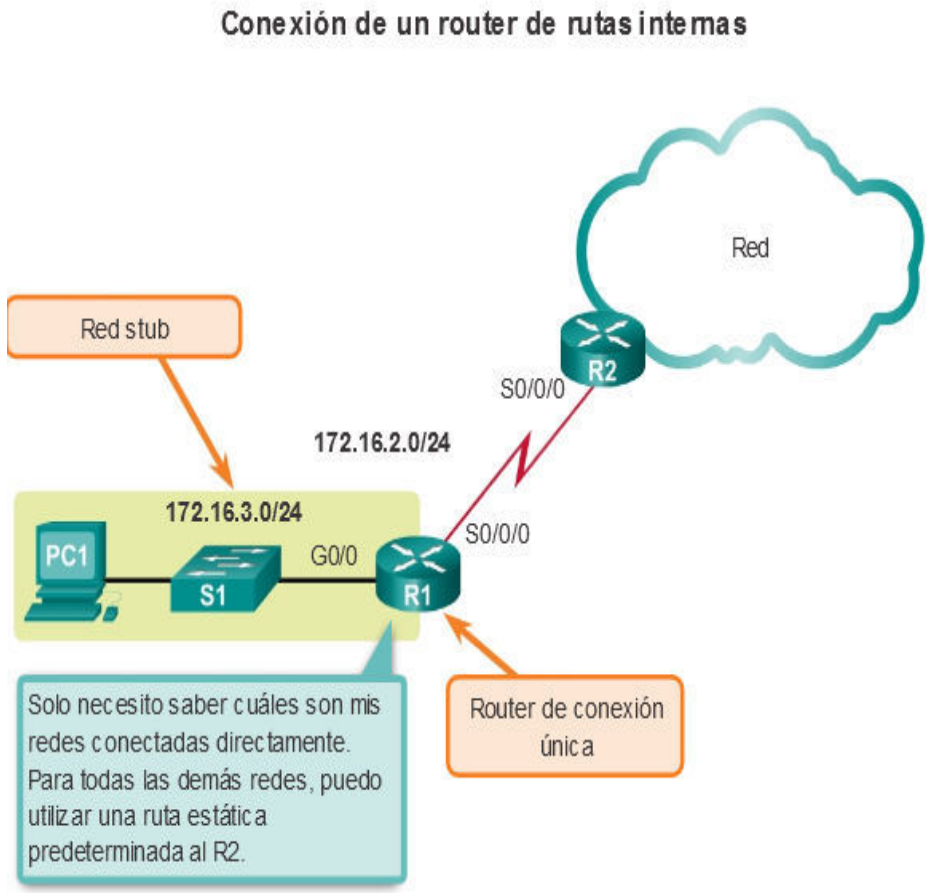
Proceso de enrutamiento
Estático estándar en Windows



Proceso de enrutamiento
Estático estándar en Windows cont.



Proceso de enrutamiento
Estático predeterminada o ruta default



Una ruta estática predeterminada es aquella que coincide con todos los paquetes.

Una ruta predeterminada identifica la dirección IP del gateway al cual el router envía todos los paquetes IP para los que no tiene una ruta descubierta o estática.

Una ruta estática predeterminada es simplemente una ruta estática con 0.0.0.0/0 como dirección IPv4 de destino.

Al configurar una ruta estática predeterminada, se crea un gateway de último recurso.

Proceso de enrutamiento
Estático predeterminada o ruta default

Las rutas estáticas predeterminadas se utilizan en los siguientes casos:

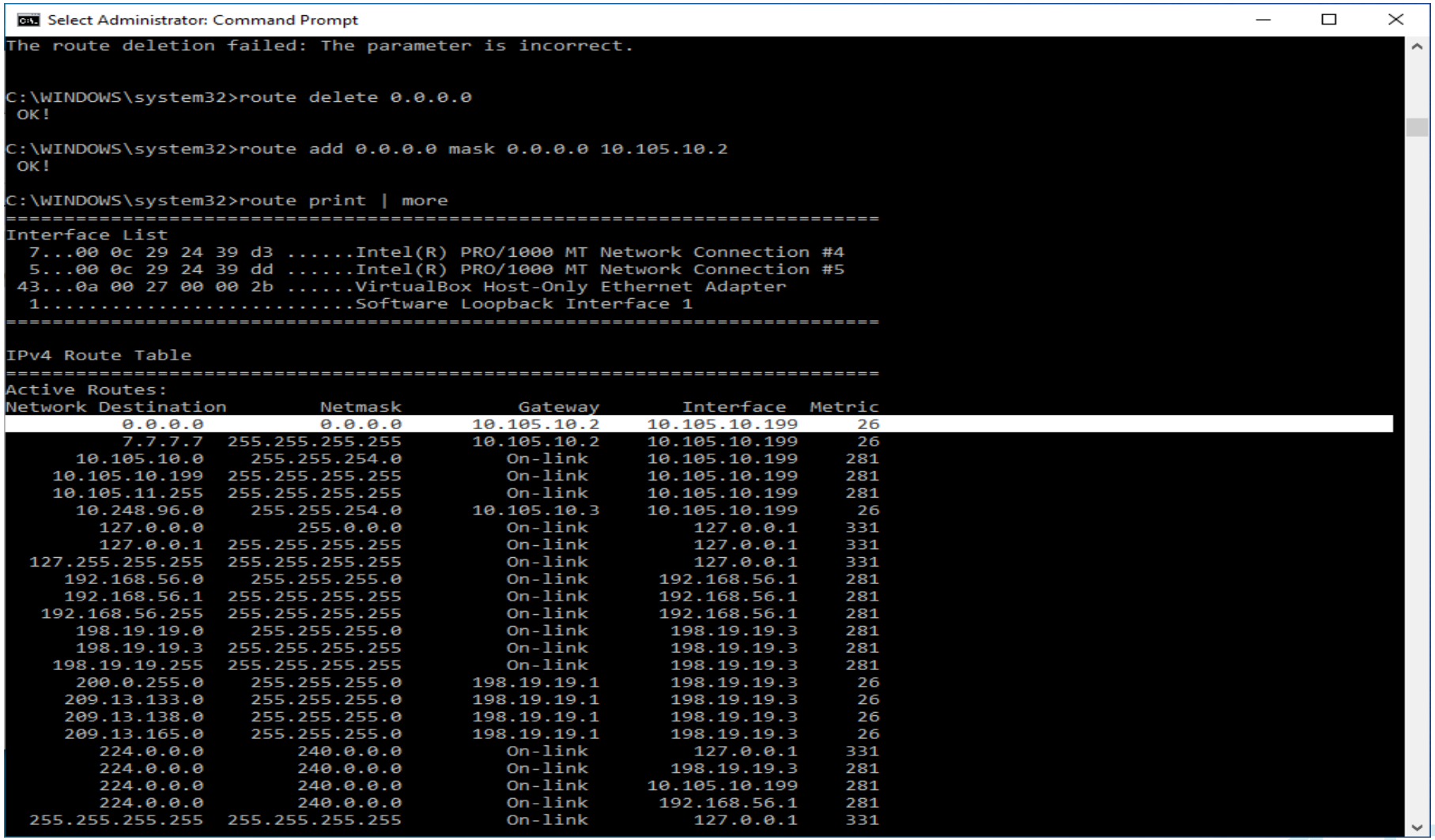
- Cuando ninguna otra ruta de la tabla de routing coincide con la dirección IP destino del paquete.
- En otras palabras, cuando no existe una coincidencia más específica.
- Se utilizan comúnmente cuando se conecta un router periférico de una compañía a la red ISP.
- Cuando un router tiene otro router único al que está conectado. Esta condición se conoce como router de conexión única.

En general, las rutas estáticas predeterminadas se utilizan al conectar:

- Un router perimetral a la red de un proveedor de servicios
- Un router de rutas internas (aquel con solo un router vecino ascendente)

Todas las rutas que identifican un destino específico con una máscara de subred más grande tienen prioridad sobre la ruta predeterminada.

Proceso de enrutamiento
Estático default en Windows



Proceso de enrutamiento
Resúmen

Ventajas y desventajas del enrutamiento estático

Ventajas	Desventajas
Fácil de implementar en una red pequeña.	Adecuado solamente para topologías simples o para fines específicos, como una ruta estática predeterminada. La complejidad de la configuración aumenta notablemente a medida que crece la red.
Muy seguro. No se envían anuncios, a diferencia del caso de los protocolos de routing dinámico.	La complejidad de la configuración aumenta significativamente cuando el tamaño de la red es mayor.
La ruta hacia el destino siempre es la misma.	Se requiere intervención manual para volver a enrutar el tráfico.
Dado que no se requieren algoritmos de routing ni mecanismos de actualización, no se necesitan recursos adicionales (CPU o RAM).	

Protocolo Dinámico

Proceso de enrutamiento Dinámico

- Los protocolos de enrutamiento se usan para facilitar el intercambio de información de enrutamiento entre los routers.

- Un protocolo de enrutamiento es un conjunto de procesos, algoritmos y mensajes que se usan para intercambiar información de enrutamiento y completar la tabla de enrutamiento con la elección de los mejores caminos que realiza el protocolo.

Proceso de enrutamiento Dinámico cont.

El propósito de los protocolos de routing dinámico incluye lo siguiente:

- Descubrir redes remotas.
- Mantener la información de enrutamiento actualizada.
- Escoger el mejor camino hacia las redes de destino.
- Poder encontrar un mejor camino nuevo si la ruta actual deja de estar disponible.

Proceso de Ruteo Dinámico

Clasificación

Proceso de enrutamiento
Dinámico Clasificación

Los protocolos de routing IPv4 se clasifican de la siguiente manera:

- **RIPv1 (antiguo):** IGP, vector distancia, protocolo con clase(classful)
- **IGRP (antiguo):** IGP, vector distancia, protocolo con clase(classful) desarrollado por Cisco (cayó en desuso a partir del IOS 12.2)
- **RIPv2:** IGP, vector distancia, protocolo sin clase(classless)
- **EIGRP:** IGP, vector distancia, protocolo sin clase desarrollado por Cisco
- **OSPF:** IGP, estado de enlace, protocolo sin clase
- **IS-IS:** IGP, estado de enlace, protocolo sin clase
- **BGP:** EGP, vector ruta, protocolo sin clase

Proceso de enrutamiento
Dinámico Clasificación

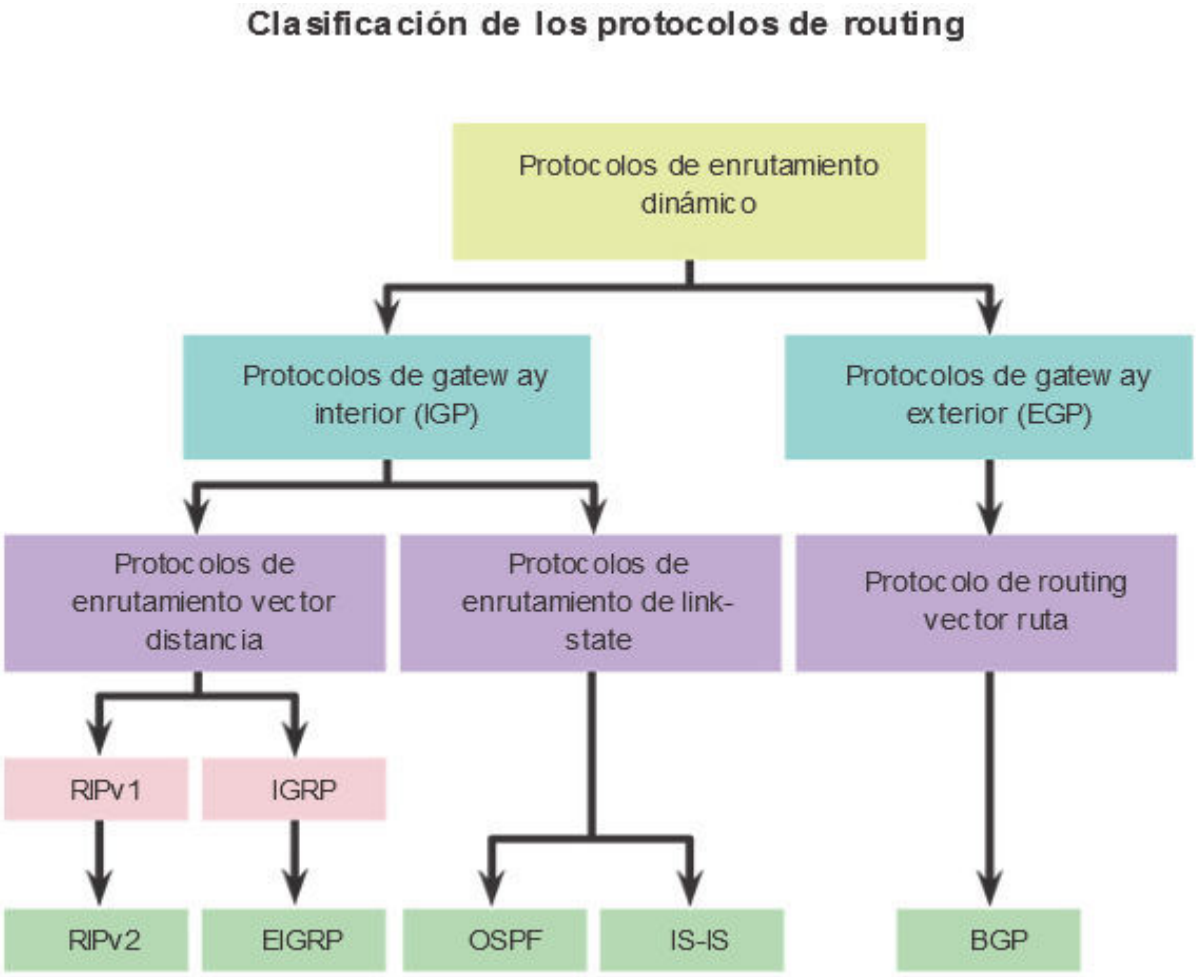
- Los protocolos de routing con clase, RIPv1 e IGRP, son protocolos antiguos y se utilizan solamente en redes antiguas.
- Estos protocolos de routing se convirtieron en los protocolos de routing sin clase RIPv2 y EIGRP, respectivamente.
- Los protocolos de routing de estado de enlace(link-state) son protocolos sin clase(classless) naturalmente.

Proceso de enrutamiento
Dinámico Clasificación

Los protocolos de enrutamiento se pueden clasificar en diferentes grupos según sus características.

- **Propósito:** protocolo de gateway interior (IGP) **I**nterior **G**ateway **P**rotocol o protocolo de gateway exterior (EGP) **E**xterior **G**ateway **P**rotocol.
- **Operación o funcionamiento:** vector distancia(distance vector), protocolo de estado de enlace(link state), protocolo vector ruta
- **Comportamiento:** protocolo con clase (antiguo) **classful** o protocolo sin clase **classless**

Proceso de enrutamiento
Dinámico Clasificación



Seguridad en Informática - Módulo 2

Docente: Carlos Cagnani

*Este documento fue realizado en concepto de capacitación en Formación Profesional y dictada para el **Sindicato CePETel** a contar del mes de mayo del año 2023.*

Conceptos Introductorios sobre Seguridad de la Información

Índice

Dato

Se refiere a hechos, eventos, transacciones, etc., que han sido registrados.

Es la entrada sin procesar de la cual se produce la información.

Los datos son la materia prima de la cual se deriva la información.

Cualquier cantidad o hecho, sin analizar, que por sí solos no tienen significado alguno y deben ser presentados en forma utilizable y colocados en un contexto que le de valor.

Ejemplos: Edad, número de artículos vendidos, sueldo, etc.

Información

Se refiere a los datos que han sido procesados y comunicados de tal manera que pueden ser entendidos e interpretados por el receptor.

En sentido general, la información es un conjunto organizado de datos, que constituyen un mensaje sobre un determinado ente o fenómeno.

Si por ejemplo organizamos datos sobre un país (número de habitantes, densidad de población, nombre del presidente, etc.) y se usa para escribir, por ejemplo, el capítulo de un libro, podemos decir que ese capítulo constituye información sobre ese país.

¿Qué representa la Información?

Información - Amenazas

AMENAZAS

Naturales

- Incendios
- Inundaciones
- Terremotos
- Huracanes

Intencionales

- Ciberdelincuentes / Vandalismo / Criminales
- Empleados Descontentos
- Competencia Desleal
- Incumplimiento Legal, Regulatorio, Contractual
- 30 millones de Adolescentes con Tiempo

Error Humano

- Falta de Planificación en Almacenam.
- Pérdida / Caducidad de Contraseñas
- Extravío de Claves Criptográficas
- Borrado Accidental de Datos
- Backups Incorrectos / Inexistentes
- Ausencia de Plan de Continuidad
- Formación insuficiente

Seguridad

Definición:

La *seguridad* puede considerarse como un estado de ausencia de peligros y de condiciones que puedan provocar daño físico, psicológico o material en los individuos y en la sociedad en general.

Deriva de seguro, que la RAE (https://dle.rae.es/seguro) define como “Libre y exento de riesgo”.

Seguridad Concepto

- La información es la columna vertebral de las empresas.
- Un incidente de seguridad puede afectar seriamente a la imagen y al negocio de la Organización.
- La seguridad pasa a ser la "necesidad primaria" que permite mantener con vida la información.

¿Dónde estamos?

¿Qué hacemos?

¿Quién y por qué?

¿Vamos bien?

Información - clasificación según estructura

- **Significado (semántica):** ¿Qué quiere decir? ¿Qué expresa?

  -> Integridad
- **Importancia (para el receptor):** ¿Cuán importante es para el receptor?

  -> Valoración
- **Vigencia (en la dimensión espacio-tiempo):** ¿Es actual o desfasada?

  -> Disponibilidad
- **Validez (relativa al emisor):** ¿El emisor es fiable o puede proporcionar información no válida (falsa)?

  -> Autenticidad
- **Valor (activo intangible volátil):** ¿Cómo de útil resulta para el destinatario?

  -> Valoración
- **Polimorfismo:** ¿En qué forma (o formato) se presenta la información?

  -> Soporte

¿Qué es la seguridad de la Información?

- Se refiere al resguardo y/o protección de información como un todo, indepentientemente del formato, soporte o resguardo de almacenamiento en que se presente.
- Es para evitar el acceso no autorizado, divulgación, alteración, destrucción o interrupción.
- Garantizar confidencialidad, integridad y disponibilidad

¿Qué es la seguridad de la Información?

- Seguridad de Información y Seguridad informática son usados con frecuencia, aunque su significado no es el mismo. Estas diferencias radican principalmente en el enfoque.
- Tiene como fin la protección de la información y de los sistemas de la información del acceso, uso, divulgación, interrupción o destrucción no autorizada.
- Involucra la implementación de estrategias que cubran los procesos en donde la información es el activo primordial. Estas estrategias se enfocan en el establecimiento de políticas, procedimientos, planes, controles, tecnologías y recursos (técnicos y humanos).
- Es un proceso de mejora continua por lo que las políticas y controles establecidos deberán revisarse y adecuarse, ante los nuevos riesgos que surjan, a fin de reducirlos y eliminarlos.

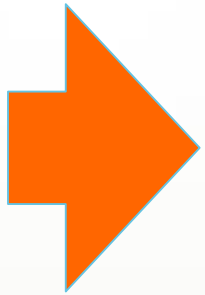
¿Qué es la seguridad Informática?

- La **seguridad informática** es la disciplina que se ocupa de diseñar las *normas, procedimientos, métodos y técnicas* destinados a proteger un sistema informático, los datos almacenados en ellos y la infraestructura de tecnología de información, contra amenazas, ataques y accesos no autorizados.

Modelo de Seguridad

Seguridad Informática

- **Asegurar** los **recursos** IT.
- Meta, o **fin a alcanzar**.
- Los **controles** se aplican **sobre los recursos IT**.
- Esquema **basado en restricciones y permisos**.
- **Responsabilidad** asignada a un **grupo de empleados**.
- Alcance de los Controles: ***Implementación***.



Seguridad de la Información

- **Asegurar** el **Negocio**.
- **Gestión Continua**.
- Los **controles** alcanzan **recursos, personas, procesos**.
- Esquema abierto, basado **accesos controlados**.
- **Responsabilidad compartida** por toda la organización.
- Alcance de los Controles: **Definición y Auditoría**.

Ciberseguridad

Es la rama de la informática que procura detectar vulnerabilidades que ponen en juego la integridad, disponibilidad y confidencialidad de los sistemas informáticos.

15

Ciberseguridad

La ciberseguridad tiene como objetivo principal resguardar la infraestructura y la información de los usuarios involucrados en ella.

Se constituye como una esfera con distintos protagonistas: empresas que ofrecen servicios asociados, expertos y analistas que investigan nuevas soluciones, desarrolladores de nuevas herramientas (tanto a nivel hardware como software), y aquellos usuarios que utilizan diferentes medios preventivos.

Es en este circuito que también actúan aquellos personajes que quieren interferir en estos sistemas, ya sea con fines delictivos, políticos o por el hecho de demostrar sus habilidades.

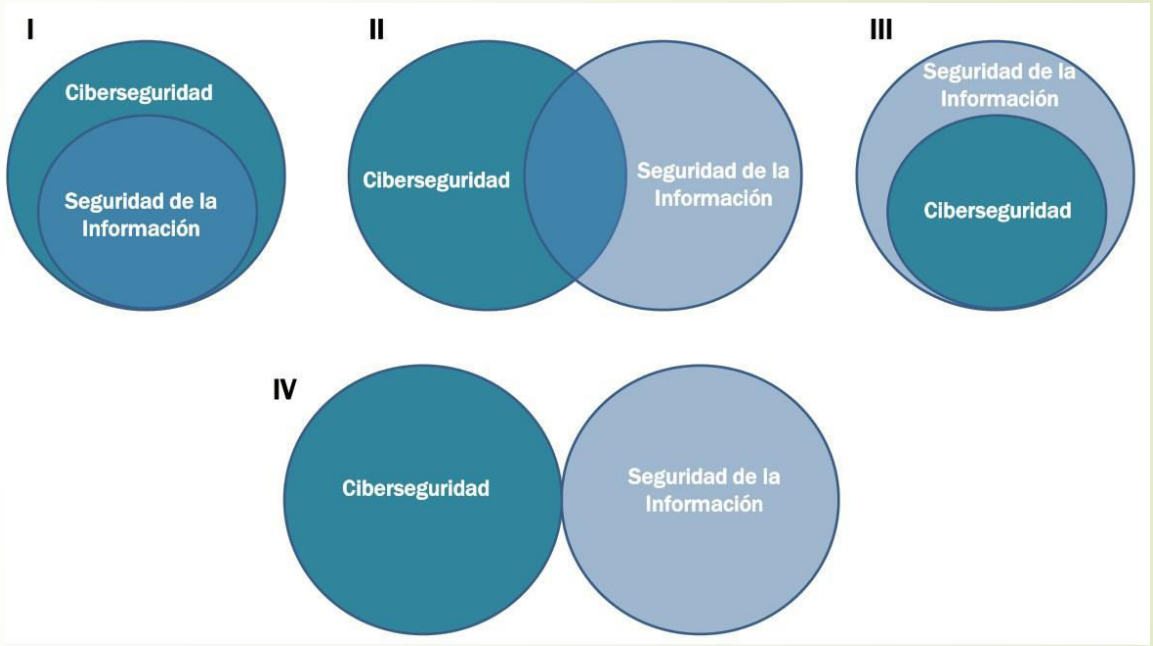
Estos últimos, son conocidos coloquialmente como **hackers**, aunque esta denominación es muy discutida ya que en realidad no refiere a cuestiones ilícitas, sino que se vincula con la manera de denominar aquellos expertos que detectan fallos y vulnerabilidades en los sistemas.

6

- **Seguridad de la Información**

Y

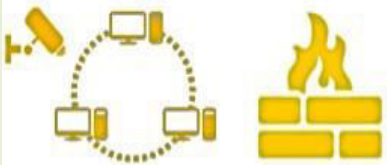
- **Ciberseguridad**



Seguridad de la Información, Seguridad Informática y Ciberseguridad

¿Seguridad Informática?

Se enfoca en proteger los riesgos y las amenazas que afectan los sistemas operativos, las bases de datos, los sistemas de información, las redes de datos (internas y externas) y los equipos de telecomunicación.



¿Seguridad de la Información?

Concepto generado a partir de normas o estándares de seguridad tales como BS7799, ISO1799, ISO27001.
Introduce el concepto de activo de información.
Todo aquello que tiene valor para la empresa.

- Formato electrónico.
- Forma verbal.
- Mensajes escritos.
- Impresos.

¿Ciberseguridad?

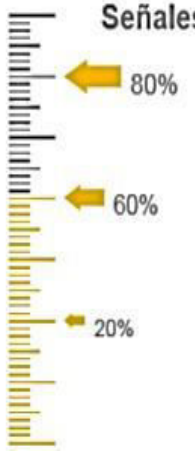
Concepto mucho más amplio (cibernético).

- Incluye la protección de datos, inteligencia de las amenazas, la seguridad física, entre otras cosas.
- Incluye prácticas ofensivas para atacar a los adversarios.
- No es un problema de TI es un problema de negocio.
- La compañía debe definir que información es relevante para su negocio (p.ej. Fórmula de la Coco Cola - Data).
- No es sólo formula, es la gestión de manufactura, distribución (Supply), precio, materia prima (azúcar). Hay que pensar en negocio y no sólo la tecnología (Firewalls)

¿Se pueden prevenir los ciberataques?

- No se pueden prevenir, por mas esfuerzos que realices.
- Según las investigaciones, las compañías se demoran en promedio 298 días en descubrir los ataques. El objetivo es reducirlos.
- No se pueden desconectar los equipos, porque eso haría que se pierdan los logs y afectarías mas a tu negocio.
- Hay que aprender en focalizar los esfuerzos. (p.ej. Talvez la página web no lo sea, pero si la base de datos.).
- Combinación de políticas, procedimientos, educación, riesgos, tecnología (Process, Procedures, Strategy, Persons).
- Hay que aprender a saber responder a estos ataques.

Señales que reflejan que existen GAPs en Seguridad de Inf.



- Perdida de datos (data loss)
- Cyberattacks
- Fusiones y adquisiciones. Integración de los sistemas de información.
- Diferencias en los presupuestos de TI (Crosselling TAS y Advisory)
- Cumplimiento de nuevas leyes y regulaciones.
- Cambios en la Gerencias principales (CIO, CISO).
- Cambios es la estrategia que le está brindando el negocio a la seguridad de información.
- Fraude y corrupción. Identificación de actividades defraude en la organización ((Crosselling FIDS y Advisory)

Impacto de un Ciberataque

Sobre la **IMAGEN**	• **Pérdida de prestigio** de la marca, • **Pérdida de confianza de su entorno**,
Sobre el **NEGOCIO**	• **Afección de la disponibilidad de los servicios** en condiciones normales, • **Pérdida de datos** de las operaciones en curso, • **Fuga de clientes**,
Sobre el **CUMPLIMIENTO**	• **Sanciones por incumplimiento de normativas** de privacidad, Ley protección de datos, GDPR, • **Incumplimiento de contratos** con clientes y/o proveedores, • **Posibles juicios por daños a terceros**,
Sobre los **ACTIVOS**	• **Depreciación de los activos** de la empresa, • **Pérdida de confianza de proveedores / financiadores**, • **Dificultad para entrar en mercados**,

Seguridad de la Información

General

¿Porqué es necesaria la Seguridad de la Información?

La mayoría de los sistemas han sido desarrollados de forma insegura,

La seguridad que puede lograrse es limitada y debe respaldarse con una gestión adecuada,

La administración de la seguridad requiere de la participación de todos (empleados, proveedores, clientes, afiliados y accionistas),

La seguridad resulta más económica y eficaz si se incorpora al inicio de cada nuevo proyecto.

¿Qué abarca la seguridad de la

Requerimientos de seguridad de la Información

- **Análisis de Riesgo**
- A la hora de dotar de seguridad a un sistema de información, hay que tener en cuenta todos los elementos que lo componen, analizar el nivel de vulnerabilidad de cada uno de ellos ante determinadas amenazas y valorar el impacto que un ataque causaría sobre todo el sistema.
- La persona o el equipo encargado de la seguridad deberá analizar con esmero cada uno de los elementos.
- A veces el descuido de un elemento considerado débil ha producido importantes fallos de seguridad.
- Al estar interrelacionados todos los elementos este descuido puede producir errores en cadena con efectos insospechados sobre la organización.

Elementos de análisis de riesgo

- Para comenzar a analizar un sistema de información al que se pretende dotar de unas medidas de seguridad, hay que tener en cuenta los siguientes elementos:

  - Activos
  - Amenazas
  - Riesgos
  - Vulnerabilidades
  - Ataques
  - Impactos.

Activos

- Son los recursos que pertenecen al propio sistema de información o que están relacionados con este.
- La presencia de los activos facilita el funcionamiento de la empresa u organización y la consecución de sus objetivos.
- Al hacer un estudio de los activos existentes hay que tener en cuenta la relación que guardan entre ellos y la influencia que se ejercen: cómo afectaría en uno de ellos un daño ocurrido a otro.

Activos Clasificación

Datos.

- Constituyen el núcleo de toda organización, hasta tal punto que se tiende a considerar que el resto de los activos están al servicio de la protección de los datos.
- Normalmente están organizados en bases de datos y almacenados en soportes de diferente tipo.
- El funcionamiento de una empresa u organización depende de sus datos, que pueden ser de todo tipo: económicos, fiscales, de recursos humanos, clientes o proveedores…
- Cada tipo de dato merece un estudio independiente de riesgo por la repercusión que su deterioro o pérdida pueda causar, como por ejemplo los relativos a la intimidad y honor de las personas u otros de índole confidencial.

Activos Clasificación

- **Software.**

Constituido por los sistemas operativos y el conjunto de aplicaciones instaladas en los equipos de un sistema de información que reciben y gestionan o transforman los datos para darles el fin que se tenga establecido.

- **Hardware.**

Se trata de los equipos (servidores y terminales) que contienen las aplicaciones y permiten su funcionamiento, a la vez que almacenan los datos del sistema de información. Incluimos en este grupo los periféricos y elementos accesorios que sirven para asegurar el correcto funcionamiento de los equipos o servir de vía de transmisión de los datos (módem, router, instalación eléctrica o sistemas de alimentación ininterrumpida, destructores de soportes informáticos…).

Activos Clasificación

- **Redes.**

Desde las redes locales de la propia organización hasta las metropolitanas o internet. Representan la vía de comunicación y transmisión de datos a distancia.

- **Soportes.**

Los lugares en donde la información queda registrada y almacenada durante largos períodos o de forma permanente (DVD, CD, tarjetas de memoria, discos duros externos dedicados al almacenamiento, microfilms e incluso papel).

- **Instalaciones.**

Son los lugares que albergan los sistemas de información y de comunicaciones. Normalmente se trata de oficinas, despachos, locales o edificios, pero también pueden ser vehículos y otros medios de desplazamiento.

Activos Clasificación

- **Personal.**

El conjunto de personas que interactúan con el sistema de información:

administradores, programadores, usuarios internos y externos y resto de personal de la empresa. Los estudios calculan que se producen más fallos de seguridad por intervención del factor humano que por fallos en la tecnología.

- **Servicios.**

que se ofrecen a clientes o usuarios: productos, servicios, sitios web,foros, correo electrónico y otros servicios de comunicaciones, información, seguridad,etc.

Amenazas

- En sistemas de información se entiende por amenaza la presencia de uno o más factores de diversa índole (personas, máquinas o sucesos) que –de tener la oportunidad– atacarían al sistema produciéndole daños aprovechándose de su nivel de vulnerabilidad.
- Hay diferentes tipos de amenazas de las que hay que proteger al sistema, desde las físicas como cortes eléctricos, fallos del hardware o riesgos ambientales hasta los errores intencionados o no de los usuarios, la entrada de software malicioso (virus, troyanos, gusanos) o el robo, destrucción o modificación de la información.

Amenazas

En función del tipo de alteración, daño o intervención que **podrían producir sobre la información,** las amenazas se clasifican en cuatro grupos:

De interrupción. El objetivo de la amenaza es deshabilitar el acceso a la información;

por ejemplo, destruyendo componentes físicos como el disco duro, bloqueando el acceso a los datos, o cortando o saturando los canales de comunicación.

De interceptación. Personas, programas o equipos no autorizados podrían acceder a un determinado recurso del sistema y captar información confidencial de la organización, como pueden ser datos, programas o identidad de personas.

De modificación. Personas, programas o equipos no autorizados no solamente accederían a los programas y datos de un sistema de información sino que además los modificarían. Por ejemplo, modificar la respuesta enviada a un usuario conectado o alterar el comportamiento de una aplicación instalada.

De fabricación. Agregarían información falsa en el conjunto de información del sistema.

Amenazas

Según su **origen** las amenazas se clasifican en:

- **Accidentales.** Accidentes meteorológicos, incendios, inundaciones, fallos en los equipos, en las redes, en los sistemas operativos o en el software, errores humanos.
- **Intencionadas.** Son debidas siempre a la acción humana, como la introducción de software malicioso –malware– (aunque este penetre en el sistema por algún procedimiento automático, su origen es siempre humano), intrusión informática (con frecuencia se produce previa la introducción de malware en los equipos), robos o hurtos. Las amenazas intencionadas pueden tener su origen en el exterior de la organización o incluso en el personal de la misma.

Riesgos

Se denomina riesgo a la posibilidad de que se materialice o no una **amenaza** aprovechando una **vulnerabilidad.** No constituye riesgo una amenaza cuando no hay vulnerabilidad ni una vulnerabilidad cuando no existe amenaza para la misma.

Ante un determinado riesgo, una organización puede optar por tres alternativas distintas:

Asumirlo sin hacer nada. Esto solamente resulta lógico cuando el perjuicio esperado no tiene valor alguno o cuando el coste de aplicación de medidas superaría al de la reparación del daño.

Aplicar medidas para disminuirlo o anularlo.

Transferirlo (por ejemplo, contratando un seguro).

Vulnerabilidades

Probabilidades que existen de que una amenaza se materialice contra un activo.

No todos los activos son vulnerables a las mismas amenazas.

Por ejemplo, los datos son vulnerables a la acción de los *hackers,* mientras que una instalación eléctrica es vulnerable a un cortocircuito.

Al hacer el análisis de riesgos hay que tener en cuenta la vulnerabilidad de cada activo.

Ataques

Se dice que se ha producido un ataque **accidental** o **deliberado** contra el sistema cuando se ha materializado una amenaza.

En función del impacto causado a los activos atacados, los ataques se clasifican en:

Activos. Si modifican, dañan, suprimen o agregan información, o bien bloquean o saturan los canales de comunicación.

Pasivos. Solamente acceden sin autorización a los datos contenidos en el sistema. Son los más difíciles de detectar.

Un ataque puede ser **directo** o **indirecto**, si se produce desde el atacante al elemento «víctima» directamente, o a través de recursos o personas intermediarias.

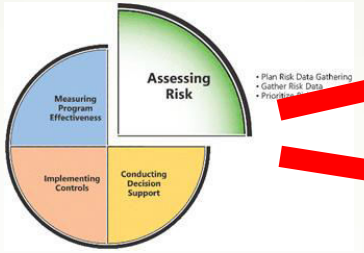
Impactos

Son la consecuencia de la materialización de una o más amenazas sobre uno o varios activos aprovechando la vulnerabilidad del sistema o, dicho de otra manera, el daño causado.

Los impactos pueden ser **cuantitativos**, si los perjuicios pueden cuantificarse económicamente, o **cualitativos,** si suponen daños no cuantificables, como los causados contra los derechos fundamentales de las personas.

¿Cómo establecer los requerimientos de seguridad?

1. Estimación del Riesgo



a. Asumir el riesgo

b. Tratar el riesgo

2. Cumplimiento de requisitos o controles propios de la Organización

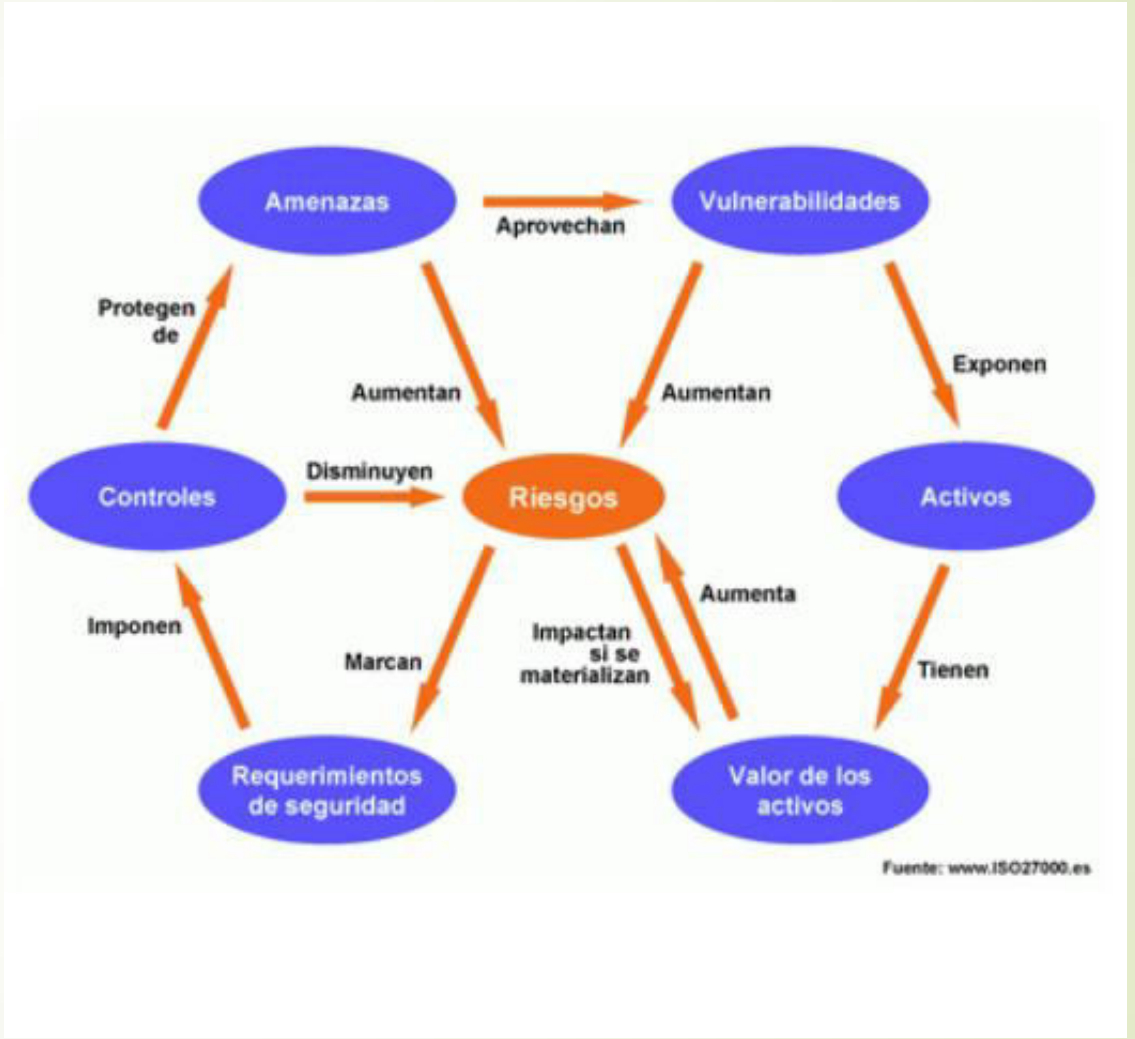
Requisitos en nuevos proyectos:

- *Arquitectura*
  - *Arquitectura de red*
  - *Tráficos*
  - *Interfaces*
  - *Separación de Entornos*
- *Política de seguridad de clientes*
- *Requisitos legales – Ley datos personales*
  - *Derechos de los afectados*
  - *Obtención/ comunicación de datos a terceros*
  - *Declaración de los Datos a la DNPDP*
- *Aspectos legales propios del sector de la org.*
- *Contingencia*
- *Seguridad de los datos*
  - *Confidencialidad*
  - *Integridad*
  - *Disponibilidad*
- *Método de Autenticación*
- *Auditabilidad (registro de logs)*
- *Requisitos de seguridad para los accesos por terceras partes*

Arquitectura de Red / Tráficos

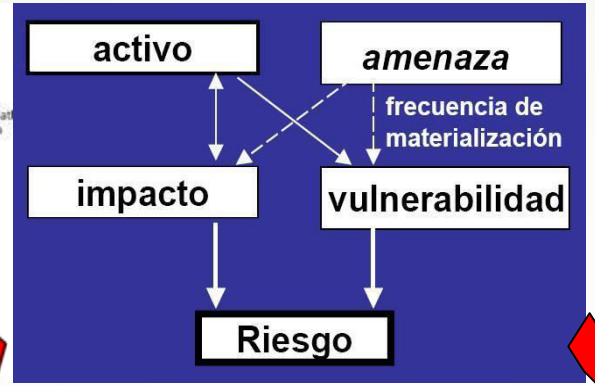
	Requerimientos de seguridad /Controles	Totalmente conforme. No necesita desarrollo adicional	Requieren una mínima personalización. El coste está incluido en la oferta.	Requieren una personalización o no puede ser puesto en práctica. El coste no está incluido en la oferta.	Comentarios
1	**Arquitectura**				
1.1	**Arquitectura de Red**				
	La arquitectura está separada en tres capas • Capa de presentación: específica para redes abiertas que deben estar visibles desde Internet, servidores web, servidores proxy, DNS's, etc. Esta capa únicamente tiene conexión con redes externas y con la capa de aplicación. • Capa de aplicación: Tráfico de servidores, servidores de aplicación, servidores de mensajes, etc. Esta capa sólo estará accesible desde la capa de presentación y la capa de datos. • Capa de datos: En esta capa se ubicarán bases de datos, directorios, DNS's privados, sistemas de información de clientes, servidores de certificados, red da administración, etc.	✓			La base de datos está en capa dos
	Los clientes únicamente acceden a las plataformas ubicadas en la capa de presentación. No tienen acceso directo a los nodos ubicados en el resto de capas.	✓			
	Los interfaces del producto de acceso exclusivo de usuarios internos están ubicados en la capa de datos.	✓			
	Todos los nodos del producto, independientemente de la capa en la que se encuentren están accesibles desde la red de gestión para su monitorización, operación, backup, etc.	✓			
1.2	**Tráficos**				
	Cada nodo tiene habilitados interfaces físicos separados para los siguientes tráficos: • Tráfico de clientes • Tráfico de facturación • Tráfico de monitorización, administración, supervisión, operaciones y mantenimiento, backup, etc.		✓		

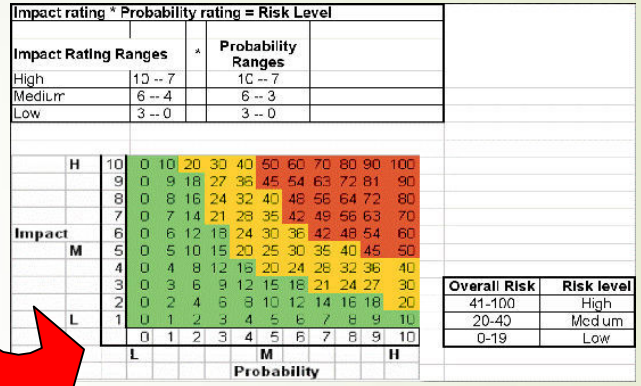
Evaluación del riesgo



Evaluación de Riesgos en materia

Cálculo del Riesgo





1. Se estima el ***impacto*** que podría provocar una falla o ***vulnerabilidad*** de seguridad en el negocio, teniendo en cuenta las potenciales consecuencias por la pérdida de CID de la información y otros recursos.

2. Se estima la ***probabilidad*** de ocurrencia de dicha falla o ***vulnerabilidad*** teniendo en cuenta las amenazas y vulnerabilidades, y los controles actualmente implementados.

3. Se calcula el

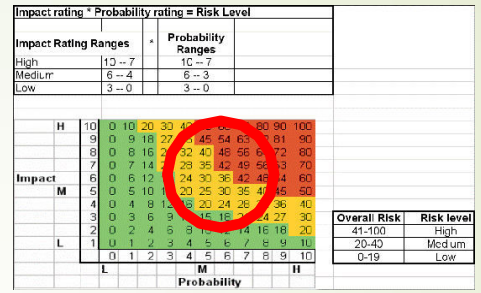
Riesgo = Probabilidad x Impacto

4. Se decide si se:

   a. ***Asume el riesgo***
   b. ***Mitiga el riesgo*** mediante la implantación de controles
   c. ***Transfiere el riesgo*** a terceros

Selección de Controles

- Una vez identificados los requerimientos de seguridad, deben *seleccionarse e implementarse controles* que *reduzcan los riesgos* a un nivel aceptable.



Valor del Activo > Costo Implementación

- Los controles deben seleccionarse teniendo en cuenta el *costo de implementación* en relación con los riesgos y el *valor de las pérdidas* que podrían producirse de tener lugar una violación de la seguridad. También deben tenerse en cuenta factores no monetarios (Ej.: daño en la reputación).

- El *responsable del proyecto*, deberá *asumir los riesgos derivados de la no implantación de las medidas* de seguridad o en caso contrario, tomar las medidas oportunas que garanticen la eliminación del riesgo.

- Esta *información se almacenara* para documentar los riesgos y disponer de la información necesaria para estimaciones de ROI o frente a posibles auditorias.

Punto de partida para la Seguridad de la Información

- Algunos controles pueden considerarse como *principios rectores* que proporcionan un buen punto de partida para la implementación de la seguridad de la información

  - Controles esenciales (legal)
    - protección de datos y confidencialidad de la inf. personal
    - protección de registros y documentos de la organización
    - derechos de propiedad intelectual

  - Controles de práctica recomendada (buenas prácticas)
    - documentación de la política de seguridad de la información
    - asignación de responsabilidades en materia de seg. de la inf.
    - formación y entrenamiento en materia de seg. de la información
    - comunicación de incidentes relativos a la seguridad
    - gestión de la continuidad de actividades de la organización

- Sin embargo *estos controles no reemplazan* la selección de controles que se obtienen a partir de *un análisis de riesgos*.

Factores Críticos del Éxito

- política de seguridad, objetivos y actividades que reflejen los objetivos de la empresa

- una estrategia de implementación de seguridad que sea consecuente con la cultura organizacional

- apoyo y compromiso manifiestos por parte de la dirección

- un claro entendimiento de los requerimientos de seguridad, la evaluación de riesgos y la administración de los mismos

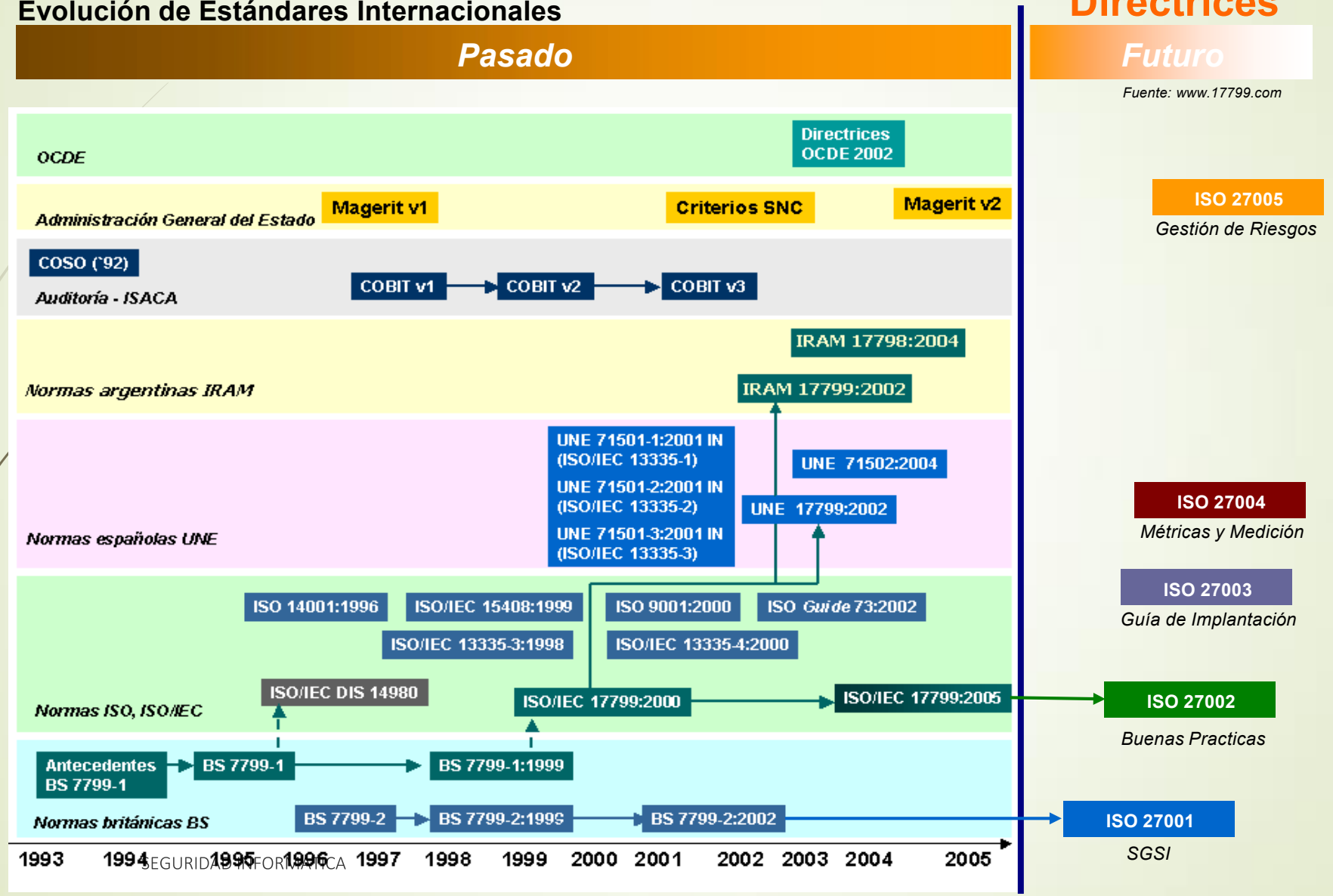
- comunicación eficaz de los temas de seguridad a todos los directivos y empleados

- distribución de guías sobre políticas y estándares de seguridad de la información a todos los empleados y contratistas

- formación y entrenamiento adecuado en todos los niveles

- un sistema eficaz de medición y evaluación del desempeño de la gestión de la seguridad, enfocada en la mejora continua

Evolución de Estándares Internacionales



Desarrollo de Directrices

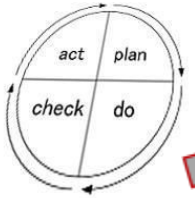
ISO/IEC 27001: 2007: SGSI - Sistema de gestión de seguridad de la información.
ISO/IEC 27002: 2007 y 2013: (Antes ISO 17799:2005). Guía de buenas prácticas sobre seguridad de la información.
ISO/IEC 27003: 2010 – Guía que se centra en los aspectos críticos para el diseño e implementación con éxito de un SGSI.
ISO/IEC 27004: 2009 – Guía para el desarrollo y utilización de métricas y técnicas de medida para la eficacia de un SGSI.
ISO/IEC 27005: 2011 – Proporciona directrices para la gestión del riesgo en la seguridad de la información.
ISO/IEC 27006: 2011 – Especifica los requisitos para la acreditación de entidades de auditoría y certificación SGSI.
ISO/IEC 27007: 2011 – Guía de auditoría de un SGSI.
ISO/IEC TR 27008: 2011- Guía de auditoría de los controles seleccionados en el marco de implantación de un SGSI.
ISO/IEC 27010: 2012 – Guía para la gestión de la seguridad de la información compartida entre organizaciones.
ISO/IEC 27011: 2008 – Guía de interpretación de implementación y gestión de la seguridad en org de sector telecomunicaciones.
ISO/IEC 27013: 2012 – Guía de implementación integrada ISO/IEC 27001 (SGSI) e ISO/IEC 20000-1 (gestión de servicios TI).
ISO/IEC 27014: 2012 – Guía de gobierno corporativo de la seguridad de la información.
ISO/IEC 27015: 2013 – Guía de SGSI para organizaciones del sector financiero y de seguros.
ISO/IEC TR 27016: 2013 – Guía de valoración de los aspectos financieros de la seguridad de la información.
ISO/IEC 27017: 2013 – Guía de seguridad para Cloud Computing.
ISO/IEC 27031: 2011 – Guía de apoyo para la adecuación de las TIC de una organización para la continuidad del negocio.
ISO/IEC 27032: 2012 – Guía relativa a la ciberseguridad.
ISO/IEC 27033 – Norma dedicada a la seguridad en redes en 7 partes
ISO/IEC 27034 – Dedicada la seguridad en aplicaciones informáticas, consistente en 5 partes
ISO/IEC 27035: 2011 – Guía sobre la gestión de incidentes de seguridad en la información.
ISO/IEC 27036: 2013 – Guía en cuatro partes de seguridad en las relaciones con proveedores
ISO/IEC 27037: 2012 – Guía de identificación, recopilación y custodia de evidencias digitales.
ISO/IEC 27038: 2013 – Guía de especificación para seguridad en la redacción digital.
ISO/IEC 27039: 2013 – Guía para la selección, despliegue y operativa de sistemas de detección y prevención de intrusión
ISO/IEC 27040: 2014 – Guía para la seguridad en medios de almacenamiento.
ISO 27799: 2008 – Proporciona directrices para apoyar la interpretación y aplicación en el sector sanitario de ISO/IEC 27002.

Estándares Internacionales

“La rueda ya esta inventada”

Estándares Internacionales

ISO 27001



COBIT

Establecimiento de Objetivos de Control en cuatro Dominios IT:

- Planificación y Organización
- Adquisición e Implantación
- Entrega y Soporte
- Monitorización

ITIL®
IT Service Management

ISO 20000

Guía de buenas prácticas para la gestión de IT de forma global:

- Asegurar que la provisión y soporte de los Servicios de IT sean apropiados a los requerimientos del Negocio
- Orientado a la calidad
- Lograr que el Negocio haga uso efectivo y eficiente de los SI

ISO 27002

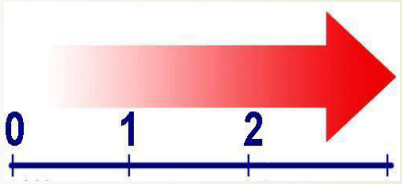
Recomendaciones para la gestión de la Seguridad de la Información:

- Base común para normativas y procedimientos
- Práctica eficaz de la gestión
- Proporcionar confianza entre Organizaciones

Desarrollo de Directrices

¿Cómo encajan los Estándares en las Organizaciones?

- Son el punto de partida para el desarrollo de lineamientos específicos (ej.: Plan Estratégico de Seguridad)



- Son un esquema que debe ajustarse a cada Organización, quitando o agregando controles que no están incluidos en el estándar

- Pueden funcionar en dos direcciones:

Guía para adopción de medidas (normativa)

Instrumento de autoevaluación (checklist)

48

Seguridad de la información

Desde el punto de vista informático

- *Aspectos Generales*
- *Definiciones*
- *Tipos de Ataques*
- *Controles InfoSec*
- *Dimensiones o Pilares de Seguridad*
- *Dónde tener en cuenta la Seguridad?*

Definición de seguridad de la información (InfoSec)

- La seguridad de la información, que suele abreviarse como InfoSec, es un conjunto de procedimientos y herramientas de seguridad que protegen ampliamente la información confidencial de la empresa frente al uso indebido, acceso no autorizado, interrupción o destrucción.
- InfoSec comprende la seguridad física y del entorno, el control de acceso y la ciberseguridad.
- Suele incluir tecnologías como **agente de seguridad de acceso a la nube** (CASB), herramientas de engaño, detección y respuesta en el punto de conexión (EDR) y pruebas de seguridad para DevOps (DevSecOps), entre otras.

Elementos clave de seguridad de la información

- **InfoSec** comprende un conjunto de herramientas, soluciones y procesos de seguridad que mantienen la información de la empresa segura entre dispositivos y ubicaciones, ayudando en la protección contra **ciberataques** u otros eventos disruptivos.

Elementos clave de seguridad de la información cont.

- **Seguridad de aplicaciones**
  - Políticas, procedimientos, herramientas y procedimientos recomendados que se aplican para proteger las aplicaciones y sus datos.
- **Criptografía**
  - Método basado en algoritmos para proteger la comunicación para garantizar que solo los destinatarios de un mensaje específico pueden verlo y descifrarlo.
- **Recuperación ante desastres**
  - Método para restablecer los sistemas tecnológicos funcionales tras un evento disruptivo como, por ejemplo, un desastre natural o un ciberataque.
- **Respuesta a incidentes**
  - El plan de respuesta de la organización para corregir y administrar las consecuencias de un ciberataque, una vulneración de datos u otro evento disruptivo.

Elementos clave de seguridad de la información cont.

- **Seguridad de infraestructura**
  - La seguridad que comprende toda la infraestructura tecnológica de una organización, incluyendo tanto los sistemas de hardware como de software.

- **Administración de vulnerabilidades**
  - El proceso que lleva a cabo una organización para identificar, evaluar y corregir vulnerabilidades en sus puntos de conexión, software y sistemas.

Elementos clave de seguridad de la información cont.

- **Seguridad en la nube**
  - Políticas, procedimientos, herramientas y procedimientos recomendados que se aplican para proteger todos los aspectos de la nube, incluidos sistemas, datos, aplicaciones e infraestructura.

Seguridad en la nube

- **Definición de la seguridad en la nube**

La seguridad en la nube es una disciplina de la ciberseguridad centrada en la protección de datos y sistemas en la nube de amenazas internas y externas, e incluye procedimientos recomendados, directivas y tecnologías que ayudan a las empresas a prevenir el acceso no autorizado y las filtraciones de datos.

Seguridad en la nube

Cuando desarrollan una estrategia de seguridad en la nube, las empresas deben tener en cuenta cuatro tipos de entornos de informática en la nube:

Entornos de nube pública
Están ejecutados por proveedores de servicios en la nube. En este entorno, los servidores están compartidos por varios espacios empresariales.

Entornos de nube privada
Pueden estar en un centro de datos propiedad del cliente o pueden estar ejecutados por un proveedor de servicios en la nube. En ambos casos, los servidores son un espacio empresarial individual y las organizaciones no tienen que compartir espacio con otras compañías.

Entornos de nube híbrida
Son una combinación de centros de datos locales y nubes de terceros.

Entornos multinube
Incluye dos o más servicios en la nube operados por distintos proveedores de servicios en la nube.

La importancia de la seguridad en la nube

- La nube se ha convertido en una parte integral de la vida en línea. Facilita el trabajo y la comunicación digital, y ha impulsado una innovación rápida en las organizaciones.
- Sin embargo, cuando los amigos comparten fotografías, los compañeros de trabajo colaboran en un nuevo producto o los gobiernos ofrecen servicios en línea, no siempre está claro dónde se están almacenando los datos.
- Las personas pueden mover accidentalmente los datos a una ubicación menos segura y, como todo es accesible desde Internet, los activos tienen un mayor riesgo de acceso no autorizado.
- Asimismo, la privacidad de los datos es cada vez más importante para las personas y los gobiernos. Las regulaciones como el Reglamento general de protección de datos (GDPR) y la Ley de transferencia y responsabilidad de seguros de salud (HIPAA) requieren que las organizaciones que recopilan información lo hagan de manera transparente y que apliquen directivas que impidan el robo o el uso indebido de los datos. Su incumplimiento puede implicar el pago de caras multas o daños en la reputación.

La importancia de la seguridad en la nube cont.

- Para ser competitivas, las organizaciones deben continuar utilizando la nube para iterar rápidamente y permitir que los empleados y los clientes tengan acceso fácilmente a los servicios, a la vez que protegen los datos y los sistemas de las siguientes amenazas:

- **Cuentas en peligro:** Los atacantes a menudo utilizan campañas de **phishing** para robar contraseñas de empleados y obtener acceso a sistemas y valiosos activos corporativos.

- **Vulnerabilidades de hardware y software:** Tanto si la organización utiliza una nube pública como si utiliza una privada, es fundamental que el hardware y el software estén actualizados y que se apliquen las revisiones oportunas.

- **Amenazas internas:** El error humano es una de las principales causas de las vulneraciones de seguridad. Un error de configuración puede abrir una puerta a usuarios malintencionados. Asimismo, los empleados a menudo hacen clic en vínculos malintencionados o mueven accidentalmente datos a ubicaciones con menos seguridad.

Como se brinda la seguridad en la Nube

La seguridad en la nube es una responsabilidad compartida entre los proveedores de servicios en la nube y sus clientes. La responsabilidad varía dependiendo del tipo de servicios ofrecidos:

- **Infraestructura como servicio (IaaS)**
  - En este modelo, los proveedores de servicios en la nube ofrecen recursos informáticos, de red y de almacenamiento a petición. El proveedor es responsable de proteger los servicios informáticos básicos. Los clientes deben proteger todo lo que se añade al sistema operativo, por ejemplo, las aplicaciones, los datos, los entornos de ejecución, el middleware y el propio sistema operativo.
- **Plataforma como servicio(PaaS)**
  - Muchos proveedores también ofrecen un entorno de desarrollo e implementación completo en la nube. Son responsables de proteger el entorno de ejecución, el middleware y el sistema operativo, además de los servicios informáticos básicos. Los clientes deben proteger sus aplicaciones, los datos, el acceso de los usuarios, los dispositivos de usuario final y las redes de usuario final.
- **Software como servicio(SaaS)**
  - Las organizaciones también pueden tener acceso al software con un modelo de pago por uso como, por ejemplo, Microsoft Office 365 o Google Drive. En este modelo, los clientes también tienen que proporcionar seguridad para sus datos, usuarios y dispositivos.

Como se brinda la seguridad en la Nube

Independientemente de quién sea responsable, la seguridad en la nube se basa en **cuatro aspectos principales**:

- **Limitación del acceso:** Como la nube permite que todo sea accesible desde Internet, es sumamente importante garantizar que solo las personas adecuadas tengan acceso a las herramientas correctas el tiempo que sea necesario.
- **Protección de los datos:** Las organizaciones deben saber dónde se encuentran sus datos y aplicar los controles correspondientes para proteger los propios datos y la infraestructura donde se hospedan.
- **Recuperación de datos:** Una buena solución de copia de seguridad y un buen plan de recuperación de datos son fundamentales en el caso de se produzca una vulneración.
- **Plan de respuesta:** Cuando una organización es atacada, necesita un plan para reducir el impacto y evitar que otros sistemas se vean en peligro.

Seguridad de la Información
Inconvenientes con la Dirección

- Hablar distintos idiomas: Negocio vs. Tecnología.
- Incapacidad de entender o cuantificar amenazas, o medir la severidad de los riesgos relacionados con los recursos.
- Comenzar un análisis con el preconcepto de que el costo de los controles necesarios, será excesivo.
- Creer que la implementación de seguridad interferirá con los objetivos de negocio.

Necesidad de concientizar a la Dirección

Seguridad de la Información

Algunos conceptos

Sujeto (entidad activa): persona, recurso, asunto o proceso que causa que la información fluya **desde y hacia** los objetos. Es siempre la entidad que altera o modifica la información del objeto, o bien, los datos almacenados dentro de él.

- **Ejemplos:** Usuarios, Programas, Procesos, Computadoras, etc.

Objeto (entidad pasiva): contiene o recibe información, datos.

- **Ejemplos:** Archivos, Bases de datos, Programas, Procesos, Impresoras, Medios de almacenamientos, etc.

- **Acreditación:** Acreditación del Sujeto.
- **Clasificación:** Clasificación del Objeto.

Seguridad de la Información

Principio de Equilibrio de la Seguridad

Seguridad de la Información
Algunos conceptos

- **Activo**: Recurso necesario para que la Organización funcione correctamente y alcance los objetivos propuestos por su Dirección. Se distinguen cinco tipos o categorías de activos:
  - Entorno
  - Sistema de Información
  - Información
  - Funcionalidades de la Organización
  - Otros activos

Definiciones de Seguridad Algunos Conceptos

- **Amenaza**: Representa un evento que puede desencadenar un incidente, produciendo daños materiales o pérdidas sobre la información. Acción capaz de modificar el estado de seguridad de un activo. La diversidad de causas permite clasificar a las amenazas según su naturaleza en:
  - **Accidentes** – Físico industrial. Avería. Físico Natural. Interrupción de servicios o suministros. Accidentes mecánicos o electromagnéticos.
  - **Errores** – De utilización. De diseño. De ruta, secuencia o entrega. Inadecuada monitorización, trazabilidad o registro del tráfico de información.
  - **Intencionales presenciales** – Destrucción o sustracción. Acceso lógico solo lectura. Acceso lógico con alteración o sustracción de información. Acceso lógico con corrupción o destrucción de información en tránsito o de configuración. Indisponibilidad de recursos humanos (huelga) o técnicos. (bloqueo).
  - **Intencionales de origen remoto** – Acceso lógico con interceptación pasiva. Acceso lógico con corrupción o destrucción de información. (man-in-the-middle) Acceso lógico con alteración de información. Suplantación de origen. Repudio del origen o de la recepción de la información en tránsito.

Definiciones de Seguridad Algunos Conceptos

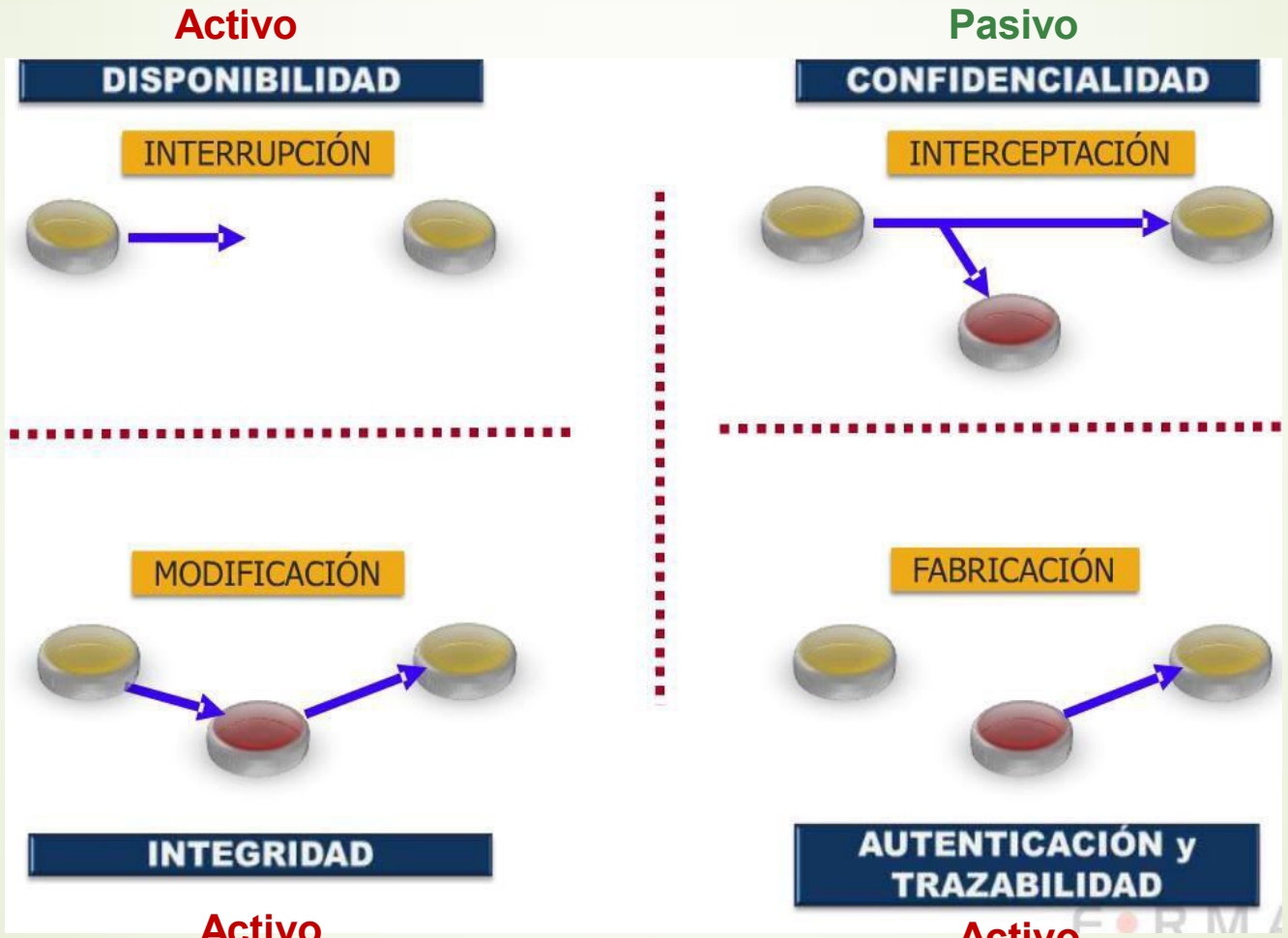
- **Vulnerabilidad**: Representa la potencialidad o posibilidad de ocurrencia de la materialización de una amenaza sobre un activo. Es una propiedad de la relación entre un activo y una amenaza, representando el mecanismo de paso desde una amenaza a la agresión materializada.
- **Impacto**: Representa la diferencia entre las estimaciones del estado de seguridad de un activo, obtenidas antes y después de la materialización de una amenaza.
- **Riesgo**: Probabilidad cuantificable de que una amenaza tome ventaja o explote una vulnerabilidad de un sistema. Representa la posibilidad de que se produzca un impacto determinado sobre un activo, dominio o en toda la Organización. Se distinguen varios tipos:
  - **Valor intrínseco** – Antes de aplicar salvaguardas.
  - **Valor residual** - El que se da tras la aplicación de salvaguardas. (simulado o real).
  - **Umbral de riesgo** – Valor establecido como base para decidir si el riesgo es asumible o aceptable.

El riesgo puede propagarse entre activos dependientes entre sí.

Definiciones de Seguridad Algunos Conceptos

- **Salvaguarda**: Representa acciones o procedimientos reductores del riesgo. Se distinguen 2 tipos de salvaguardas:
  - **Preventivas** – Actúan sobre la debilidad, reduciendo la potencialidad de materialización de una amenaza. (Ej. Concienciación, Información y formación, Disuasión, Prevención, Detección preventiva).
  - **Curativas** – Actúan sobre el impacto y reducen su gravedad. (Ej. Corrección, Recuperación, Detección curativa).
- **Contramedida o Control (Corrective Control):** Sinónimos de Salvaguarda.

Daños a la Información – Ataques Activos y Pasivos

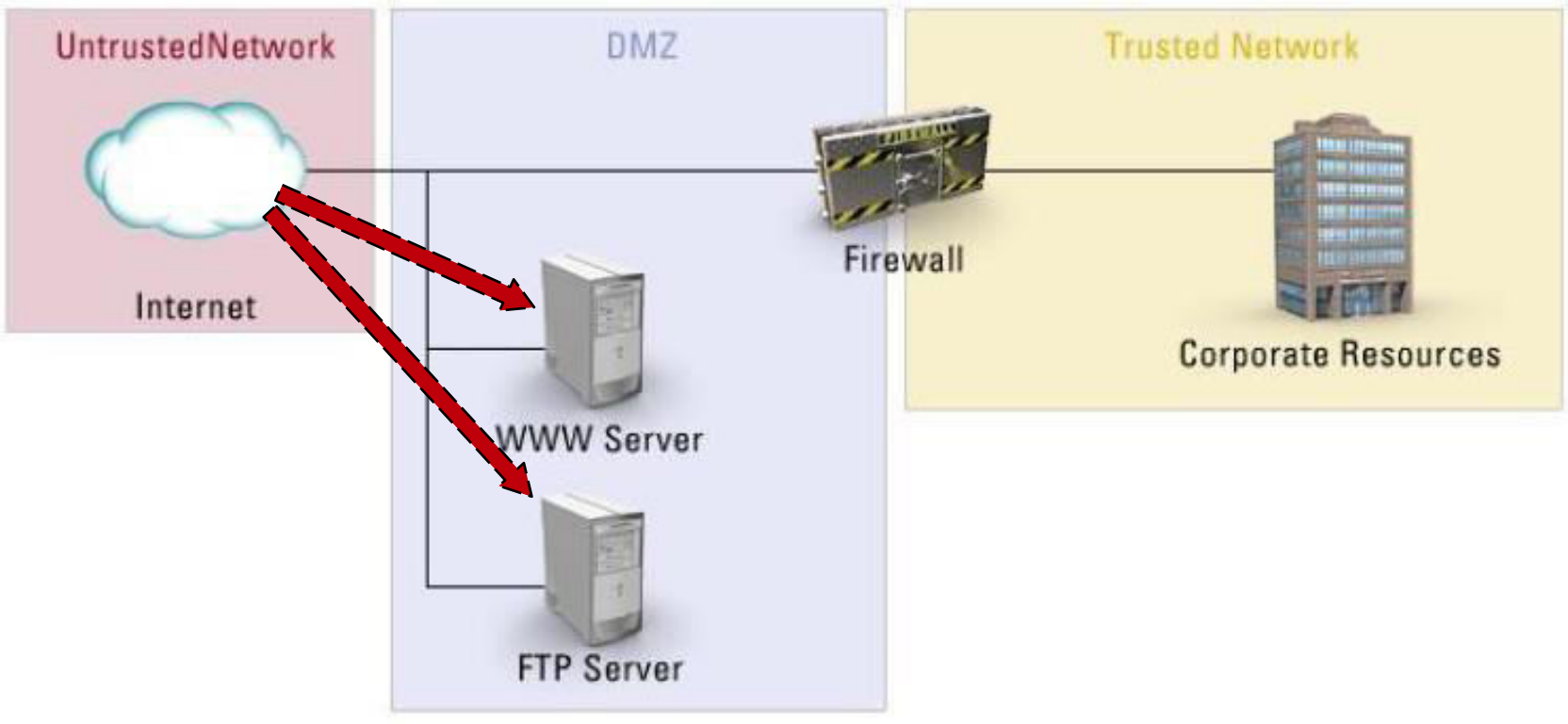


Daños a la Información Ataques Activos

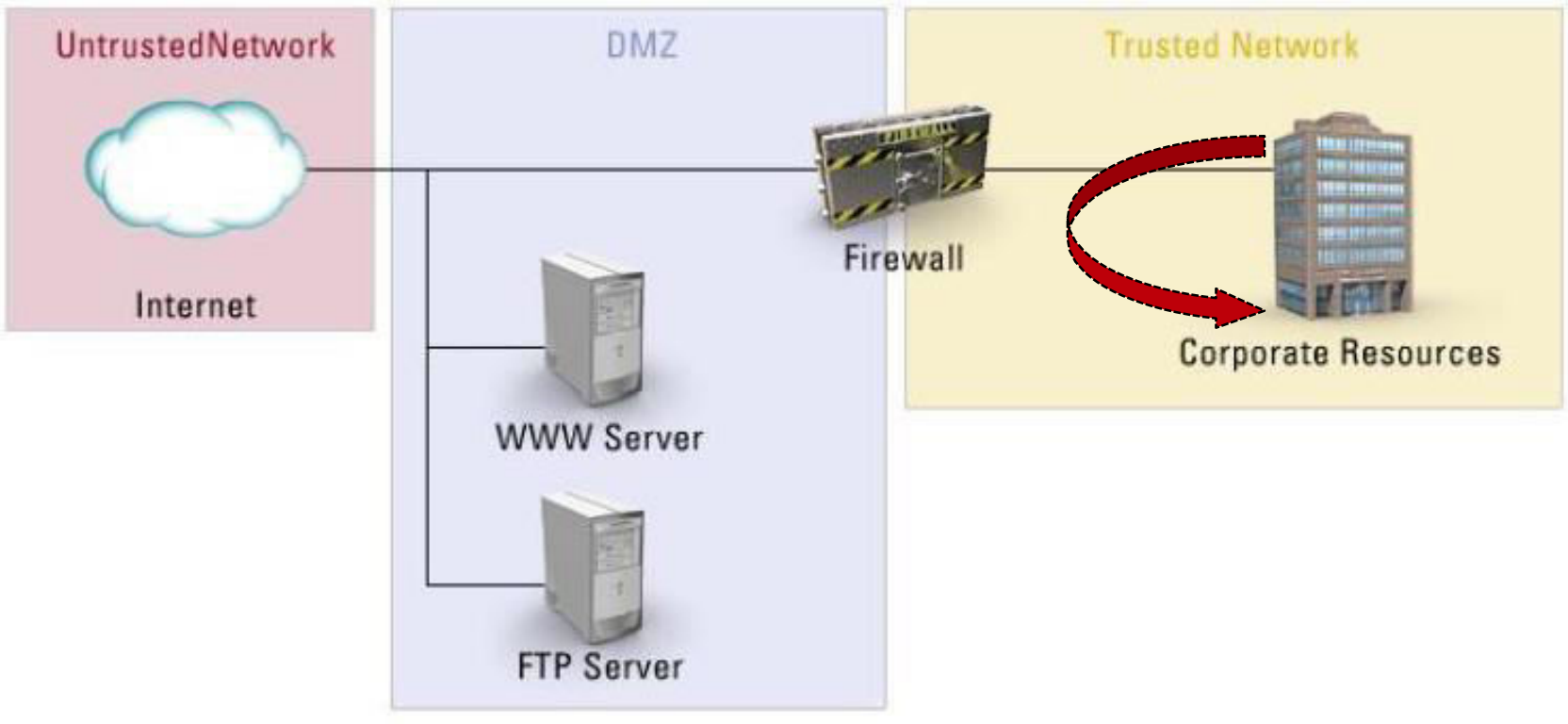
Los ataques Activos pueden a su vez dividirse en:

- **Suplantación de identidad**: tiene lugar cuando el intruso se hace pasar por otro. Normalmente incluye alguna de las otras formas de ataque activo. Por ejemplo, secuencias de autenticación pueden ser capturadas y repetidas, permitiendo a una entidad no autorizada acceder a una serie de recursos privilegiados suplantando a la entidad que posee esos privilegios (Ej.: robar la contraseña de acceso a una cuenta).
- **Reactuación**: tiene lugar cuando uno o varios mensajes legítimos son capturados y repetidos para producir un efecto no deseado (Ej.: transferencias repetidas de dinero a una misma cuenta).
- **Modificación de mensajes**: tiene lugar cuando una parte del mensaje legítimo es alterada o los mensajes son retardados o reordenados, para producir un efecto no autorizado. Ej.: "transferencia a la *cuenta A*, es desviada a la *cuenta B*".
- **Degradación fraudulenta del servicio**: tiene lugar cuando se impide o se inhibe el uso normal o la gestión de los recursos informáticos y las comunicaciones. (Ej.: un intruso podría suprimir todos los mensajes dirigidos a una determinada entidad o se podría interrumpir el servicio de una red inundándola con mensajes sin sentido.

Ataque Externo: Agresión originada desde fuentes no confiables.



Ataque Interno: **Agresión originada desde fuentes confiables.**



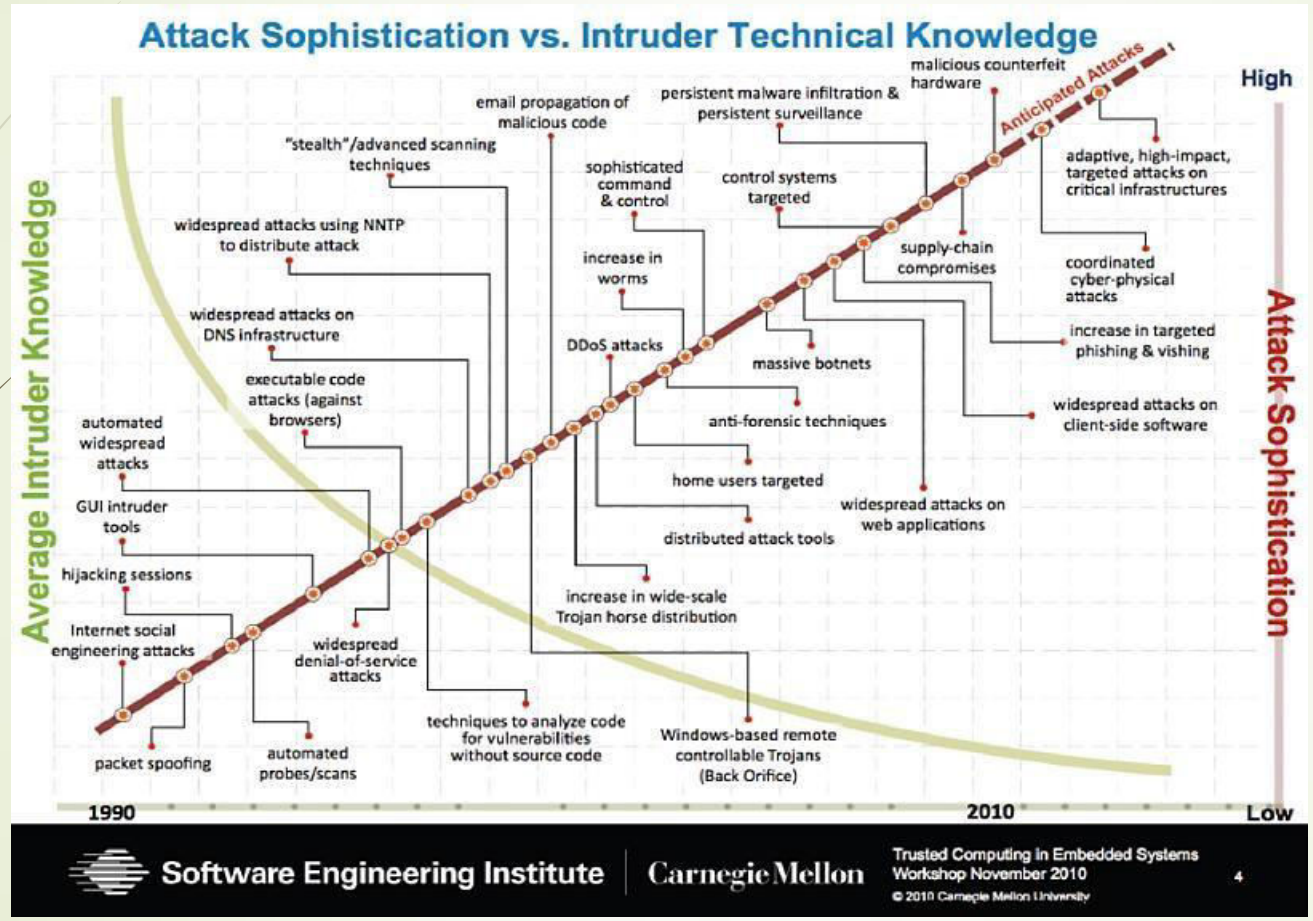
Ataque Estructurado: Metódico

- Se da cuando el atacante dispone de los medios (equipos), determinación, conocimiento (técnico y entorno), recursos (dinero), y tiempo.
- El profesional debe dificultar al máximo el trabajo del atacante utilizando un enfoque de seguridad por capas.

Ataque No Estructurado: Desorganizado

- Se da cuando el atacante no tiene conocimientos ni experiencia.
- Sin embargo, las redes públicas le permiten acceder a un repositorio de herramientas y utilidades, infinitas.

Ataques evolución

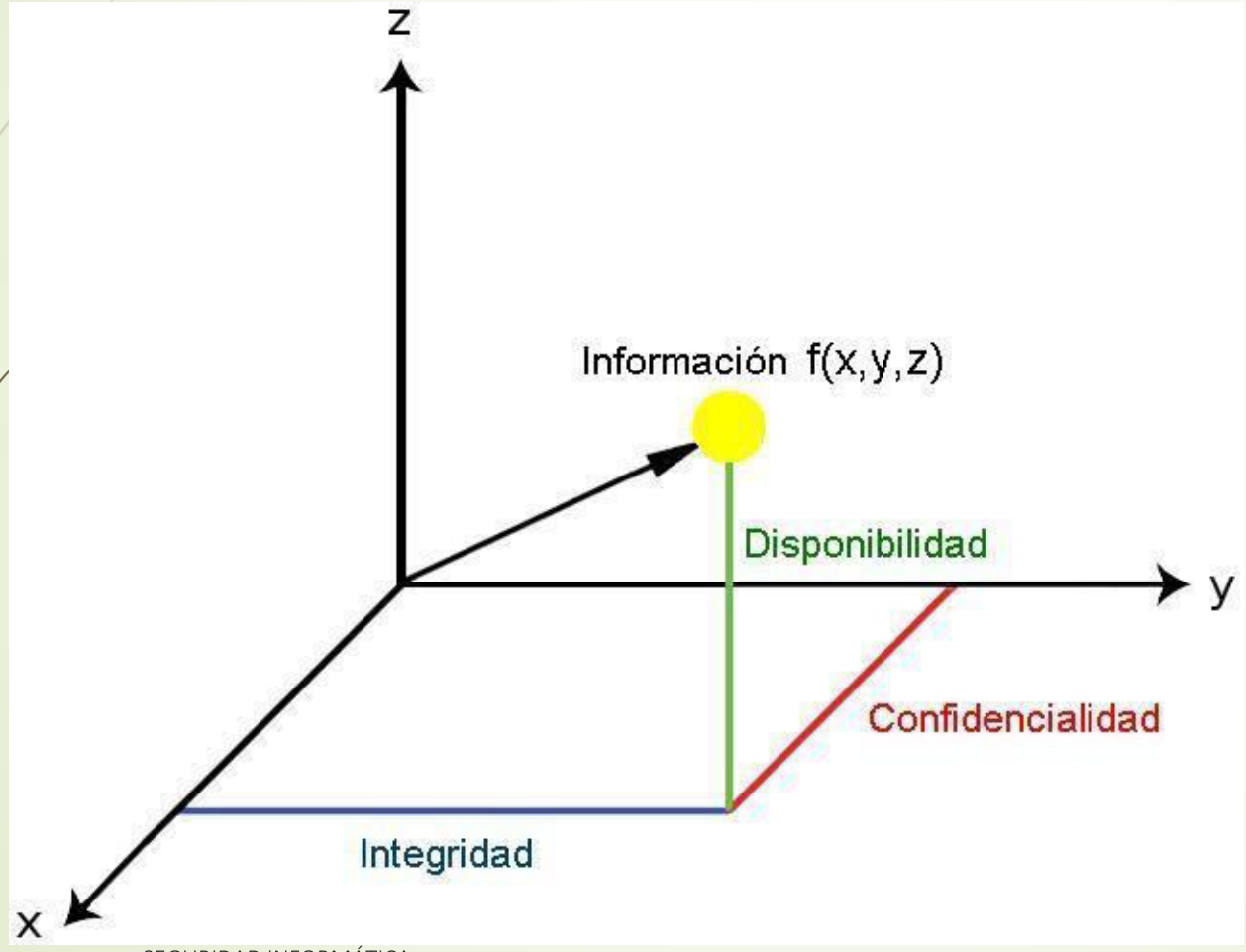


Dimensiones de la Seguridad

The Big Three

Dimensiones de Seguridad

The Big Three

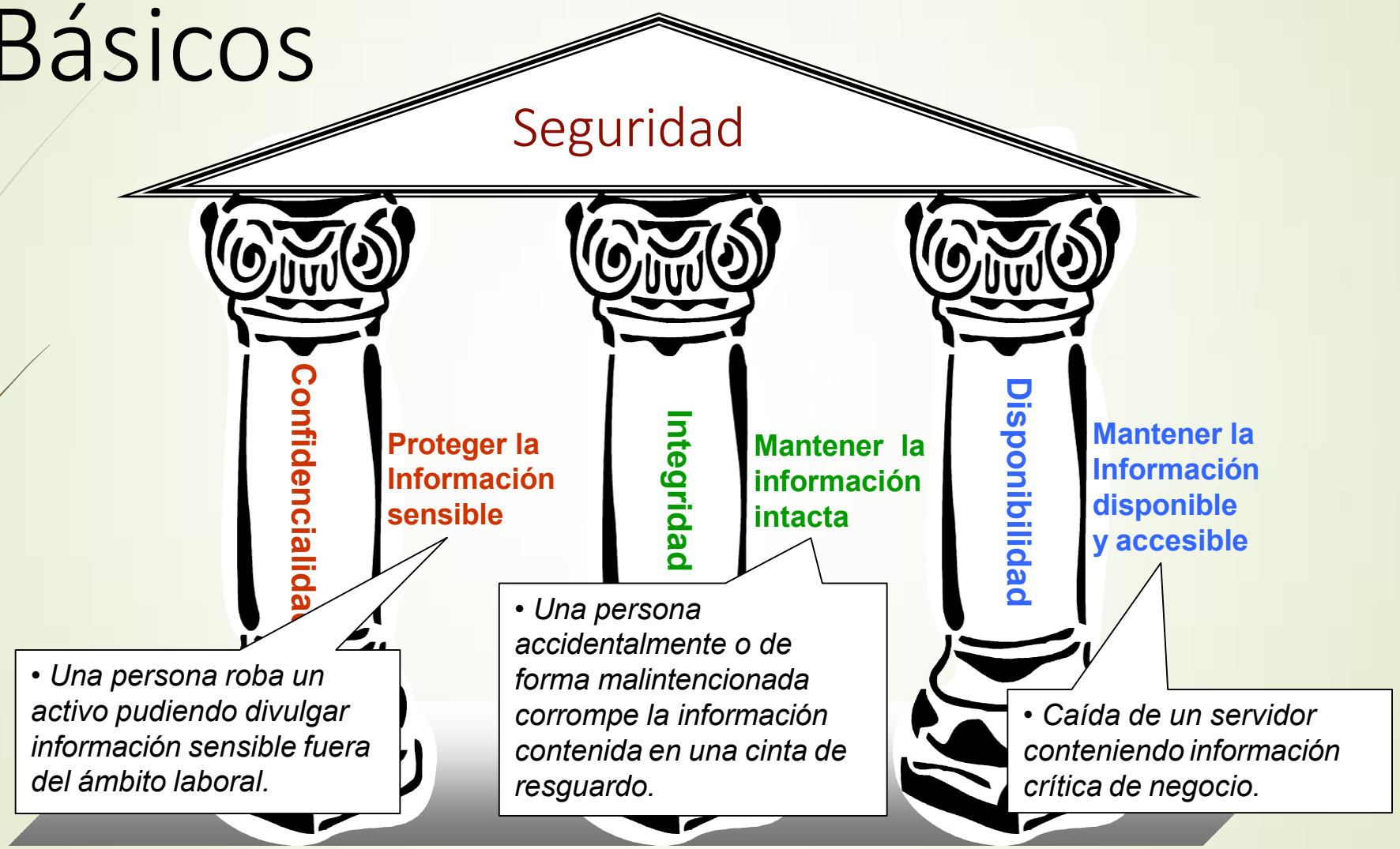


Valoración **CID**

Tríada de Seguridad

Dimensiones de Seguridad

Básicos



Confidencialidad

- Previene contra la divulgación no autorizada de los datos
  - Proporciona un grado de certeza de que los datos no han sido comprometidos, puestos a disposición o divulgados a personas no autorizadas, a procesos, u otras entidades. En esencia, se asegura que los datos sólo pueden accedidos entre las partes de confianza.
  - Puede ser violada mirando detrás del hombro (shoulder surfing), snifeando o monitoreando la red, robando una contraseña o por medio de técnicas de spoofing o de ingeniería social.
  - En el mundo electrónico, la confidencialidad se logra a través de mecanismos criptográficos o de cifrado.

Confidencialidad

- Es la propiedad de **tener datos y recursos accesibles solo para aquellos que están autorizados a acceder a ellos, y mantenerlos en secreto para todas las demás partes.**
- Esto significa que para que la información mantenga un estado verdaderamente confidencial, nadie más debería poder mirarla o tenerla en sus manos, ya sean piratas informáticos dedicados o simplemente una vecina entrometida.
- Los datos confidenciales deben mantenerse protegidos en todo momento, lo que significa que debemos encontrar formas de evitar que personas no autorizadas accedan a ellos mientras están almacenados, en tránsito e incluso durante el procesamiento.

Confidencialidad

- **¿Cuándo corre peligro la confidencialidad?**

- Los atacantes tienen a su disposición una variedad de tácticas diferentes que pueden usar para obtener acceso a los datos y violar tu confidencialidad.
- Estas incluyen pero no se limitan a:

- Robar un disco duro o un portátil.
- Plantar malware en un dispositivo,
- Realizar un intercambio de SIM y hacerse cargo de una cuenta.
- Ataques de ingeniería social como el phishing.
- Escaneo de puertos.
- Robo de contraseñas y otras credenciales.

Confidencialidad

- **¿Cuándo corre peligro la confidencialidad? Cont.**

- Con una gran cantidad de personas sin escrúpulos en Internet y un montón de técnicas diferentes a través de las cuales pueden violar la confidencialidad de los datos, debemos prestar mucha atención a los mecanismos de seguridad que utilizamos para evitar el acceso no autorizado.
- **Los accidentes, la falta de supervisión y otros tipos de negligencia también pueden dar lugar a violaciones no autorizadas de la confidencialidad** .
- Estos pueden incluir cosas a nivel individual, como dejar documentos confidenciales en la bandeja de la impresora u olvidarse de cifrar un mensaje.
- En un nivel superior, los errores que violan la confidencialidad pueden incluir la mala configuración de los controles de seguridad u otros errores administrativos.

Confidencialidad

- ¿Cuándo corre peligro la confidencialidad? Cont.

- Incluso si estas acciones no son intencionales, **aún pueden tener consecuencias dramáticas para las personas afectadas por la infracción y la organización responsable**.
- Una infracción no intencional puede dejar a las personas afectadas vulnerables a actos dañinos como el fraude, mientras que la organización responsable puede enfrentar sanciones legales y una variedad de otros costes.
- Seguir las prácticas de seguridad adecuadas puede ayudar a limitar los riesgos de amenazas tanto de accidentes como de atacantes, así como ayudar a reducir la posibilidad de que se viole la confidencialidad de tus datos.

Confidencialidad

- ¿Cómo mantenemos la confidencialidad de los datos?

- Si tienes planes secretos para dominar el mundo☺☺ y quieres mantenerlos confidenciales, puedes guardarlos **bajo llave** en una habitación. Mientras seas el único con una llave y nadie logre entrar, puedes asumir que tus planes secretos mantienen **su confidencialidad**.

- Restringir el acceso físico como en el ejemplo anterior es una forma de mantener la confidencialidad de los datos.

Confidencialidad

- **¿Cómo mantenemos la confidencialidad de los datos?**

- **En el entorno digital, tendemos a utilizar algoritmos de cifrado como AES y RSA**, junto con una variedad de otros cifrados.

- Estos algoritmos funcionan bastante bien y no es factible que los atacantes los rompan en esta etapa. Sin embargo, los algoritmos seguros como AES y RSA aún deben implementarse correctamente para ser seguros.

- Otra advertencia importante es que los algoritmos como AES y RSA solo pueden proporcionar confidencialidad *si las claves que cifran los datos no se ven comprometidas*.

- Si una parte **no autorizada** obtiene las claves, estos algoritmos de cifrado ya no pueden mantener la privacidad de los datos.

- Los algoritmos de cifrado generalmente se completan con medidas como la capacitación adecuada de los empleados, los mecanismos de control de acceso, los sistemas de autenticación y la clasificación de datos.

Integridad

Es la NO degradación de la calidad de los datos.

- Los datos que se han modificado o tienen la posibilidad de ser modificados en un servidor o en tránsito, son datos en los que **no se puede confiar.**
- La integridad brinda protección contra la modificación no autorizada o destrucción de información. Garantiza que los datos fluyen de extremo a extremo sin modificación. Asegura que ambos extremos son realmente quien dicen ser.
- Hay tres principios básicos que se utilizan para establecer la integridad de la información de una organización:
  - **Necesidad de conocer (need to know): Los usuarios deben tener acceso estrictamente sólo a los datos que deben conocer para cumplir con sus funciones. Este estado es conocido como el del "mínimo privilegio" (least privileged).**
  - **Separación de funciones: Garantiza que una única persona no tenga el control de una transacción completa (de principio a fin). Siempre, deben existir dos o más personas responsables.**
  - **Rotación de tareas: Las responsabilidades del trabajo deben de cambiar periódicamente de modo que los usuarios encuentren dificultades para conspirar o ejercer el control completo de una transacción con fines fraudulentos.**

Integridad

¿Qué es la integridad?

- Cuando hablamos de integridad, nos referimos a **proteger la exactitud y corrección de los datos**. Entonces, necesitamos implementar medidas para asegurarnos de que los datos no se modifiquen, alteren o corrompan.
- Por supuesto, esto no significa que no podamos cambiar nuestros datos nosotros mismos: las modificaciones intencionales y autorizadas no se consideran una violación de la integridad.
- ***Nos preocupamos principalmente por detener, detectar y rectificar violaciones no autorizadas o accidentales de la integridad de los datos.***
- Los atacantes pueden violar la integridad de los datos liberando virus, violando los sistemas de seguridad y manipulándolos, o incluso intentando hacer pasar datos fraudulentos como los datos originales.

Integridad

¿Qué es la integridad?

- Los administradores también pueden configurar incorrectamente los sistemas, lo que genera problemas de integridad de la información a mayor escala.
- Los datos también pueden corromperse a través de la transmisión o durante largos períodos de almacenamiento, por lo que es importante que también podamos detectar y corregir estas violaciones de integridad.
- Como puedes ver, existen varios tipos de violaciones de integridad. Ahora, ¿qué podemos hacer para protegerlos?

Integridad

¿El cifrado, proporciona integridad?

- Para comenzar, diremos que entendemos por cifrado una forma de codificar la información para impedir el acceso a ella.
- En ciertos casos, el cifrado puede ayudar a preservar la integridad de un mensaje. Después de todo, si un atacante no puede acceder a los datos de texto sin formato, será más difícil manipularlos.
- Sin embargo, preservar la integridad de los datos no es para lo que está diseñado el cifrado, y **nunca debe ser el único mecanismo en el que se confíe** para proporcionar integridad .
- Hay un par de razones para esto. Una es que ciertos cifrados de flujo son *maleables*, lo que significa que un atacante puede manipular datos sin conocer la clave de cifrado para ello. Esto hace posible que un atacante comprometa la integridad de los datos, sin violar su confidencialidad.
- Otra forma en que un atacante podría violar la integridad de las comunicaciones es si intercambia un mensaje cifrado por un mensaje cifrado visto anteriormente.

Integridad

Ejemplo de Cifrado

- Si por ejemplo se tiene el siguiente diálogo
  - A - ¿Hay partido?
  - B - Si
  - A - ¿Se juega con lluvia el partido?
  - B – Si

Integridad

Ejemplo de Cifrado Cont.

- Se cifra usando el siguiente cifrado, se desplaza una letra a la derecha del abecedario a por b, b por c, c por d, y así sucesivamente
- Quedaría el diálogo

- A - ¿Hay partido? →¿Ibz qbsujep?
- B - Si → Tj
- A - ¿Se juega con lluvia? → ¿Tf kvfhb dpñ mvwjb?
- B – Si → Tj

Integridad

Ejemplo de Cifrado Cont.

- No hace falta que se entienda lo que dice para violar la integridad.
- Si se cambia alguna letra del mensaje, ya se viola

- A - ¿Hay partido? →¿Ibz qbsujep?
- B - Si → Tj
- A - ¿Se juega con lluvia? → ¿Tf kvfhb dpñ mvwjb?
- B – Si → Op

Disponibilidad

Disponibilidad: Previene contra la denegación no autorizada de los datos

- La disponibilidad es el atributo que garantiza el acceso confiable y oportuno (ya mismo!) de las personas autorizadas a los recursos.
- Gestionando el ancho de banda se puede lograr que el trafico de alta prioridad llegue primero a destino (Calidad de Servicio - QoS) o se puede proporcionar alta disponibilidad y redundancia en la red. Sin embargo no se puede garantizar que un sistema esté operativo y sea capaz de responder a todas las solicitudes de los usuarios.

- Hay dos aspectos de la disponibilidad que se estudian habitualmente:
  - **Ataques de denegación de servicio (DoS)** – Son acciones maliciosas de usuarios o atacantes sobre los recursos informáticos, de manera tal que el sistema queda inutilizable o no puede ser accedido por los usuarios autorizados.
  - **Pérdida de Capacidad** - Cuando los desastres naturales (incendios, inundaciones, terremotos) o la acción humana (huelgas, código malicioso) afectan la capacidad de procesamiento de datos.

Disponibilidad

¿Cómo hacer que los datos estén disponibles?

- Existe una amplia gama de problemas que pueden hacer que los datos no estén disponibles, ya sea de forma no intencional o mediante un ataque deliberado.
- Debido a que hay una gran variedad de cosas que pueden salir mal, tenemos que diseñar cuidadosamente nuestros sistemas con una serie de medidas para ayudar a garantizar que los datos estén disponibles tanto como sea posible.
- Desafortunadamente, no podemos garantizar que los datos siempre estarán disponibles. Incluso los gigantes de Internet con todos los recursos del mundo, como Facebook y Amazon, experimentan tiempos de inactividad de vez en cuando.

Disponibilidad

¿Cómo hacer que los datos estén disponibles?

Para que nuestros datos estén disponibles de manera confiable tanto como sea posible, necesitamos crear sistemas resistentes. Estos deben incluir:

1- Infraestructura que tiene la capacidad de manejar tensiones y alta demanda.
2- Diseño del sistema que evita puntos únicos de falla.
3- Redundancias para todos los sistemas críticos. Estos deben ser probados regularmente.
4- Copias de seguridad de todos los datos importantes. Debe haber varias copias de todo, incluida al menos una almacenada en un sitio separado.
5- Planes de continuidad de negocio para crisis.
6- Controles de acceso como identificación, autenticación, autorización y rendición de cuentas.
7- Herramientas para monitorear el tráfico y el rendimiento de la red.
8- Mecanismos de protección contra ataques de denegación de servicio

Dimensiones de Seguridad Secundarias

Auditabilidad: Previene contra la falta de evidencias de acciones realizadas sobre los datos.

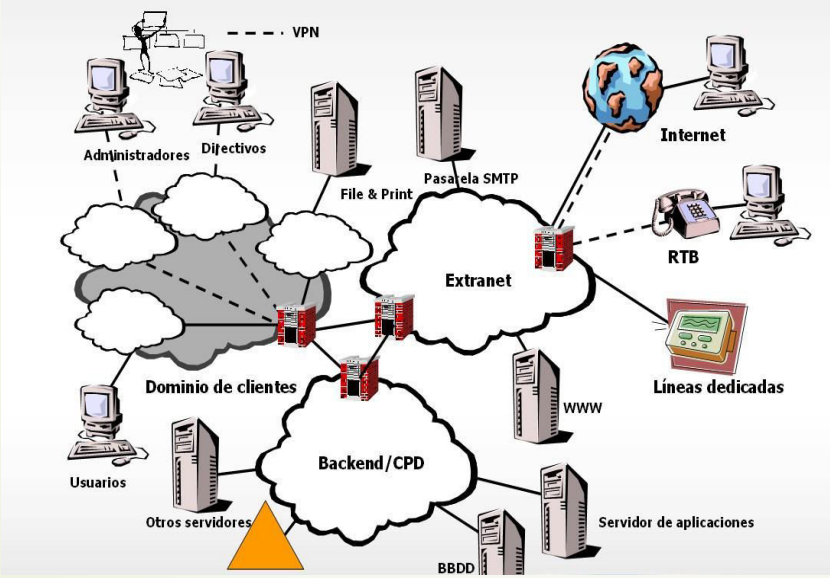
Autenticación: Proceso de verificar la identidad de una persona. Verifica que el usuario es quien dice ser.

No Repudio: Implica que el emisor no puede negar el envío porque el destinatario tiene pruebas de éste.

Profesional de ciberseguridad

El profesional de seguridad deberá garantizar tres cosas En la protección de la Infraestructura:

Que la información se mantenga confidencial,
Que la información se mantenga íntegra
Que la información esté disponible cuando sea necesario.



El profesional de seguridad tiene que:

- Demostrar conocimiento en el campo de Seguridad de la Información.
- Confirmar su compromiso con la profesión.
- Mejorar la credibilidad profesional.
- Ofrecer un aspecto diferenciador.
- Adquirir o fijar conocimientos.
- Incrementar salario, cambiar de empleo.
- Explotar la demanda de profesionales.
- Recorrer un camino de excelencia.

El profesional de seguridad sobre la organización tiene que:

- Garantizar el establecimiento de buenas practicas.
- Cumplir algún tipo de norma o requerimiento externo.
- Contar con profesionales comprometidos con un comportamiento ético.
- Adicionar credibilidad a su plantel interno.
- La garantía de contar con personal actualizado en la materia.
- Nivelar el conocimiento general del área de seguridad de la información en la organización.
- Elevar la imagen o percepción de clientes, partners, mercado, ámbito, etc.

El profesional de seguridad debe:

- Definir y mantener un programa integral de seguridad, el cual permita asegurar la existencia de los tres requerimientos básicos: Confidencialidad, Integridad y Disponibilidad.
- Establecer objetivos, alcance, prioridades, estrategias, y un plan de acción.

=> Plan Estratégico de Seguridad

El profesional de seguridad debe:

- Formulación de planes para salvaguardar archivos informáticos.
- Atención a las emergencias en materia de proceso de datos.
- Seguimiento de los informes sobre virus informáticos.
- Supervisión del uso de archivos de datos.
- Regulación del acceso para salvaguardar la información contenida en archivos informáticos.
- Implementación de protocolos criptográficos y herramientas de seguridad basadas en estos protocolos.
- Análisis y detección de amenazas de seguridad y desarrollo de técnicas de prevención.
- Conocimiento e interpretación normativa de centros de respuesta a incidentes de seguridad.
- Creación y desarrollo de proyectos de seguridad informática y de las comunicaciones.
- Análisis forense y análisis malware.

El profesional de seguridad debe:

- Este profesional también diseña y desarrolla proyectos, planes, programas y herramientas de seguridad que dan soporte o automatizan parte de las tareas a realizar.
- Puede implementar Sistemas de Gestión de la Seguridad en la Información (SGSIS) como administración de cortafuegos, antivirus en sistemas operativos Microsoft, Linux, Android, etc.;
- Se encarga de la resolución de incidencias, control de infraestructuras de seguridad TI, Seguridad Perimetral de Routing&Switching, WAN, LAN y wifi;
- Es responsable de la gestión de seguridad: hacking ético, análisis de vulnerabilidades, diseño de soluciones y herramientas, de mecanismos de autentificación, y de autorización, encriptación de dispositivos de almacenamiento masivo y de dispositivos móviles.

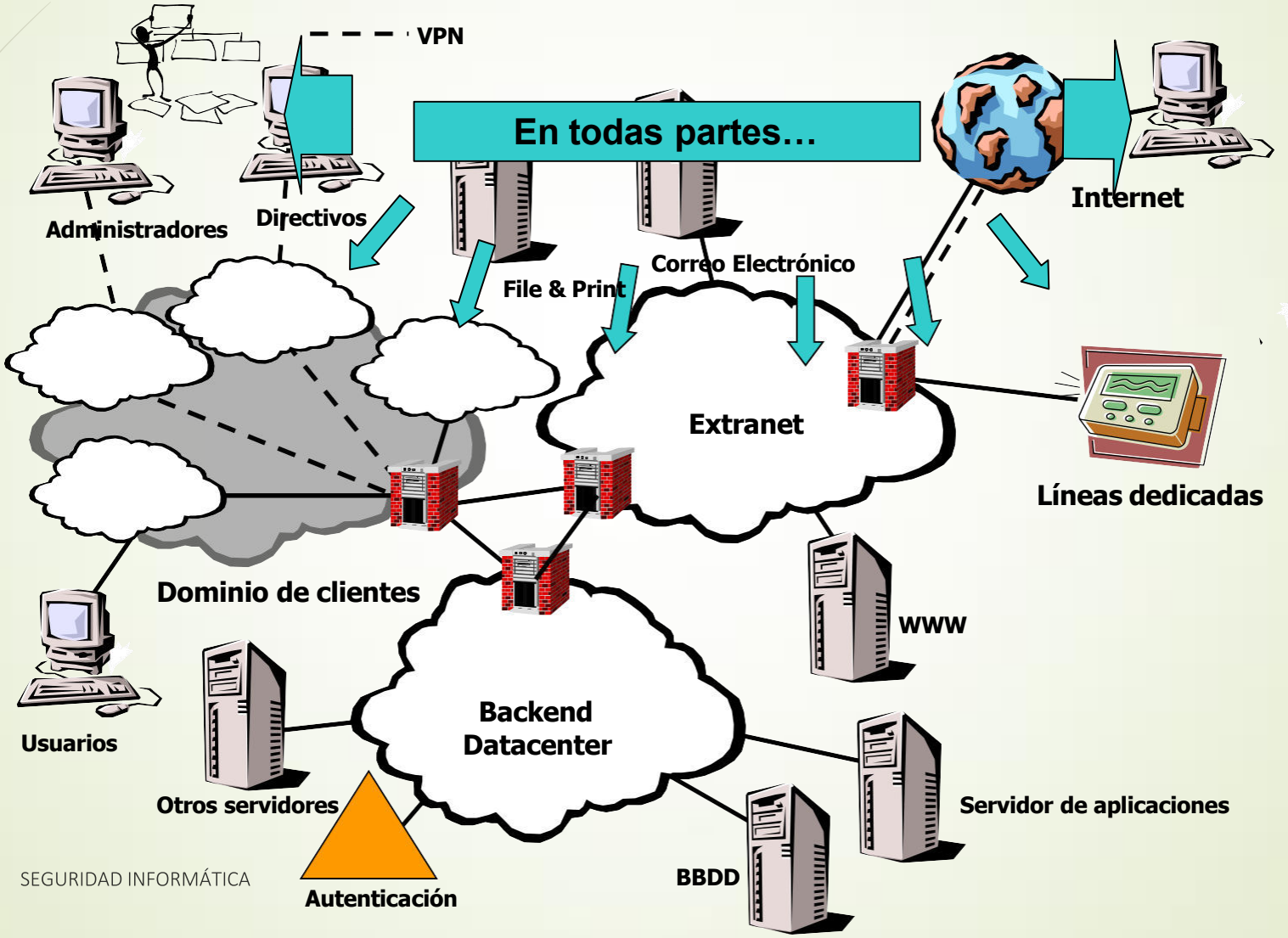
El profesional - formación:

- **Conocimientos de entornos tecnológicos**: SCADA, mobility, servidores, Smart Grid y otras arquitecturas tecnológicas.
- **Conocimientos de análisis forense**: sistemas de archivos, adquisición de evidencias, timeline, análisis de memoria, file carving, reconstrucción de ficheros, criptografía, etc.
- **Conocimientos de análisis de malware**: ASM x86/x64, determinación de funciones, métodos de infección y persistencia, desinfección de malware, ingeniería inversa/reversing, criptografía. Todo ello enfocado a diferentes tipos de formatos: PE, PDF, SWF, MS Office, APK, etc.
- Conocimientos de análisis y evaluación de vulnerabilidades técnicas para el descubrimiento y explotación de vulnerabilidades tanto en servidores como en puestos: test de intrusión, análisis forense, etc.
- Conocimientos de gestión de incidentes (Incident handling): sitemas operativos, networking, IDS, IPS, FW, análisis de logs, análisis de tráfico en red.

El profesional - certificaciones:

- Certificaciones: CISA, CISM, CISSP, CDPP, CCSK, CHFI, CEH, DLP, IRM, GIAC, LOPD, SOX, PCI, LEAD AUDITOR CCNA, CCNP, ISO 27001, etc.
- Securización y virtualización de sistemas: UNIX, LINUX, WINDOWS, MAINFRAME.
- Metodologías: OSSTMM, ISSAF.
- Fundaciones: OWASP.
- Tecnologías: FIREWALLS, IDS/IPS, SIEM, DLP, ntimalware solutions, VPNS, CISCO.

Dónde tener en cuenta la seguridad?



Redes Informáticas

Direccionamiento en redes IP

Agotamiento de IPV4

Agotamiento de direcciones Situación actual

- La situación actual es la siguiente:

1. El organismo internacional de primer nivel, la IANA (Internet Assigned Numbers Authority), repartió el último bloque libre en enero de 2011.
2. La IANA reparte los bloques a los proveedores regionales, los RIR (Regional Internet Registry), que son cinco a nivel mundial: APNIC (Asia-Pacific Network Information Centre), RIPE NCC (Réseaux IP Européens Network Coordination Centre), **LACNIC** (Latin America and Caribbean Network Information Centre), ARIN (American Registry for Internet Numbers) y AFRINIC (African Network Information Center).
3. De esos cinco proveedores regionales, cuatro han repartido ya todos sus bloques, por lo que actualmente sólo AFRINIC tiene bloques disponibles para repartir.

Agotamiento de direcciones LACNIC

4

Fases de Agotamiento de IPv4

- **Fase 0**

  Esta fase comenzó en Octubre de 2013 y se asignaron recursos IPv4 hasta haber alcanzado el último /9 disponible.

- **Fase 1**

  Esta fase comenzó el 19 de Mayo de 2014 y se asignaron recursos IPv4 hasta haber alcanzado el bloque /10 reservado para la fase de agotamiento gradual.

- **Fase 2**

  Esta fase comenzó el 10 de Junio de 2014 y se asignaron recursos IPv4 hasta agotar el /10 reservado para la fase 2.

- **Fase 3**

  Esta reserva es el último espacio disponible de LACNIC. Está compuesto por bloques IPv4 post agotamiento asignado por la IANA, junto a bloques recuperados y devueltos. El pasado 19 de Agosto de 2020, LACNIC agotó su pool de direcciones IPv4, contando actualmente sólo con recursos recuperados y devueltos y una reserva destinada exclusivamente a infraestructura crítica.

Agotamiento de direcciones LACNIC cont.

https://www.lacnic.net/1001/1/lacnic/fases-de-agotamiento-de-ipv4

Agotamiento de IPv4: LACNIC asignó el último bloque *19 de agosto 2020*

- El Registro de Direcciones de Internet de América Latina y Caribe (LACNIC) anuncia que hoy ha otorgado la reserva del último bloque disponible de direcciones IPv4.
- Durante esta última fase, que comenzó en febrero 2017, LACNIC y los NIRs asignaron más de 5,6 millones de direcciones IPv4. El proceso de agotamiento ha sido implementado de acuerdo a las políticas definidas por la comunidad y debidamente informado en distintas instancias.

Agotamiento de direcciones LACNIC

Fases de Agotamiento de IPv4

6

Lista de espera para recibir direcciones IPv4

- La lista de espera se creó el 19 agosto del 2020 cuando se asignó el último bloque disponible de direcciones IPv4 y tiene como objetivo generar un orden entre las organizaciones que solicitan direcciones IPv4.
- De acuerdo al comportamiento que ha tenido la recuperación de recursos, se estima que la última solicitud de la lista de espera IPv4 recibirá recursos en **2029** y únicamente podrán recibir un **máximo de 1.024** direcciones IPv4.*
- **Es importante aclarar que la fecha - anteriormente mencionada- no es exacta y puede variar, ya que es una estimación en base a la información histórica. No es posible saber con exactitud la cantidad de bloques IPv4 que se recuperarán en los próximos meses.*
- El aumento en el tiempo de espera se da porque hay cada vez más solicitudes de las que se pueden atender con el espacio recuperado o devuelto a LACNIC.
- Las organizaciones que hoy están recibiendo direcciones del espacio recuperado debieron esperar en promedio unos 805 días.

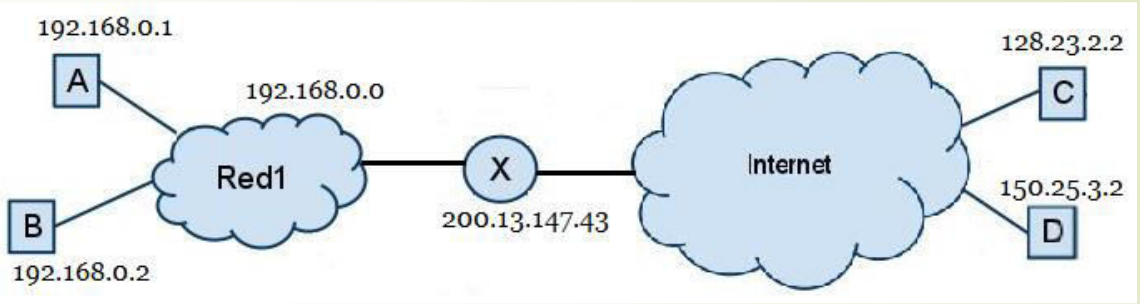
Agotamiento de direcciones Paliativos o parches ☺

Las más significativas son las siguientes:

- **NAT (Network Adress Translation):** Es la utilización de direcciones privadas para las redes internas y la reserva de las direcciones IPs públicas sólo para el dispositivo que está conectado a Internet.
- **CIDR (Classless Inter-Domain Routing):** Dividir los bloques de direcciones IPs, dejando de utilizar las clases en Internet, ya que antiguamente los bloques eran muy grandes, de 8, 16 o 24 bits. Con esto se pasa a la utilización de bloques de cualquier tamaño en bits sin ningún tipo de problema.
- **CGNAT (Carrier Grade NAT):** Este parche es mucho más reciente y no es más que una ampliación del mecanismo NAT, llevado al siguiente nivel. Lo que hace es los usuarios de Internet tengamos en nuestro ámbito un dispositivo con direccionamiento IP privada, que es el router, que tiene un direccionamiento IP privada interno, pero su dirección IP externa no es una dirección IP publica, sino una dirección IP de un rango nuevo, llamado CGNAT, que hace que esté a su vez en otra dirección privada, en este caso del proveedor, y que un dispositivo del mismo sea la que tenga la dirección IPv4 publica.

Agotamiento de direcciones NAT/PAT

- Network Address Translation (NAT) o Traducción de Direcciones de Red es una técnica que modifica la información de dirección IP en la cabecera de un paquete IP mientras el mismo es transmitido de una red a otra por medio de un router o similar.



Dirección Emisor	Dirección Pública	Dirección Receptor
192.168.0.1	200.13.147.43	128.23.2.2
192.168.0.2	200.13.147.43	150.25.3.2

Agotamiento de direcciones Tipos de NAT

- **Traducción estática de direcciones (NAT estática)**: asignación de direcciones uno a uno entre una dirección local y una global.
- **Traducción dinámica de direcciones (NAT dinámica)**: asignación de varias direcciones a varias direcciones entre direcciones locales y globales.
- **Traducción de la dirección del puerto (PAT)**: asignación de varias direcciones a una dirección entre direcciones locales y globales. Este método también se conoce como "sobrecarga" (NAT con sobrecarga).

Agotamiento de direcciones NAT estático

- **NAT estático**
- La NAT estática consiste en una asignación uno a uno entre direcciones locales y globales. Estas asignaciones son configuradas por el administrador de red y se mantienen constantes.
- En la ilustración, el R2 se configuró con las asignaciones estáticas para las direcciones locales internas del Svr1, la PC2 y la PC3. Cuando estos dispositivos envían tráfico a Internet, sus direcciones locales internas se traducen a las direcciones globales internas configuradas. Para las redes externas, estos dispositivos tienen direcciones IPv4 públicas.
- La NAT estática resulta útil, en especial para los servidores web o los dispositivos que deben tener una dirección constante que sea accesible tanto desde Internet, como desde el servidor web de una empresa.
- También es útil para los dispositivos a los que debe poder acceder el personal autorizado cuando no está en su lugar de trabajo, pero no el público en general en Internet.
- Por ejemplo, un administrador de red puede acceder a la dirección global interna del Svr1 (209.165.200.226) desde la PC4 mediante SSH. El R2 traduce esta dirección global interna a la dirección local interna y conecta la sesión del administrador al Svr1.
- La NAT estática requiere que haya suficientes direcciones públicas disponibles para satisfacer la cantidad total de sesiones de usuario simultáneas.

Agotamiento de direcciones NAT estático

- Consiste en una asignación **uno a uno** entre direcciones locales y globales. Estas son configuradas por el administrador de red y se mantienen fijas.

Conjunto de NAT para IPv4

Dirección local interna	Conjunto de direcciones globales internas: direcciones a las que se puede llegar a través del R2
192.168.10.12	209.165.200.226
Disponibles	209.165.200.227
Disponibles	209.165.200.228
Disponibles	209.165.200.229
Disponibles	209.165.200.230

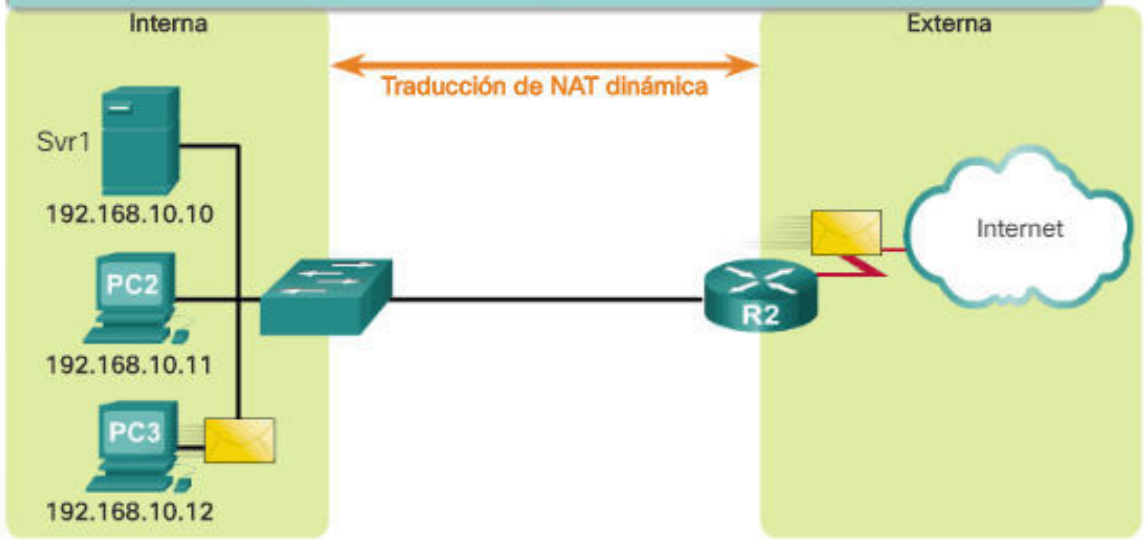


Imagen 2: NAT dinámica

Agotamiento de direcciones NAT dinámico

- La NAT dinámica utiliza un conjunto de direcciones públicas y las asigna según el orden de llegada.
- Cuando un dispositivo interno solicita acceso a una red externa, la NAT dinámica asigna una dirección IPv4 pública disponible del conjunto.
- En la ilustración, la PC3 accede a Internet mediante la primera dirección disponible del conjunto de NAT dinámica.
- Las demás direcciones siguen disponibles para utilizarlas.
- Al igual que la NAT estática, la NAT dinámica requiere que haya suficientes direcciones públicas disponibles para satisfacer la cantidad total de sesiones de usuario simultáneas.

Agotamiento de direcciones NAT dinámico

- La NAT dinámica utiliza un conjunto de direcciones públicas y las asigna según el orden de llegada. Cuando un dispositivo interno solicita acceso a una red externa, la NAT dinámica asigna una dirección IPv4 pública disponible del conjunto.

Dirección local interna	Conjunto de direcciones globales internas: direcciones a las que se puede llegar a través del R2
192.168.10.12	209.165.200.226
Disponibles	209.165.200.227
Disponibles	209.165.200.228
Disponibles	209.165.200.229
Disponibles	209.165.200.230

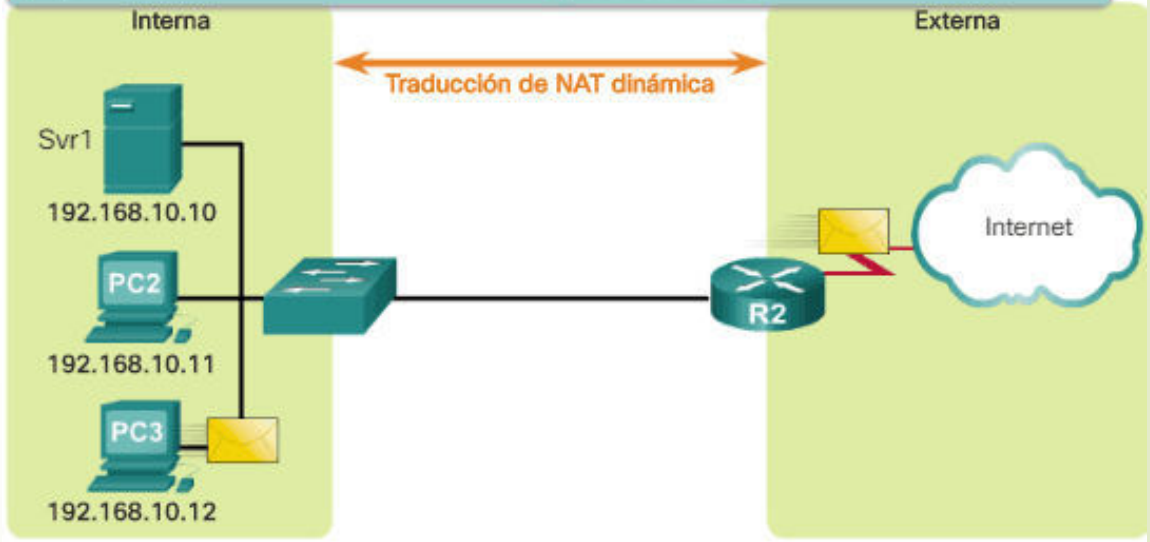
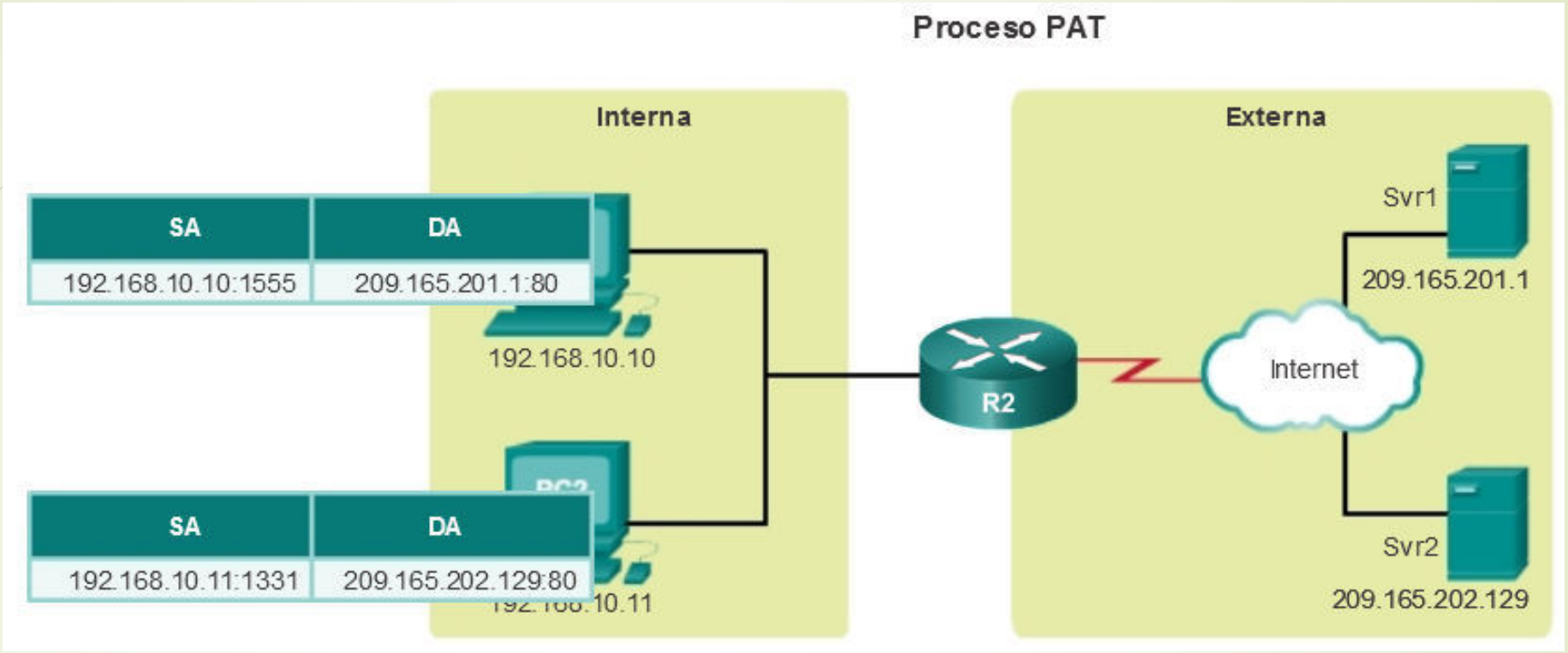


Imagen 2: NAT dinámica

Agotamiento de direcciones PAT Port Address Translation

- PAT, también conocida como “NAT con sobrecarga”, asigna varias direcciones IPv4 privadas a una única dirección IPv4 pública o a algunas direcciones.
- Esto es lo que hace la mayoría de los routers domésticos.
- El ISP asigna una dirección al router, no obstante, varios miembros del hogar pueden acceder a Internet de manera simultánea. Esta es la forma más común de NAT.
- Con PAT, se pueden asignar varias direcciones a una o más direcciones, debido a que cada dirección privada también se rastrea con un número de puerto.
- Cuando un dispositivo inicia una sesión TCP/IP, genera un valor de puerto de origen TCP o UDP para identificar la sesión de forma exclusiva.
- Cuando el router NAT recibe un paquete del cliente, utiliza su número de puerto de origen para identificar de forma exclusiva la traducción NAT específica.
- PAT garantiza que los dispositivos usen un número de puerto TCP distinto para cada sesión con un servidor en Internet.

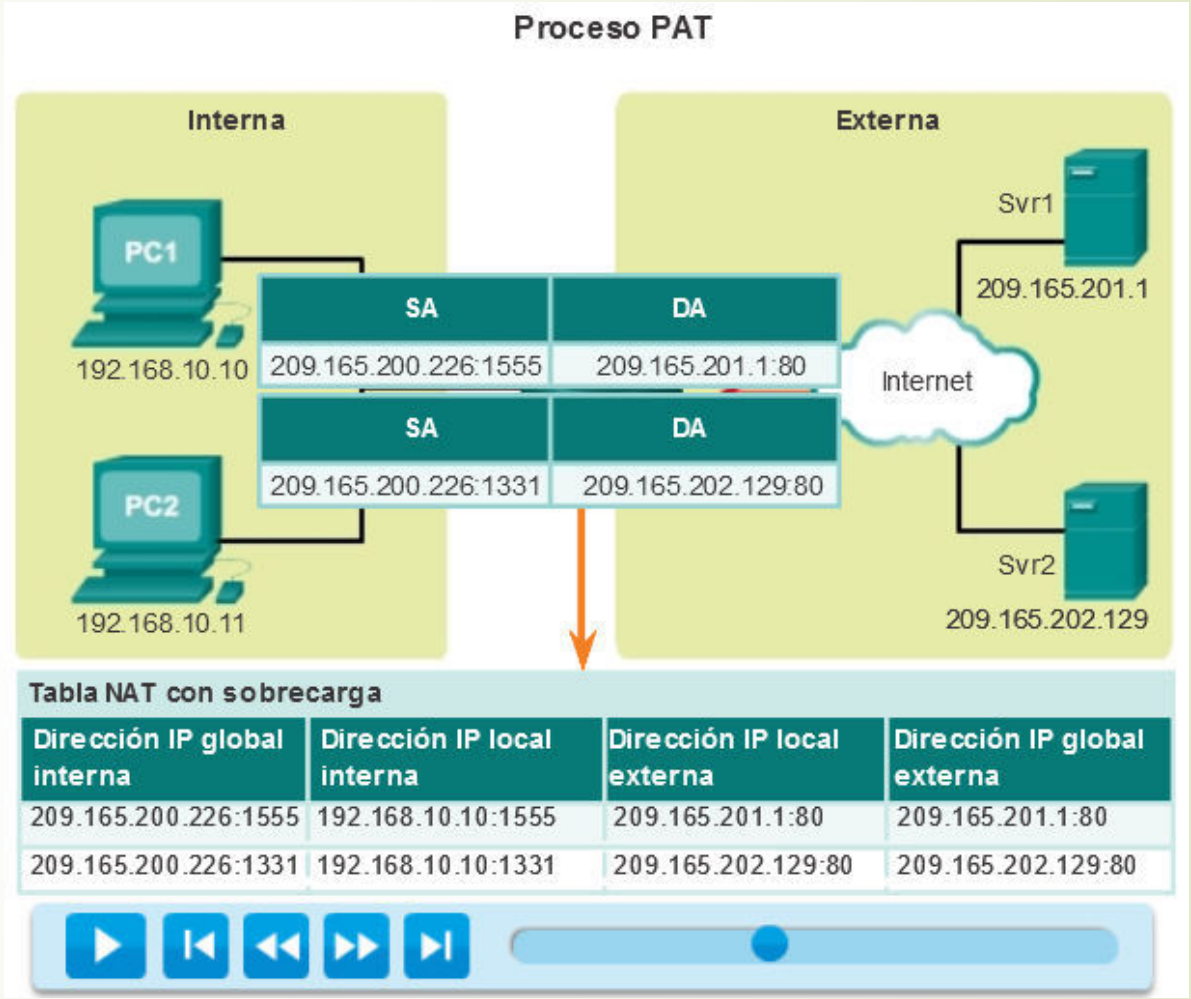


Agotamiento de direcciones PAT **P**ort **A**ddress **T**ranslation

Agotamiento de direcciones PAT **P**ort **A**ddress **T**ranslation

- Cuando llega una respuesta del servidor, el número de puerto de origen, que se convierte en el número de puerto de destino en la devolución, determina a qué dispositivo el router reenvía los paquetes.
- El proceso de PAT también valida que los paquetes entrantes se hayan solicitado, lo que añade un grado de seguridad a la sesión.
- A medida que el R2 procesa cada paquete, utiliza un número de puerto (**1331 y 1555**, en este ejemplo) para identificar el dispositivo en el que se originó el paquete.
- La dirección de origen (SA) es la dirección local interna a la que se agregó el número de puerto TCP/IP asignado. La dirección de destino (DA) es la dirección local externa a la que se agregó el número de puerto de servicio.
- En este ejemplo, el puerto de servicio es **80, que es HTTP**.
- Para la dirección de origen, el R2 traduce la dirección local interna a una dirección global interna con el número de puerto agregado.

Agotamiento de direcciones PAT **P**ort **A**ddress **T**ranslation



Agotamiento de direcciones
PAT **P**ort **A**ddress **T**ranslation

- La dirección de destino no se modifica, pero ahora se la denomina “dirección IP global externa”.
- Cuando el servidor web responde, se invierte la ruta.

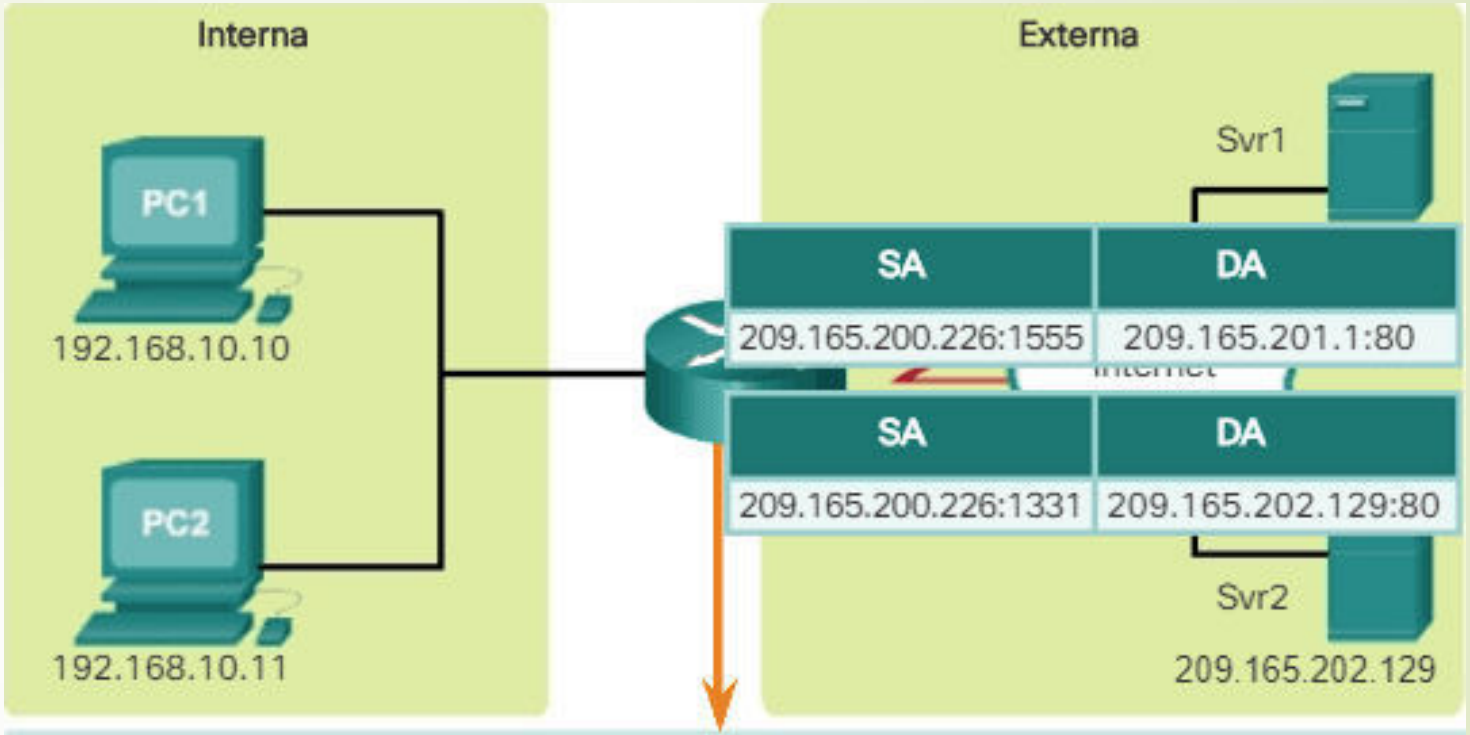


Tabla NAT con sobrecarga

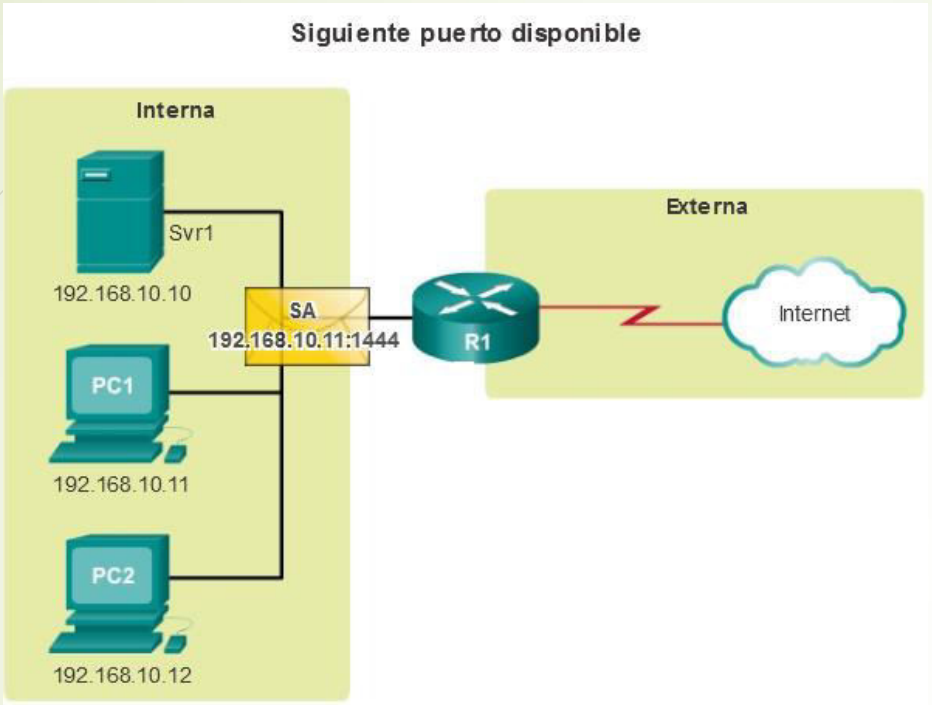
Dirección IP global interna	Dirección IP local interna	Dirección IP local externa	Dirección IP global externa
209.165.200.226:1555	192.168.10.10:1555	209.165.201.1:80	209.165.201.1:80
209.165.200.226:1331	192.168.10.10:1331	209.165.202.129:80	209.165.202.129:80

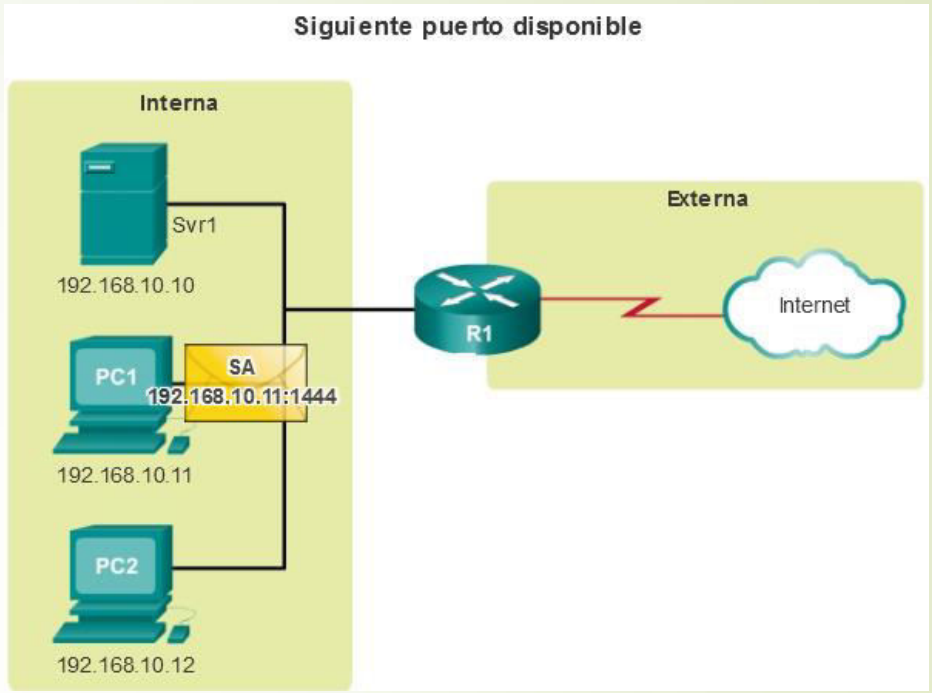
Imagen 3: Traducción de la dirección del puerto (PAT)

Agotamiento de direcciones PAT **P**ort **A**ddress **T**ranslation

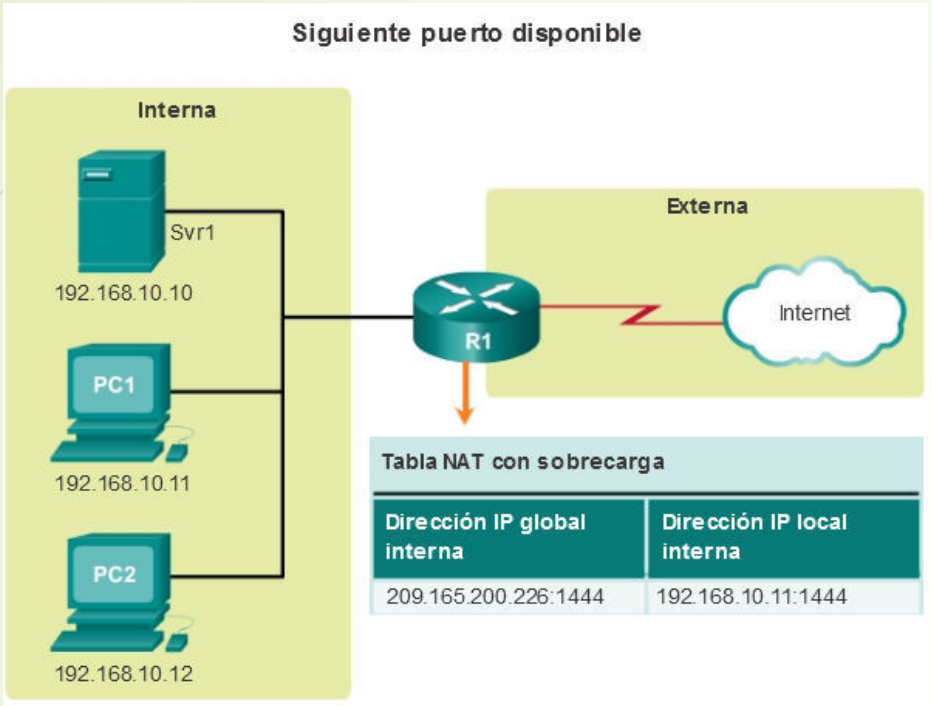
Siguiente puerto disponible

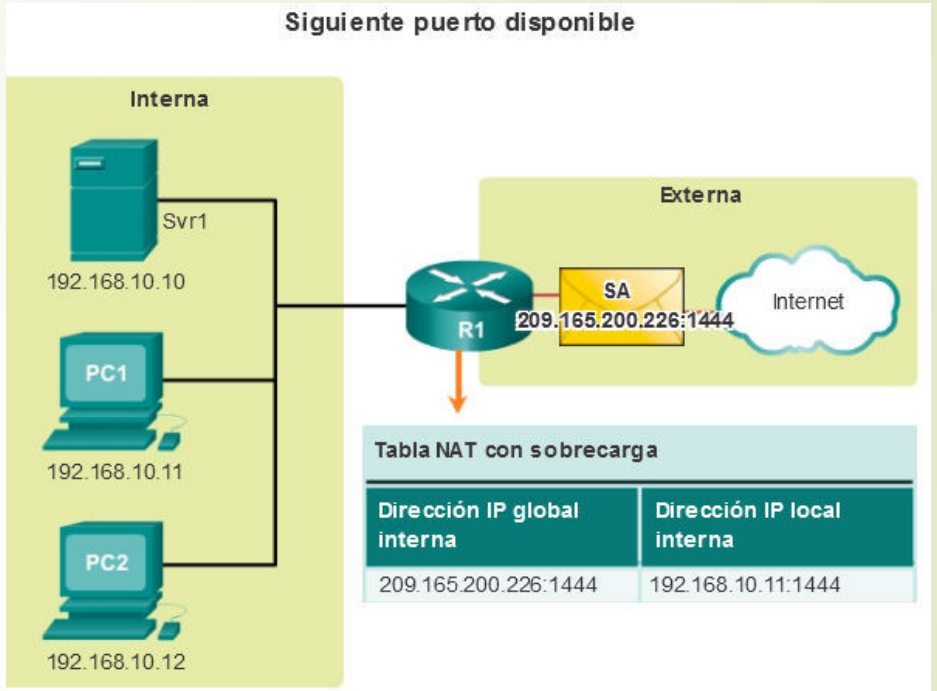
- En el ejemplo anterior, los números de puerto del cliente, 1331 y 1555, no se modificaron en el router con NAT habilitada.
- Esta no es una situación muy probable, porque existe una gran posibilidad de que estos números de puerto ya se hayan conectado a otras sesiones activas.
- PAT intenta conservar el puerto de origen inicial. Sin embargo, si el puerto de origen inicial ya está en uso, PAT asigna el primer número de puerto disponible desde el comienzo del grupo de puertos correspondiente de 0 a 511, 512 a 1023 o 1024 a 65535.
- Cuando no hay más puertos disponibles y hay más de una dirección externa en el conjunto de direcciones, PAT avanza a la siguiente dirección para intentar asignar el puerto de origen inicial.
- Este proceso continúa hasta que no haya más direcciones IP externas o puertos disponibles.





Agotamiento de direcciones PAT **P**ort **A**ddress **T**ranslation



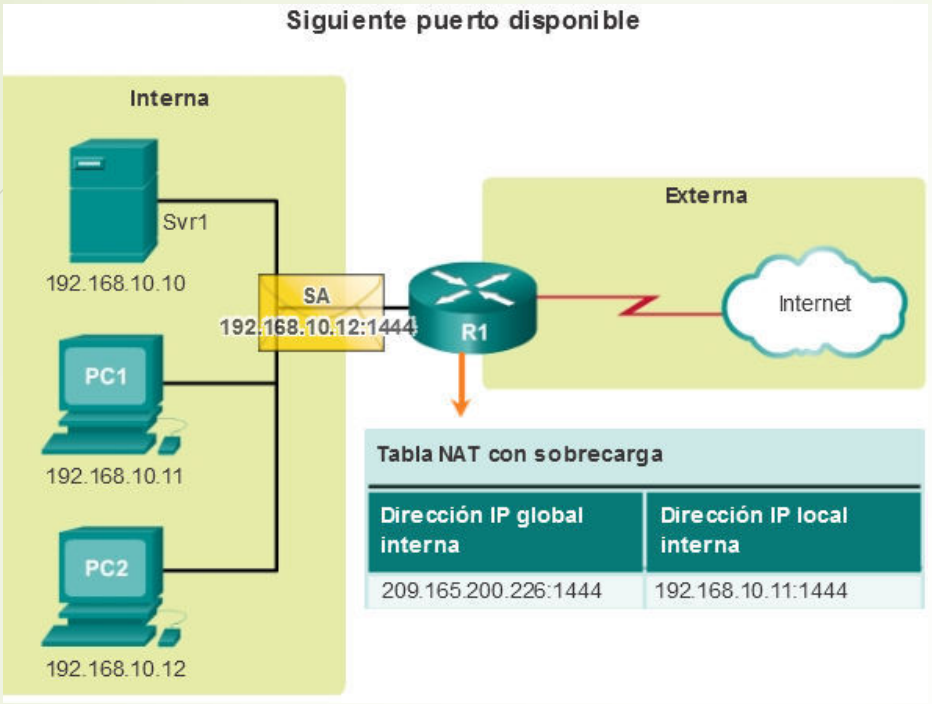


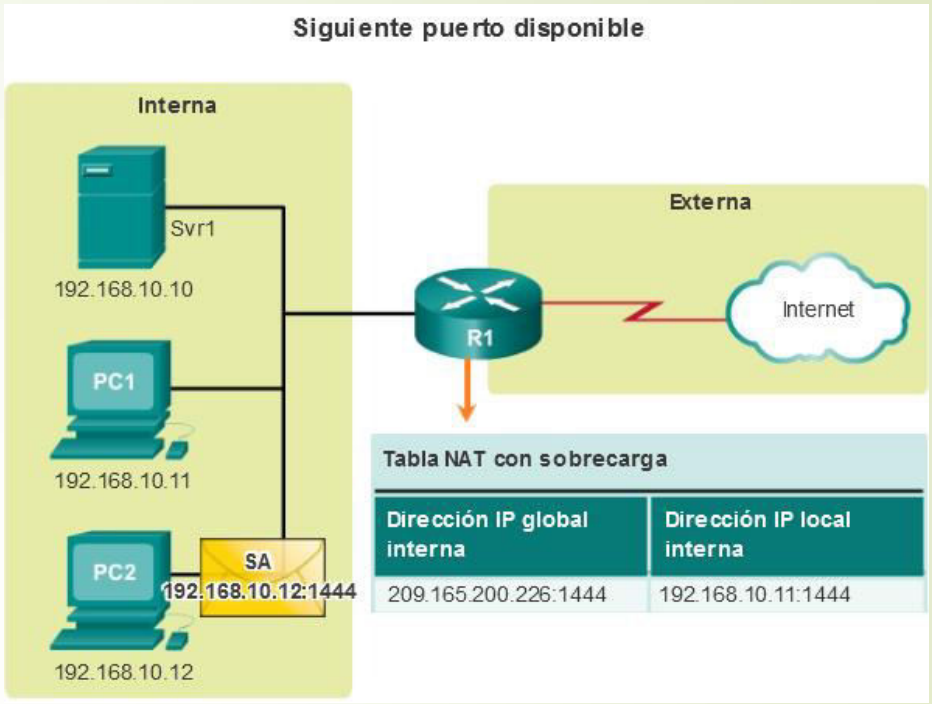
Agotamiento de direcciones PAT **P**ort **A**ddress **T**ranslation

Agotamiento de direcciones PAT **P**ort **A**ddress **T**ranslation

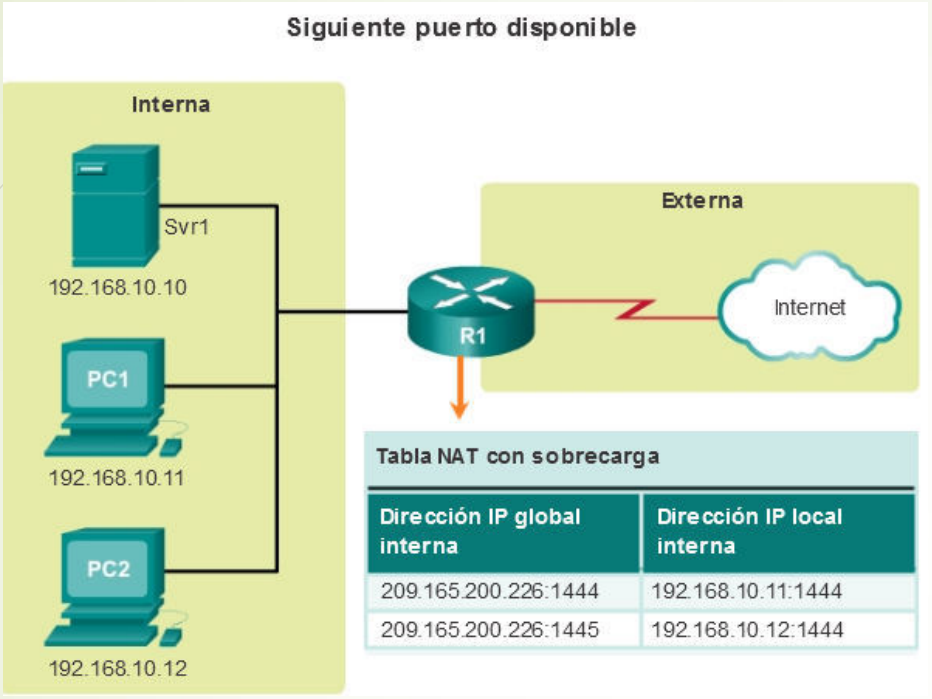
Siguiente puerto disponible

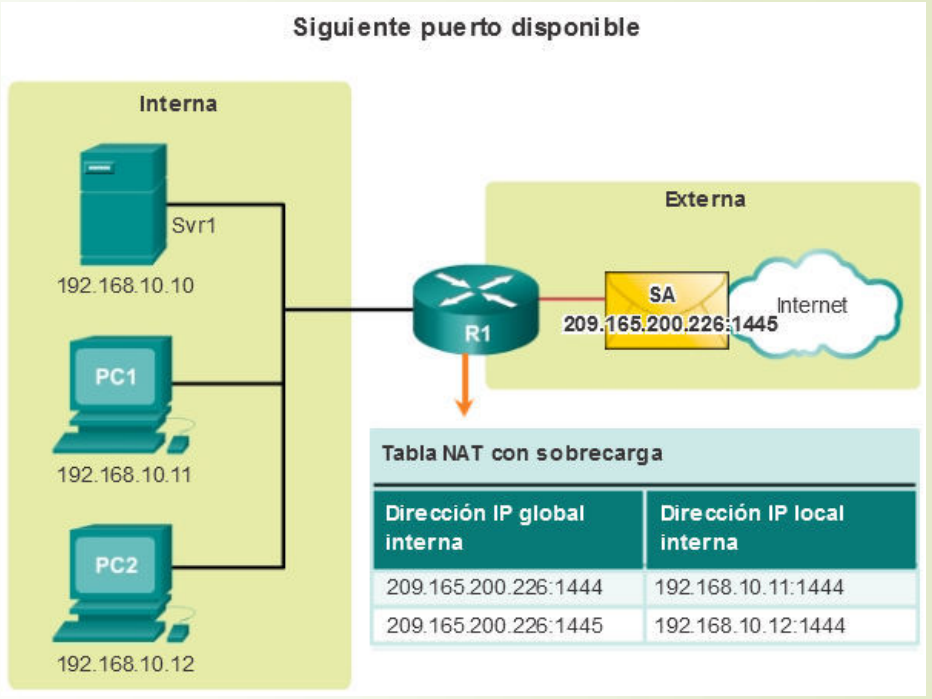
- Los hosts eligieron el mismo número de puerto **1444**. Esto resulta aceptable para la dirección interna, porque los hosts tienen direcciones IP privadas únicas.
- Sin embargo, en el router NAT, se deben cambiar los números de puerto; de lo contrario, los paquetes de dos hosts distintos saldrían del R2 con la misma dirección de origen.
- En este ejemplo, PAT asignó el siguiente puerto disponible (**1445**) a la segunda dirección host.





Agotamiento de direcciones PAT **P**ort **A**ddress **T**ranslation





Agotamiento de direcciones PAT **P**ort **A**ddress **T**ranslation

Agotamiento de direcciones NAT y PAT Comparación

- NAT traduce direcciones IPv4 en una relación de 1:1 entre direcciones IPv4 privadas y direcciones IPv4 públicas.
- PAT modifica la dirección y el número de puerto.
- NAT reenvía los paquetes entrantes a su destino interno mediante la dirección IPv4 de origen de entrada proporcionada por el host en la red pública.
- PAT hay solo una o muy pocas direcciones IPv4 públicamente expuestas.
- Los paquetes entrantes de la red pública se enrutan a sus destinos en la red privada consultando una tabla en el router NAT.
- Esta tabla hace un seguimiento de los pares de puertos públicos y privados. Esto se denomina “seguimiento de conexiones”.

Agotamiento de direcciones NAT y PAT Comparación

- **Paquetes sin segmento de capa 4**
- ¿Qué sucede con los paquetes IPv4 que transportan datos que no son segmentos TCP o UDP? Estos paquetes no contienen un número de puerto de capa 4.
- PAT traduce la mayoría de los protocolos comunes transmitidos mediante IPv4 que no utilizan TCP o UDP como protocolo de la capa de transporte.
- El más común de ellos es **ICMPv4**.
- PAT maneja cada uno de estos tipos de protocolos de manera diferente.
- Por ejemplo, los mensajes de consulta, las solicitudes de eco y las respuestas de eco de ICMPv4 incluyen una ID de consulta.
- ICMPv4 utiliza la ID de consulta para identificar una solicitud de eco con su respectiva respuesta. La ID de consulta aumenta con cada solicitud de eco enviada.
- PAT utiliza la ID de consulta en lugar de un número de puerto de capa 4.
- **Nota:** otros mensajes ICMPv4 no utilizan la ID de consulta. Estos mensajes y otros protocolos que no utilizan los números de puerto TCP o UDP varían y exceden el ámbito de

Agotamiento de direcciones NAT y PAT Comparación

- **Ejemplo de ICMP en un router Huawei**

- [HUAWEI_HOME]dis nat session protocol icmp
- NAT Session Table Information:
- Protocol : ICMP(1)
- SrcAddr Vpn : 192.168.15.2
- DestAddr Vpn : 4.2.2.2
- Type Code IcmpId : 8 0 3
- NAT-Info
- New SrcAddr : 192.168.111.5
- New DestAddr : ----
- New **IcmpId : 14105**

- Total : 1

Agotamiento de direcciones NAT y PAT Comparación

NAT

Conjunto de direcciones globales internas	Dirección local interna
209.165.200.226	192.168.10.10
209.165.200.227	192.168.10.11
209.165.200.228	192.168.10.12
209.165.200.229	192.168.10.13

PAT

Dirección global interna	Dirección local interna
209.165.200.226:1444	192.168.10.10:1444
209.165.200.226:1445	192.168.10.11:1444
209.165.200.226:1555	192.168.10.12:1555
209.165.200.226:1556	192.168.10.13:1555

ComparaciÓn entre NAT y PAT

Agotamiento de direcciones Ventajas y desventajas NAT

Ventajas

- **Conserva el esquema de direccionamiento legalmente registrado al permitir la privatización de las intranets**. NAT **PAT** conserva las direcciones mediante la multiplexación de aplicaciones en el nivel de puerto.
-
- **Aumenta la flexibilidad de las conexiones a la red pública**. Enmascara la red interna detrás de una sola IP.
- **Optimiza la demanda de IP públicas**. Ya que con una IP puede salir una corporación entera a Internet.
- I**ndependencia de direccionamiento interno**. Los costos de redireccionamiento de hosts pueden ser considerables. NAT permite mantener el esquema de direcciones IPv4 privadas existente a la vez que facilita el cambio a un nuevo esquema de direccionamiento público. Esto significa que una organización podría cambiar los ISP sin necesidad de modificar ninguno de sus clientes internos.

Agotamiento de direcciones Ventajas y desventajas NAT

Desventajas

- **Protocolos con problemas:** Hay aplicaciones que no soportan funcionar con NAT. Ejm. Túneles GRE y algunas aplicaciones seguras.

- **Trazabilidad**. Se complica el diagnóstico de aplicaciones ya que si se traslada por puerto, hay que usar un analizador de protocolos (Wireshark)

- **Servicios entrantes**. Dificulta la posibilidad de dar brindar servicios que entren desde Internet.

- **Direcciones públicas**: Tanto el NAT estático como el dinámico **No** son beneficiosas en cuando al ahorro de direcciones, ya que siempre trasladan uno a uno.

- El único que ahorra direcciones es el **PAT,** ya que una IP se enmascara toda una red detrás.

Agotamiento de direcciones IPv6

Mejoras:

- Direccionamiento
  - Más espacio
  - Mayor flexibilidad – encabezados opcionales
  - Modos de estructurar los bits
- Formato de cabecera simplificado
- Capacidad de QoS
- Seguridad
- Soporte para paquetes de gran tamaño (+64Kbytes)
- Fragmentación solo en origen
- Campo de suma de comprobación eliminado
- Incremento en eficiencia de procesado de paquetes, por disponer de cabecera fija (relativo)

Agotamiento de direcciones IPv6 vs IPV4 Comparación

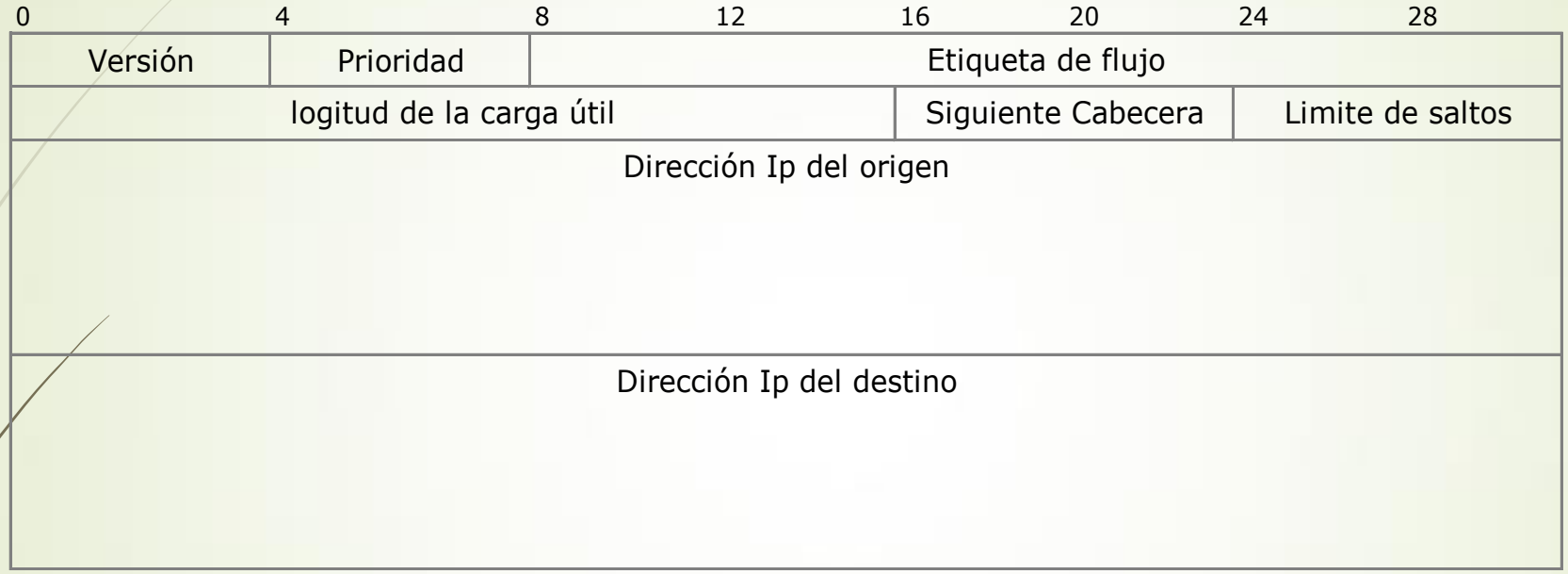
- **IPv4** soporta 4,294,967,296 (2^{32}) direcciones que es poco menos de 4.3 billones

  4 bytes = 8bits * 4 = 32 ➔ 2^{32}

- **IPv6** ofrece 3.4 x 10^{38} (2^{128}) direcciones, un número similar a 6.67126144781401e+23 direcciones IP por cada metro cuadrado sobre la superficie de la Tierra

  16 bytes = 8bits * 16 = 128 ➔ 2^{128}

Agotamiento de direcciones
Cabecera IPv6



- Versión:6.
- Prioridad: Permite servicios diferenciados
- Etiqueta de Flujo: Identifica la QoS solicitada.
- Long. Carga útil: datos sin la cabecera (max 65535 bytes)
- Siguiente Cabecera: Identifica el tipo de cabecera que sigue
- Limite de Saltos: Ídem TTL

Agotamiento de direcciones
Extensión de cabecera

Cabecera IPv6	40 octetos
Cabecera opciones de Salto	Variable
Cabecera de encaminamiento	Variable
Cabecera de fragmentación	8 octetos
Cabecera de autenticación	Variable
Cabecera de encapsulado de seguridad de la caga util	Variable
Cabecera de opciones de destino	Variable
Cabecera TCP	20 octetos mi
Datos de aplicación	Variable

- Permiten suministrar funciones adicionales a las que posee la cabecera basica.
- Ídem campo opciones en IPv4
- Se encadenan mediante el campo cabecera siguiente

Ejercicios de NAT

Seguridad en Informática - Módulo 3

Docente: Carlos Cagnani

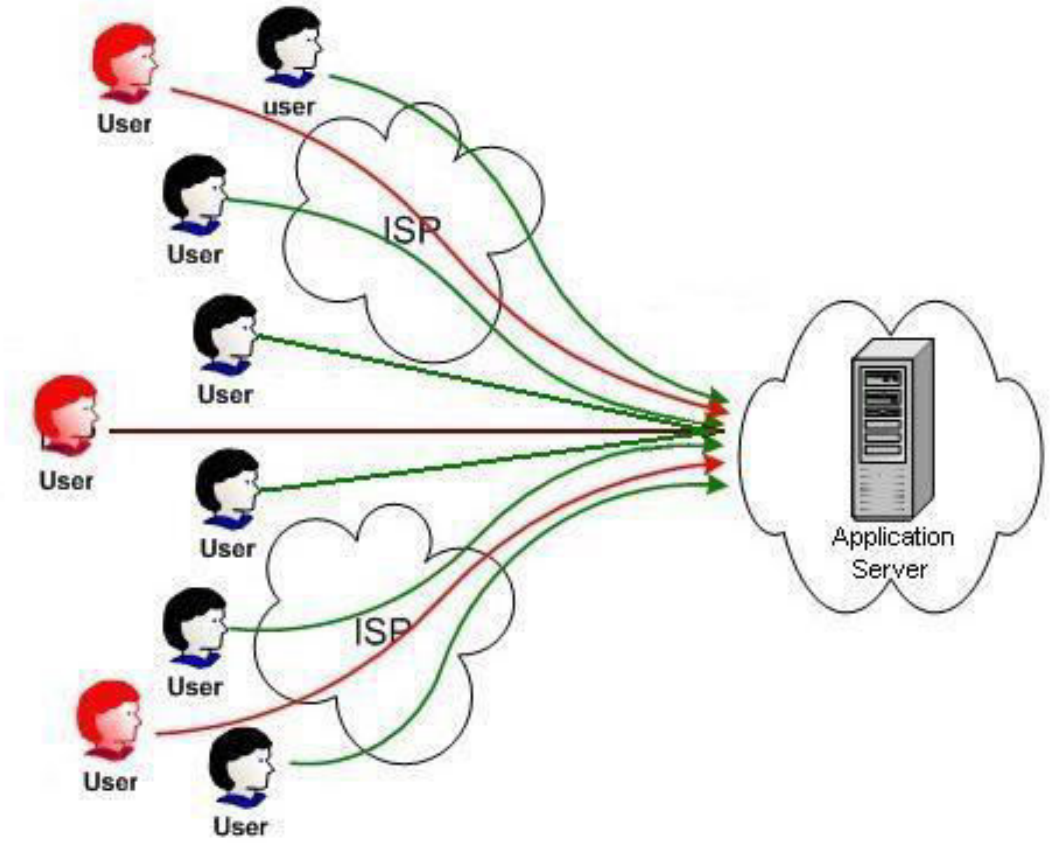
*Este documento fue realizado en concepto de capacitación en Formación Profesional y dictada para el **Sindicato CePETel** a contar del mes de mayo del año 2023.*

Seguridad en Sistemas

CLASE 3

Índice de temas

Gestión Estratégica en Seguridad de la Información



Algunos Escenarios

Caso A:

- La última aplicación estratégica del portal B2C, desarrollada en un tiempo récord (para cumplir con el mínimo *time to market* que Marketing imprime a toda la organización), ve afectada su **disponibilidad**. ¿Cómo no se tuvo en cuenta el ancho de banda que requerían las 100.000 peticiones concurrentes de los usuarios en el día de su lanzamiento oficial?

Algunos Escenarios

Caso B:

- Un “hacker” consigue la lista de tarjetas de crédito de cientos de clientes de una compañía de e-commerce, merced a la explotación de una vulnerabilidad de la aplicación de carrito de la compra. Problema de **confidencialidad**. Las pérdidas económicas y de imagen, unidas a la multa de la Dirección de Protección de Datos, forzaron el cierre de la empresa.

Algunos Escenarios

Caso C:

- El grupo de desarrollo de una compañía confunde el entorno de prueba con el de producción y pisa la BD de cliente real con la de testing. Problema de **Integridad**. Puede ocasionar la pérdida irrecuperable, si es que NO existe una política adecuada de backup de los originales.

- Otro caso de Integridad es el del redondeo de cuentas corrientes del Banco.

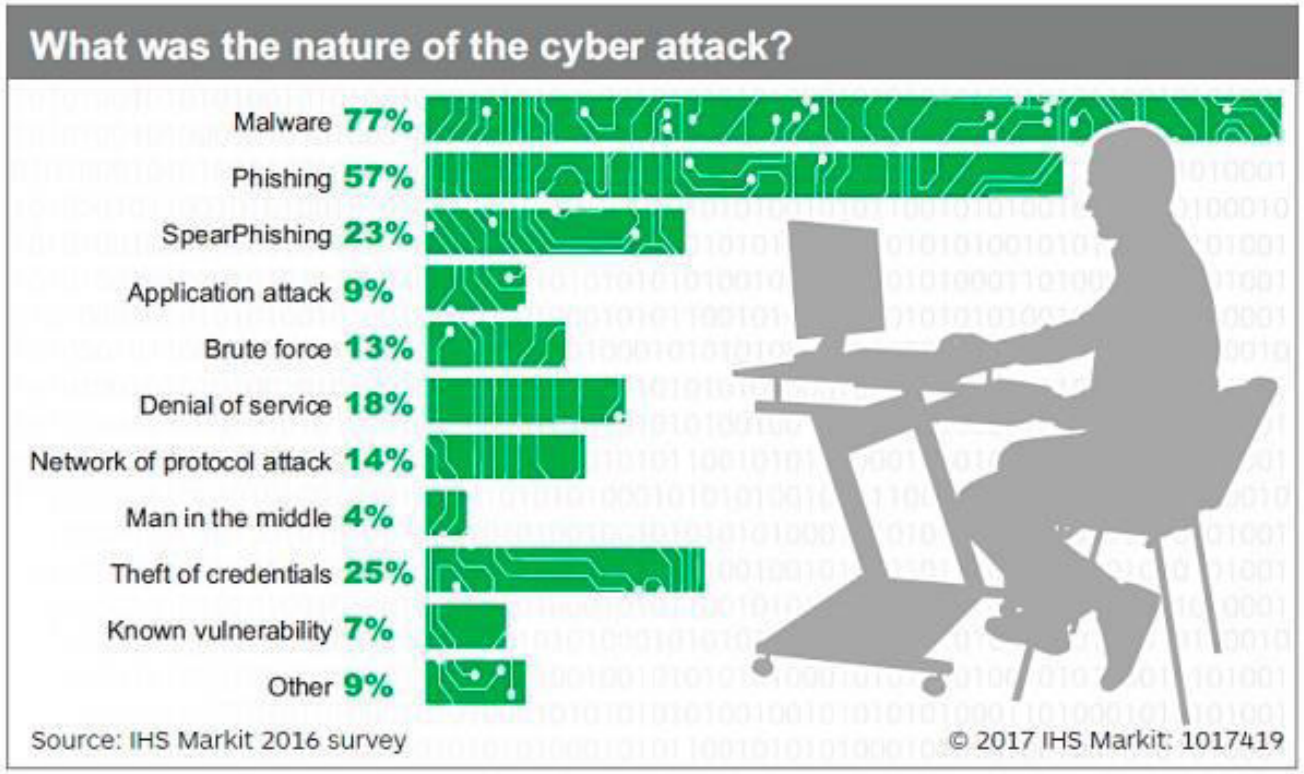
Gestión Estratégica en Seguridad de la Información

Ranking de ataques

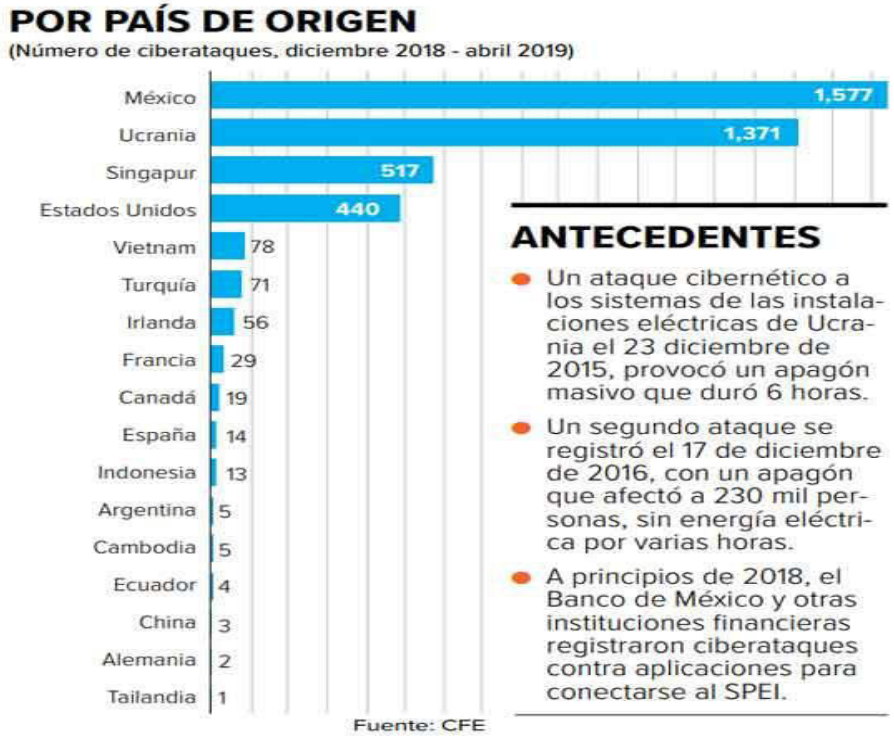
Top 10 most valuable information to cyber criminals	Top 10 biggest cyber threats to organizations
1. Customer information (17%)	1. Phishing (22%)
2. Financial information (12%)	2. Malware (20%)
3. Strategic plans (12%)	3. Cyberattacks (to disrupt) (13%)
4. Board member information (11%)	4. Cyberattacks (to steal money) (12%)
5. Customer passwords (11%)	5. Fraud (10%)
6. R&D information (9%)	6. Cyberattacks (to steal IP) (8%)
7. M&A information (8%)	7. Spam (6%)
8. Intellectual property (6%)	8. Internal attacks (5%)
9. Non-patented IP (5%)	9. Natural disasters (2%)
10. Supplier information (5%)	10. Espionage (2%)

Gestión Estratégica en Seguridad de la Información

Naturaleza de ataques



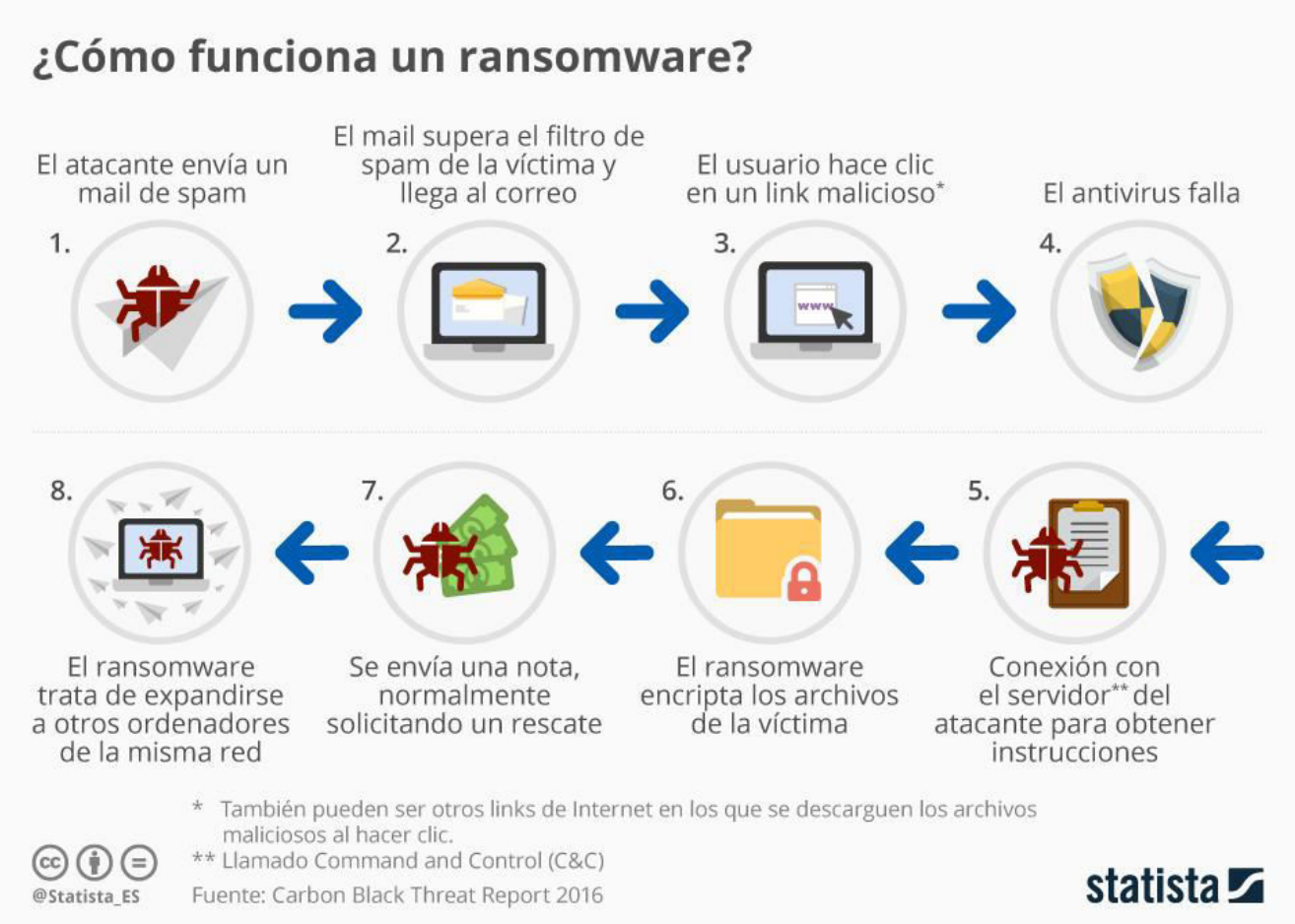
Fuentes



https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents

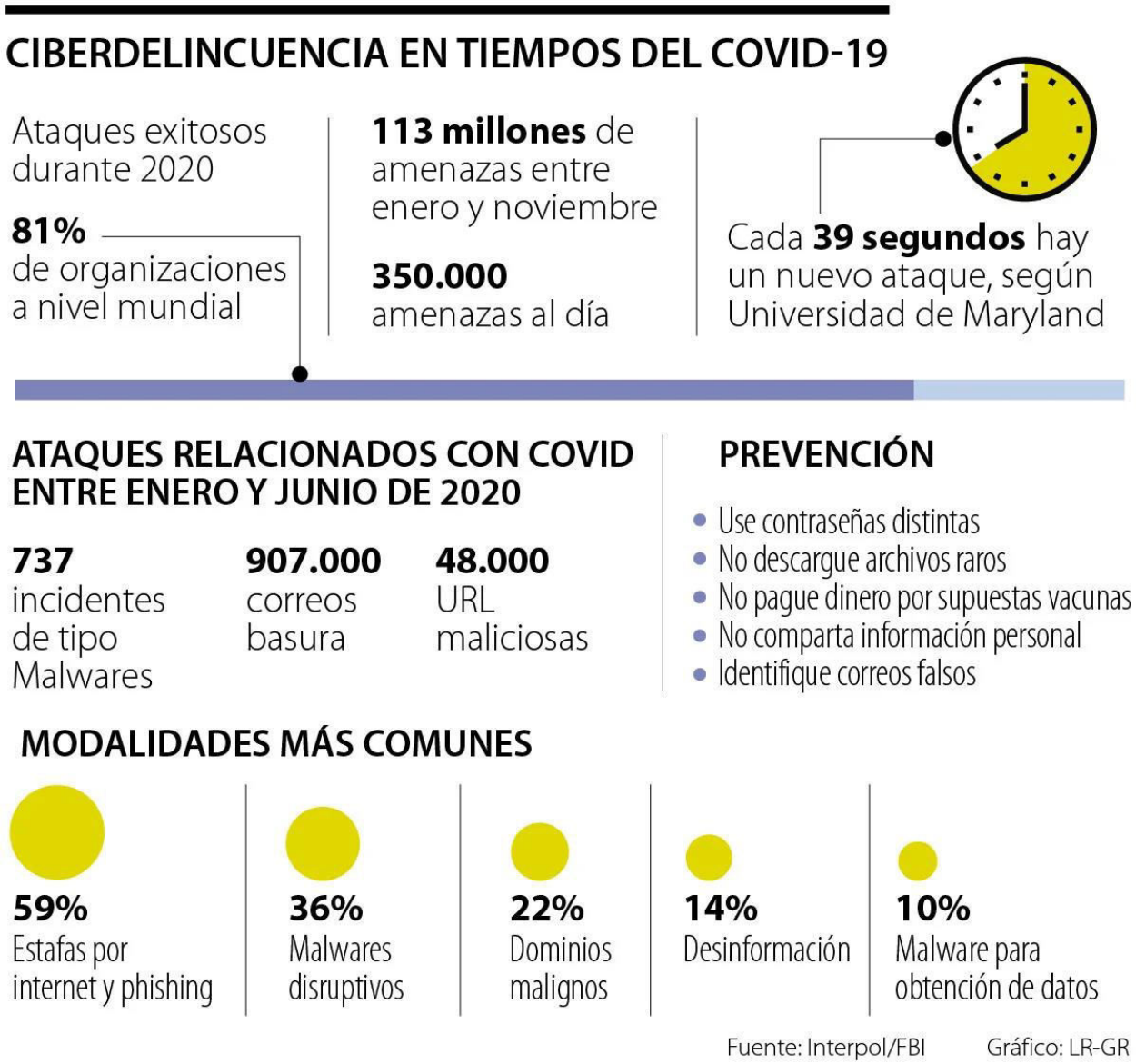
Gestión Estratégica en Seguridad de la Información

Ataques en COVID19



Gestión Estratégica en Seguridad de la Información

Detalles de los Ataques



Gestión Estratégica en Seguridad de la Información

Detalles de los Ataques

Figure 55 Functions Most Likely to Be Affected by a Public Breach

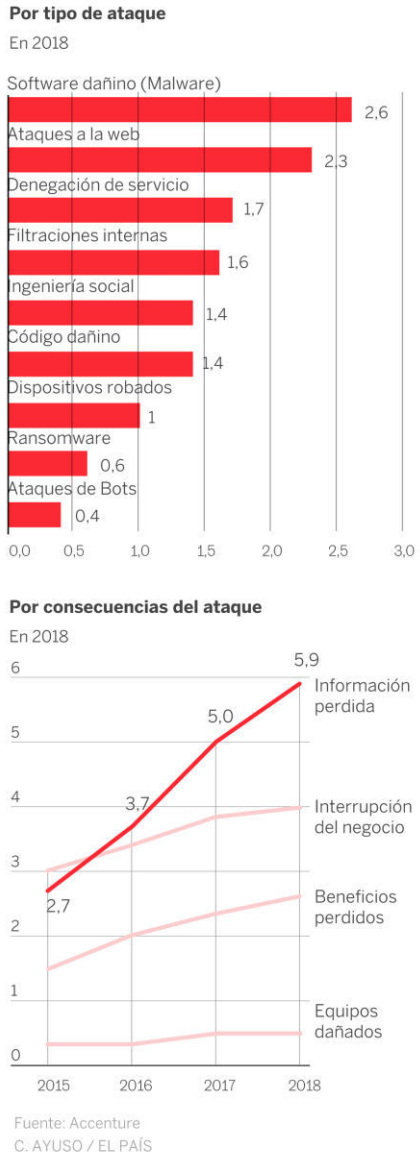
Source: Cisco Security Research

For more info visit: **www.cisco.com/go/acr2017**

cisco

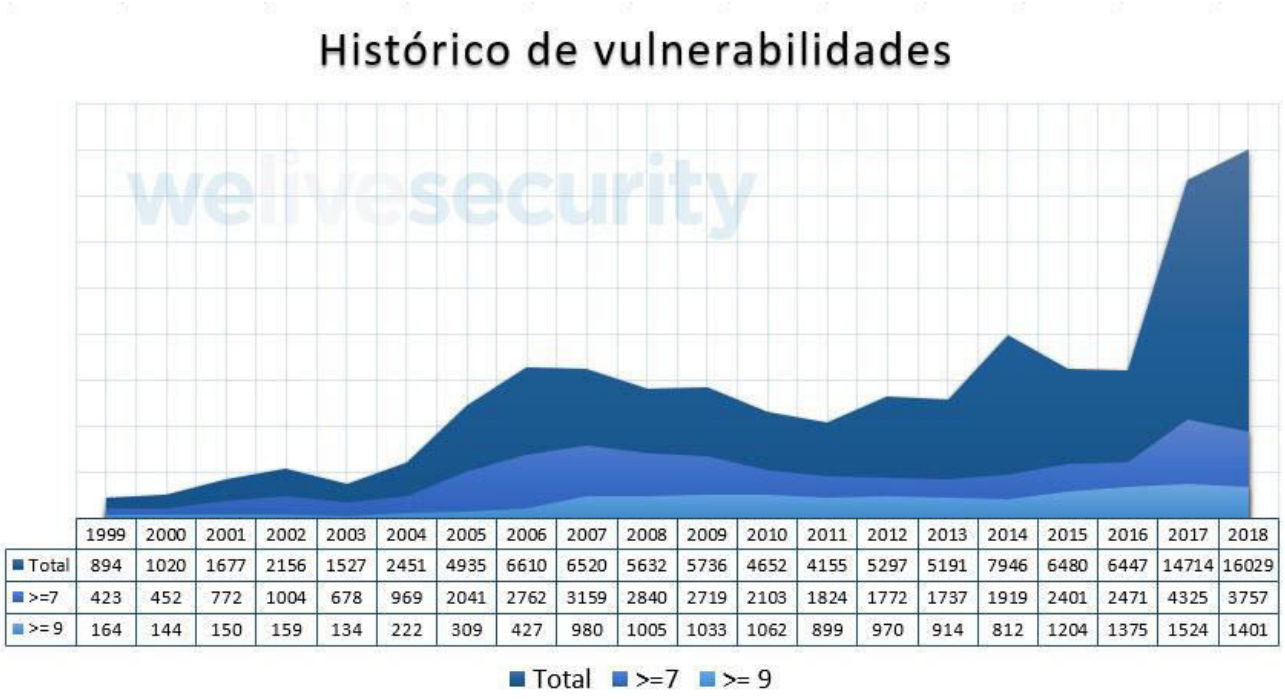
Gestión Estratégica en Seguridad de la Información

Distribución y Porcentaje de los Ataques



Gestión Estratégica en Seguridad de la Información

Vulnerabilidades Reportadas



	1999	2000	2001	2002	2003	2004	2005	2006	2007	2008	2009	2010	2011	2012	2013	2014	2015	2016	2017	2018
Total	894	1020	1677	2156	1527	2451	4935	6610	6520	5632	5736	4652	4155	5297	5191	7946	6480	6447	14714	16029
>=7	423	452	772	1004	678	969	2041	2762	3159	2840	2719	2103	1824	1772	1737	1919	2401	2471	4325	3757
>= 9	164	144	150	159	134	222	309	427	980	1005	1033	1062	899	970	914	812	1204	1375	1524	1401

Seguridad en Sistemas

El Problema

- Muchas de las aplicaciones se desarrollan sin tener en cuenta los criterios de seguridad y la integración con la arquitectura de seguridad global de la organización.

Las Causas

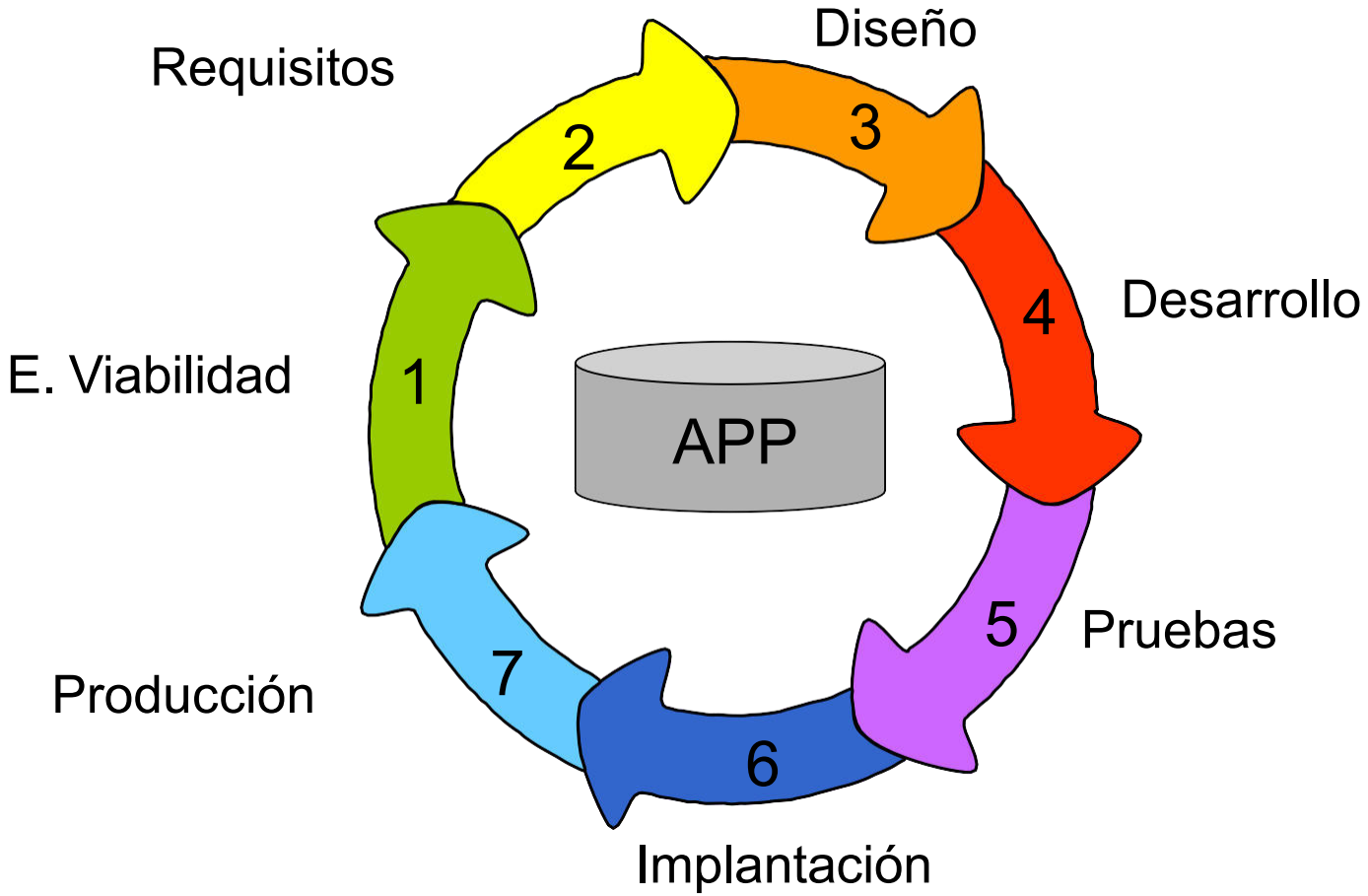
- Inexistencia de metodologías de desarrollo formales,
- Caso contrario: existencia de múltiples y variadas metodologías de desarrollo,
- Desconocimiento por parte de las áreas de desarrollo de las infraestructuras centralizadas de seguridad (autenticación, acceso, logs, etc),
- Mínimo “time to market” con el que se cuenta en muchos casos.
- Ámbito de actuación del responsable de seguridad, en muchos casos muy vinculado a las áreas de operación, sin potestad para la definición de normas de desarrollo obligatorias,
- Subcontratación generalizada de desarrollos de terceros, con sus propias metodologías y arquitecturas, lo que conlleva a una diversificación importante de cómo se ve la seguridad,
- Creer que la seguridad de los sistemas es una arquitectura de red fuertemente segmentada y una correcta aplicación de parches a los sistemas operativos y servidores Web.

Seguridad en Aplicaciones

La **seguridad de las aplicaciones** se refiere a las medidas de seguridad, a nivel de aplicación, cuyo propósito es impedir el robo o el secuestro de datos o códigos dentro de la aplicación.

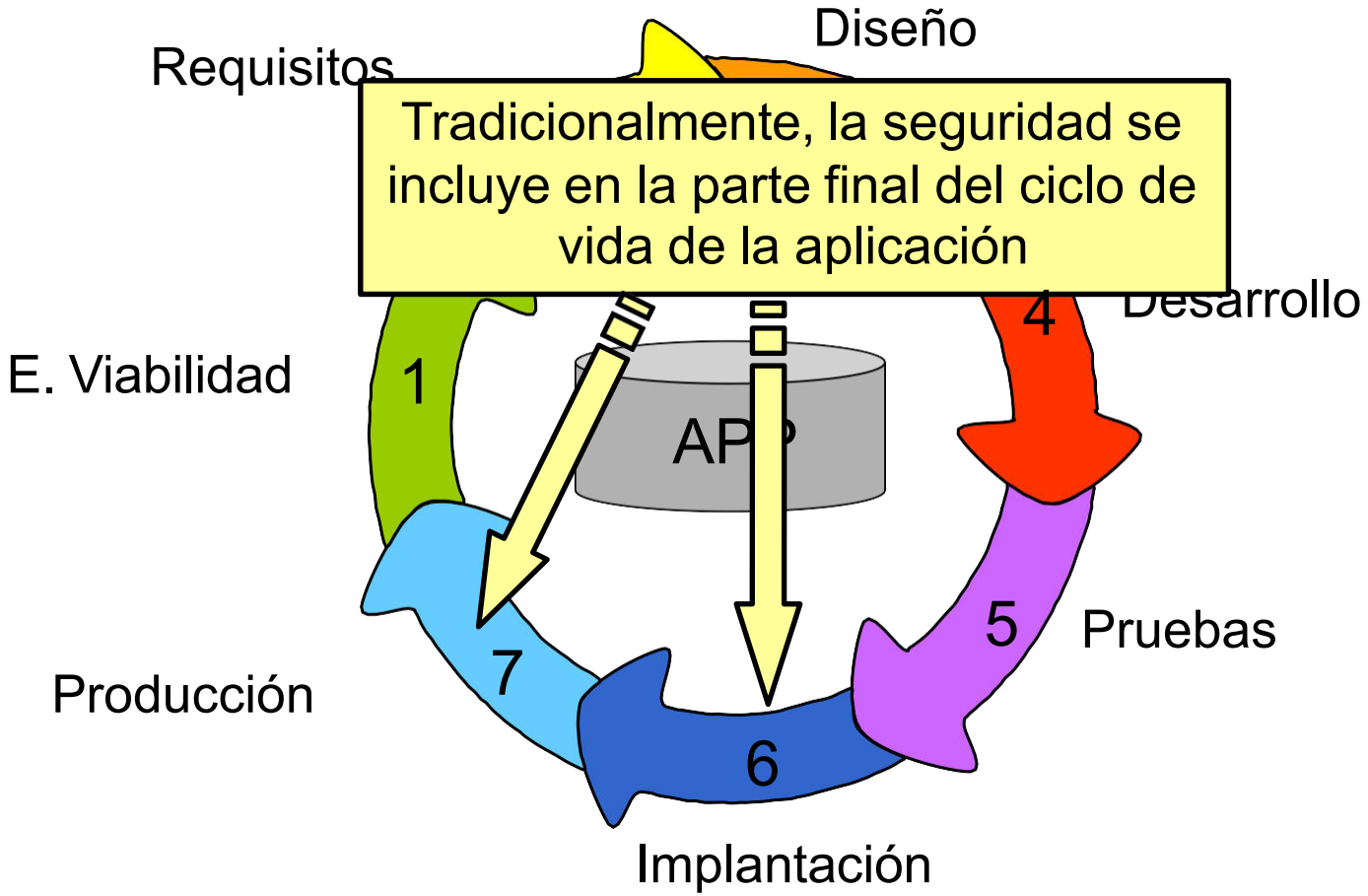
Abarca las consideraciones de seguridad que se deben tener en cuenta al desarrollar y diseñar aplicaciones, además de los sistemas y los enfoques para proteger las aplicaciones después de distribuirlas

Ciclo de Vida de Desarrollo de una Aplicación



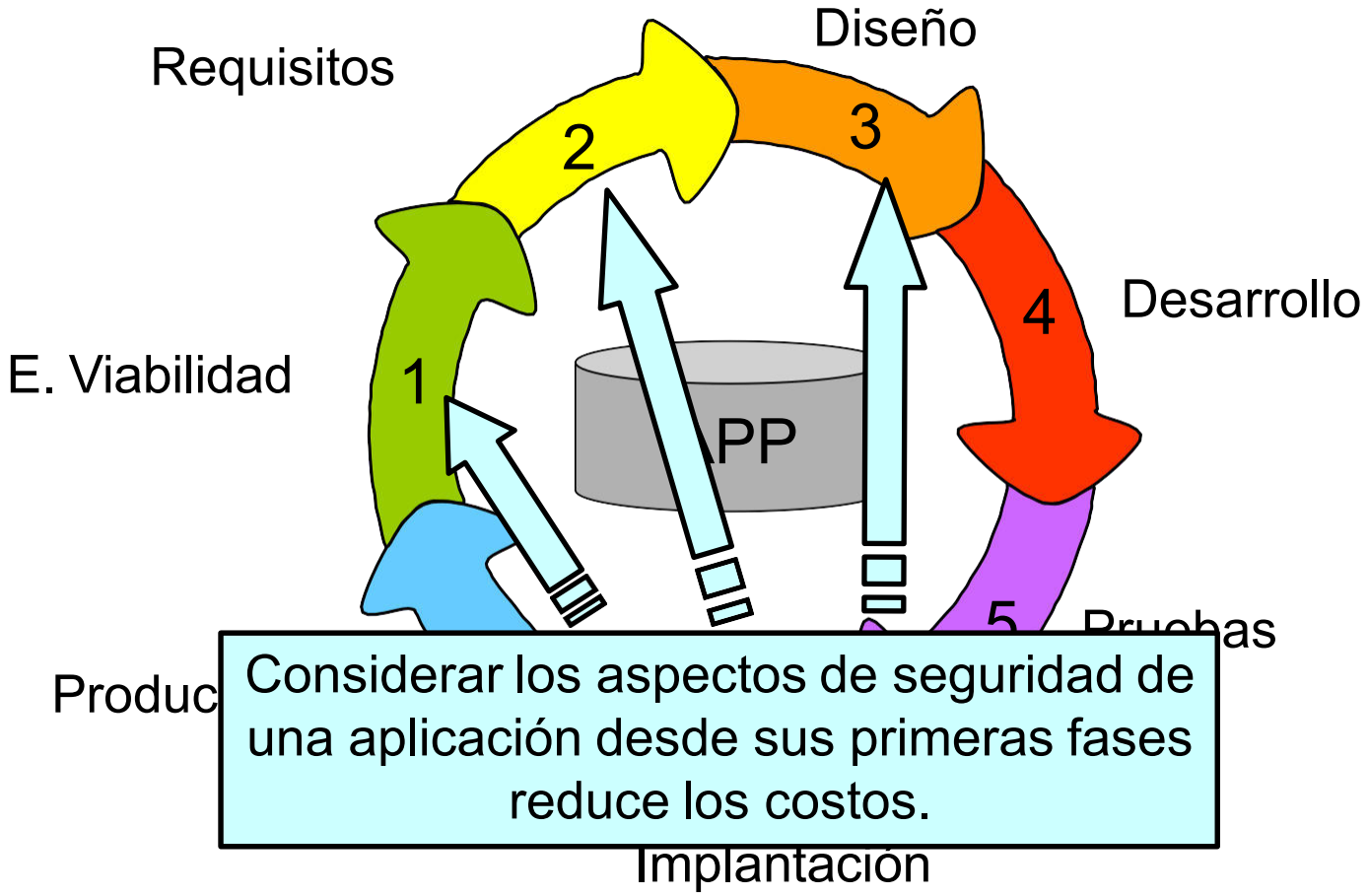
Ciclo de Vida de Desarrollo de una Aplicación

¿Dónde se considera la seguridad?



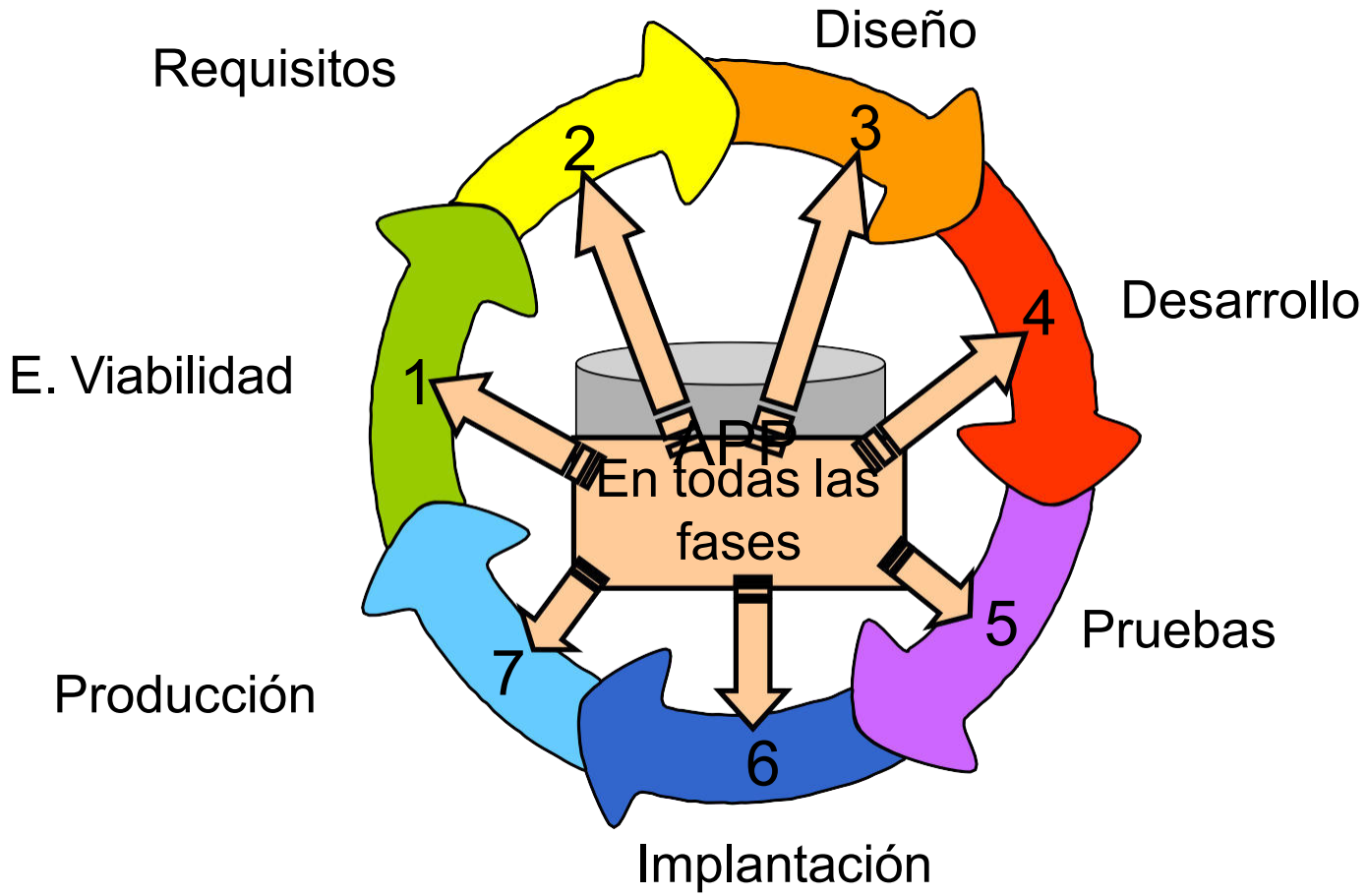
Ciclo de Vida de Desarrollo de una Aplicación

¿Dónde se debe considerar la seguridad?

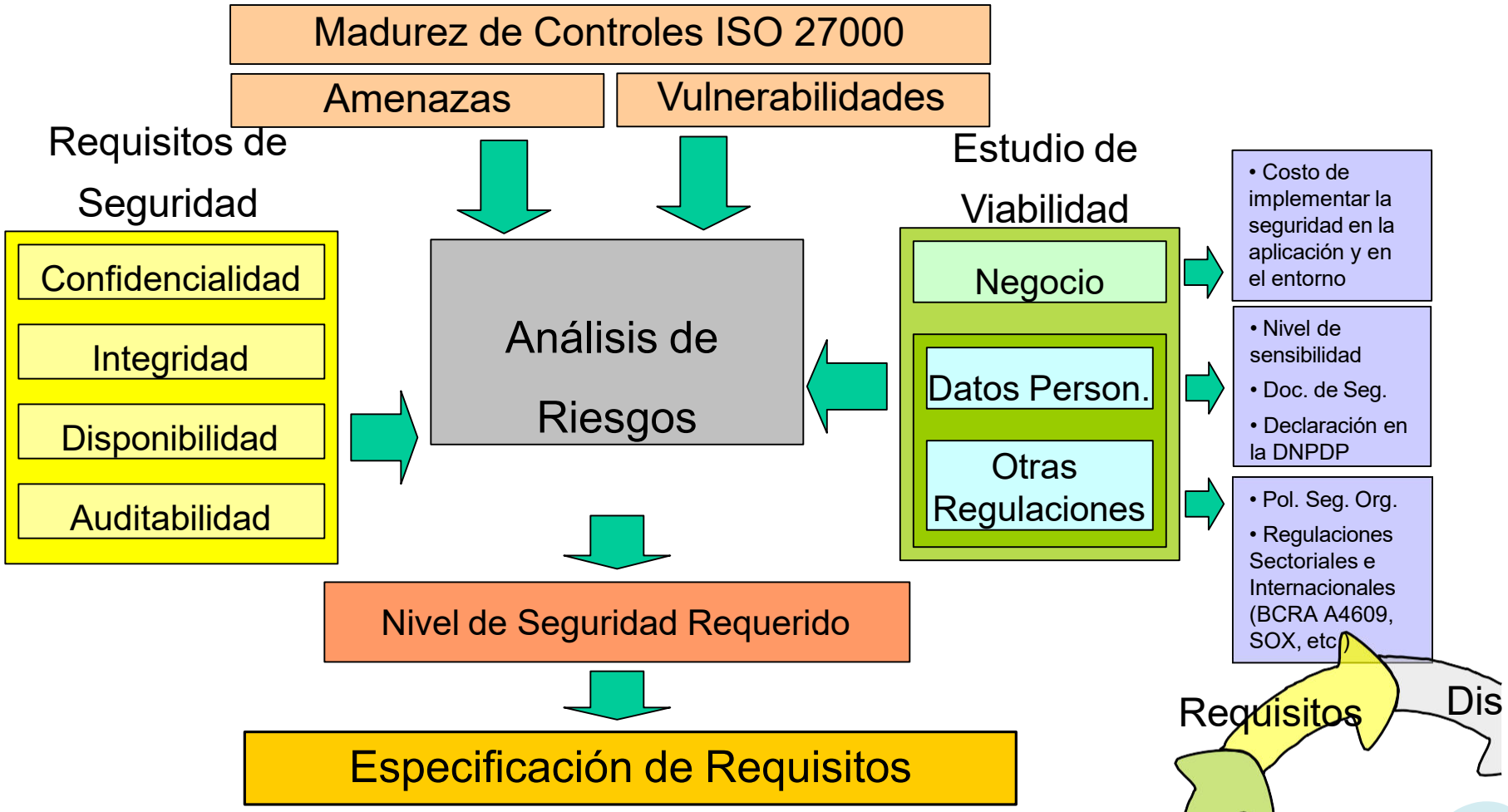


Ciclo de Vida de Desarrollo de una Aplicación

¿Dónde se propone incluir medidas de seguridad?

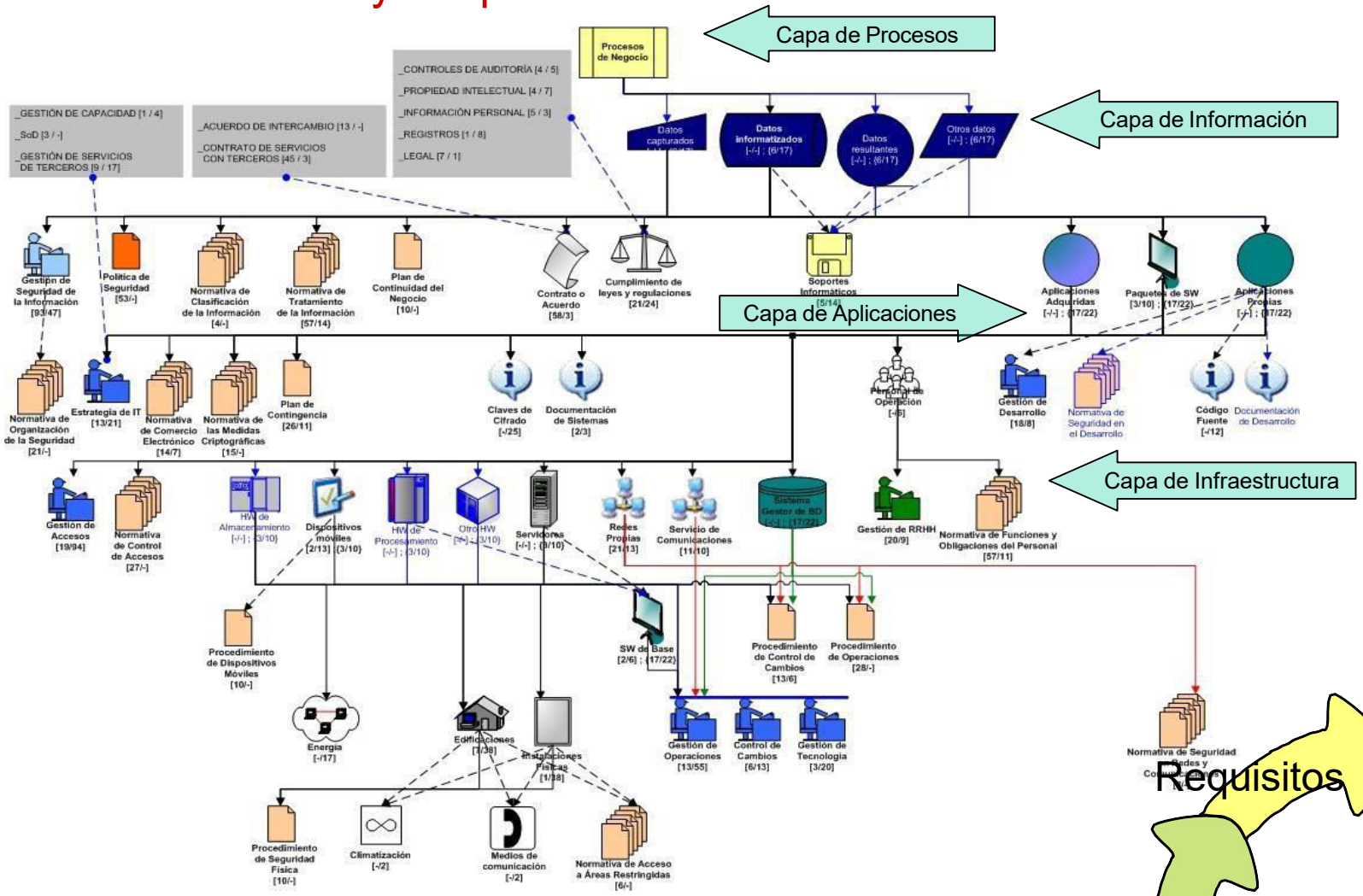


Estudio de Viabilidad y Requisitos



Estudio de Viabilidad y Requisitos

Árbol de Dependencias Permitidas



Estudio de Viabilidad y Requisitos

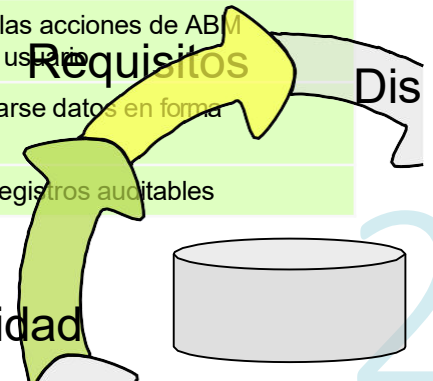
Esquema de Clasificación de la Información

CONFIDENCIALIDAD	
SECRETA	Su difusión afecta directamente al "core-business"
CONFIDENCIAL	Información de alta sensibilidad por impacto financiero, potencial de fraude, o requisitos legales
RESTRINGIDA	Información accesible por ciertas áreas, pero no toda la compañía
USO INTERNO	Información accesible por todos los miembros de la Organización
PUBLICA	Sin restricciones en su difusión

INTEGRIDAD	
CRUCIAL	No puede volver a obtenerse una calidad o prestación semejante. Irremplazable
ALTA	Se puede reemplazar con un activo de similar calidad, con esfuerzo alto
NORMAL	Se puede reemplazar con un activo de similar calidad, con esfuerzo medio
BAJA	Se puede reemplazar con un activo de similar calidad, con esfuerzo bajo
REEMPLAZABLE	Se puede reemplazar fácilmente con un activo de igual calidad

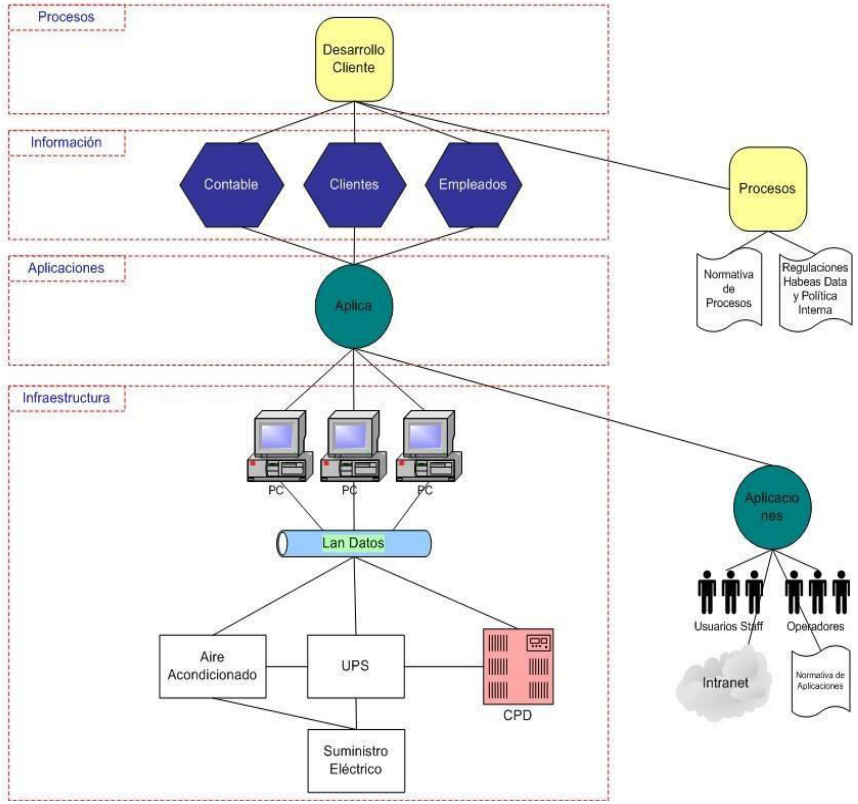
DISPONIBILIDAD	
VITAL	La Información debe estar disponible de forma ininterrumpida
DELICADA	La Información debe recuperarse en menos de 3 (tres) horas
SENSIBLE	La Información debe recuperarse en menos de 8 (ocho) horas
RELEVANTE	La Información debe recuperarse en menos de 24 (veinticuatro) horas
ESTANDAR	La Información puede recuperarse dentro de los plazos acordados como estándar

AUDITABILIDAD	
TRAZA TOTAL	Deben registrarse TODAS las acciones (ABMs, lecturas, intentos de lectura, etc.), para cada usuario
POR CAMBIOS	Deben registrarse todas las acciones de ABM, para cada usuario
PARTICULAR	Deben registrarse las acciones de ABM críticas, para cada usuario
GENERICA	Solo deben registrarse datos en forma genérica
LIBRE	Sin necesidad de registros auditables



Estudio de Viabilidad y Requisitos

ARBOL DE DEPENDENCIAS



Ejemplo de Resultados Obtenidos

CLASIFICACIÓN DE LA INFORMACIÓN

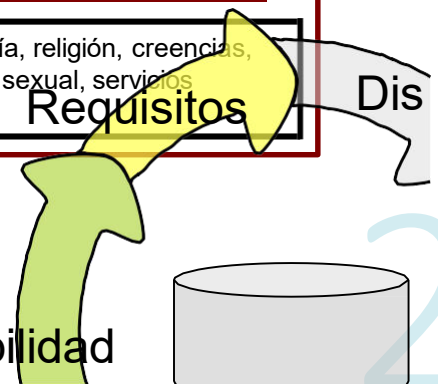
ACTIVO DE INFORMACION	A	C	I	D	R
Contable	4	4	5	4	5
Clientes	4	4	4	4	4
Empleados	4	3	4	3	2

A	C	I	D
3	3	3	3

ALTO	>4
MEDIO	3:4
BAJO	0:2

PROTECCIÓN DATOS PERSONALES

NIVEL CRITICO	Datos sensibles; ideología, religión, creencias, origen racial, salud, vida sexual, servicios financieros o crédito.

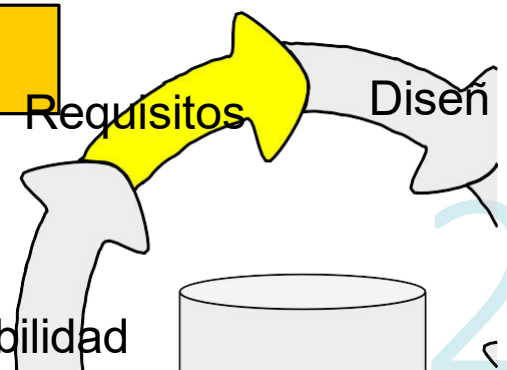


Especificación de Requisitos

Normas de desarrollo seguro

- Globales (Buenas Prácticas)
- Por arquitectura
  - ❑ Web
  - ❑ Host
  - ❑ Cliente - Servidor
- Adecuadas a cada nivel de seguridad (H.D.)
  - ❑ Crítico / Medio / Bajo

Especificación de Requisitos de Seguridad

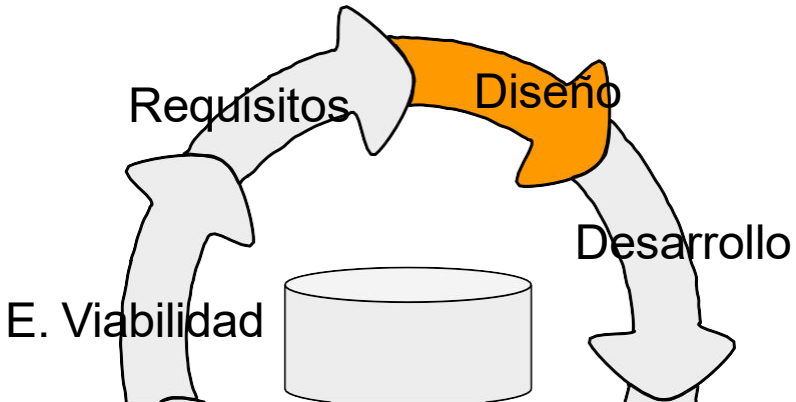


Diseño de la Aplicación

- Interfaz de programación de aplicaciones (APIs)
  - ❑ Criptografía
  - ❑ Auditoría (logs)
- Integración en la arquitectura de seguridad
- Manual buenas prácticas

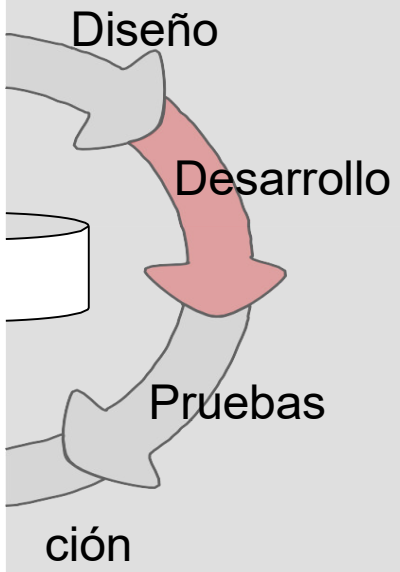
- Evitar que los desarrolladores tengan la responsabilidad de diseñar y construir mecanismos de seguridad.
- Reinventar la rueda para cada aplicación lleva a perdidas de tiempo y agujeros de seguridad masivos.

API DE CRIPTOGRAFÍA
- Firmar,
- Comprobar la firma,
- Obtener 'Hash',
- Comprobar un 'Hash',
- Cifrar,
- Descifrar.



Seguridad en Sistemas

Desarrollo de la Aplicación



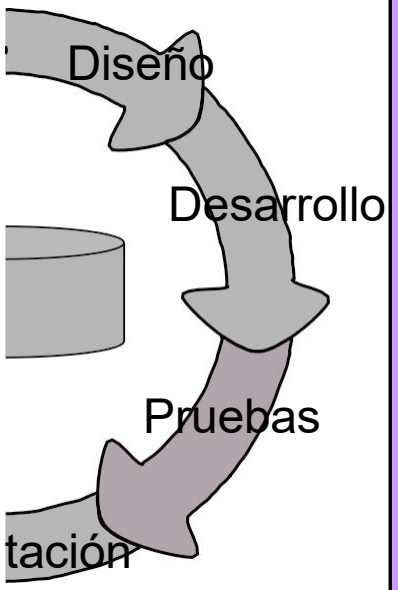
- Normas de seguridad del entorno de desarrollo
  - ❑ Relación con subcontratistas
  - ❑ Acceso a datos reales
  - ❑ Cesión de datos
    - o Procedim. solicitud descarga
    - o Procedim. disociación
- Generadores de datos de pruebas

Normas de desarrollo seguro para tecnologías o sistemas

- HTML
- XHTML
- XML
- Java
  - Servlets
  - JSP
  - EJB
  - JDBC
  - Applets
- .NET
- ASP
- PHP
- Javascript
- C, C++
- [...]

- Oracle
- Teradata
- SQL Server
- MySQL
- Posgress
- DB2
- MongoDB
- SAP
- [...]

Pruebas de la Aplicación



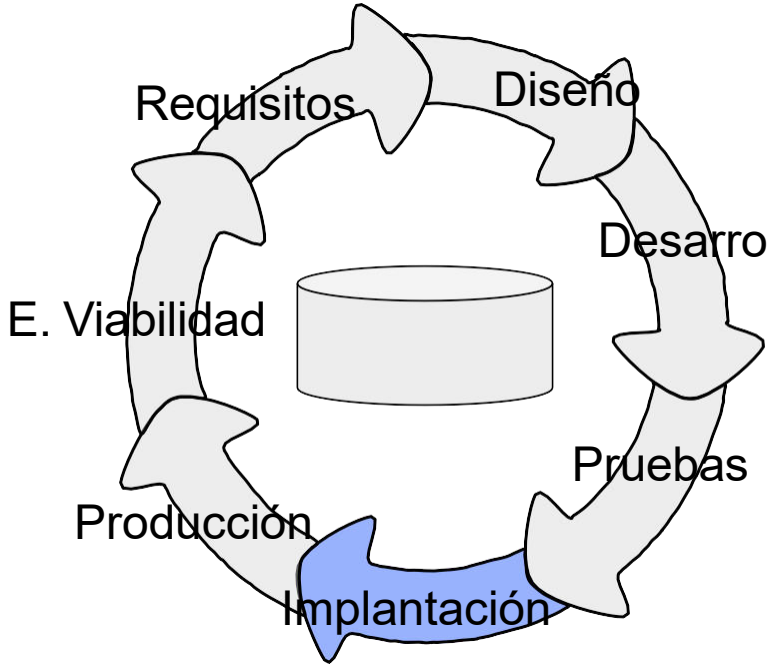
- Planes de pruebas
  - Global
  - Web
  - [...]
- Análisis de vulnerabilidades a nivel aplicación
  - ❑ Core Impact
  - ❑ Acunetix
  - ❑ W3AF (Web)
  - ❑ Nikto
- Generadores de datos de prueba
- Revisión del código

❑ Mecanismos de cifrado de los datos: Ej.: uso de SSL
❑ Control de accesos
❑ Autenticación.
❑ Mantenimiento de sesión.
❑ Interacción con los servlets, JSPs...
❑ Validación de parámetros de entrada en la parte interactiva.
❑ Auditoría (logs).

❑ Manejo de DNS
❑ Protección de Estructura Interna del Sitio Web
❑ Protección contra Robots
❑ Manejo de Privacidad
❑ Canales seguros
❑ Mecanismos de Control de Acceso
❑ Protección de Software
❑ Hosting / Sitio Propio
❑ Roles Mínimos a asegurar

Implantación de la Aplicación

El momento más crítico…

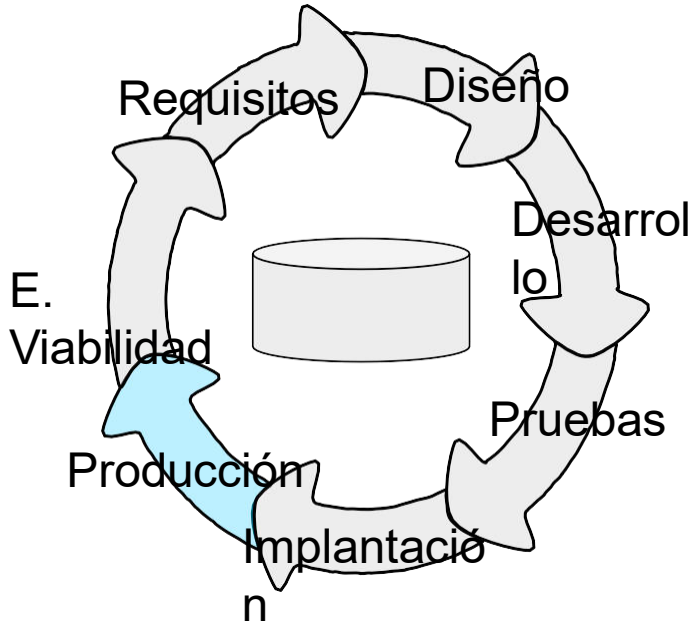


Normas de implantación segura de aplicaciones

- Permisos sobre los archivos
- Privilegios del personal
- Configuración de la aplicación

Producción de la Aplicación

- Protección a nivel aplicativo (Firewall de aplicación)
- Auditoría de cumplimiento
- Penetration Test Infraestructura
  - Nessus
  - Nmap
- Penetration Test de App
  - Core Impact
  - Acunetix
  - W3AF (Web)
  - Nikto
- Tablero de control de seguridad de aplicaciones



Recomendaciones Finales

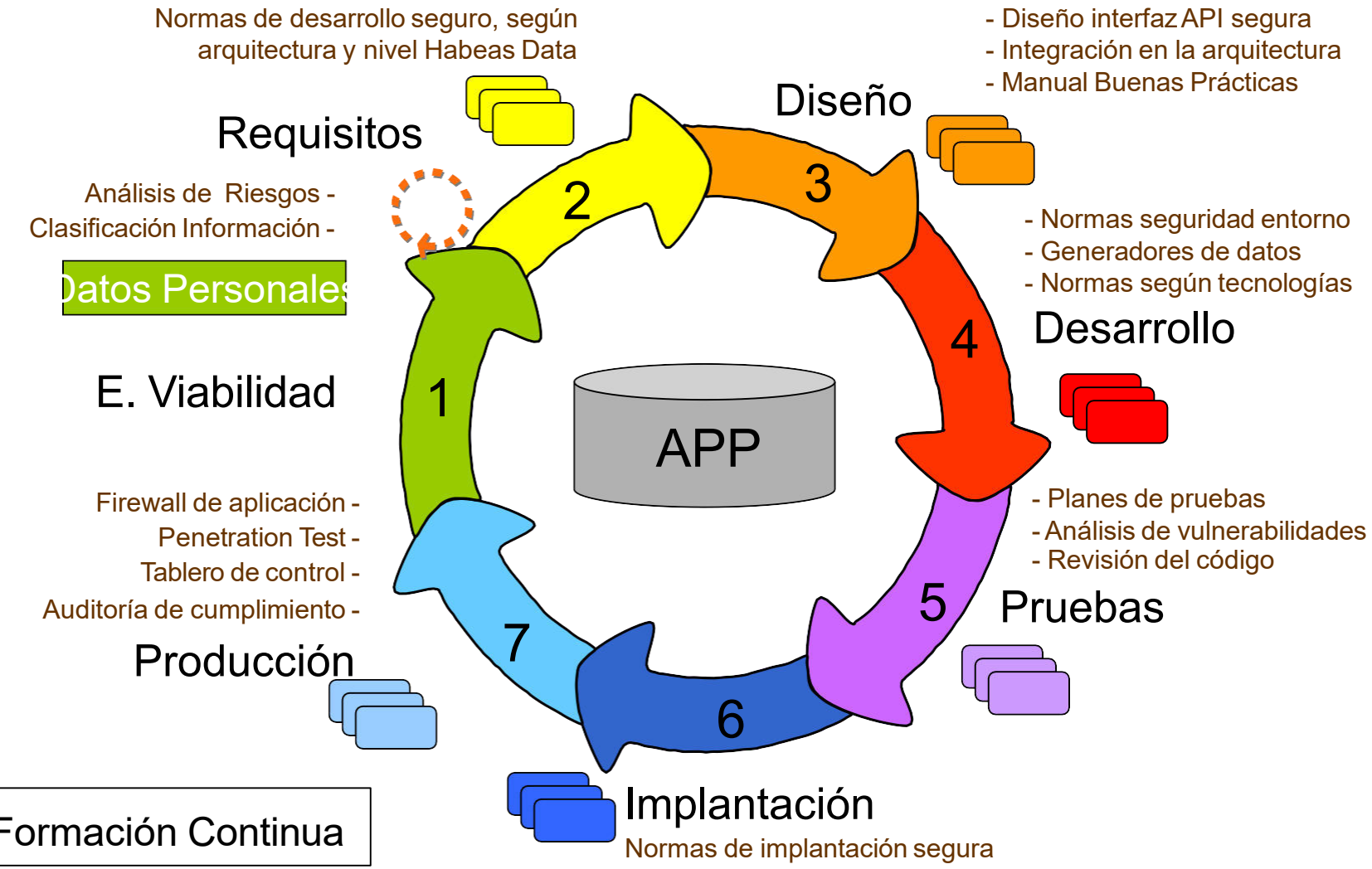
Proyecto OWASP

Open Web Application Security Project, metodología de libre acceso que puede ser utilizada como material de referencia por parte de los arquitectos de software, desarrolladores, y profesionales de la seguridad involucrados en el diseño de la seguridad de las aplicaciones.

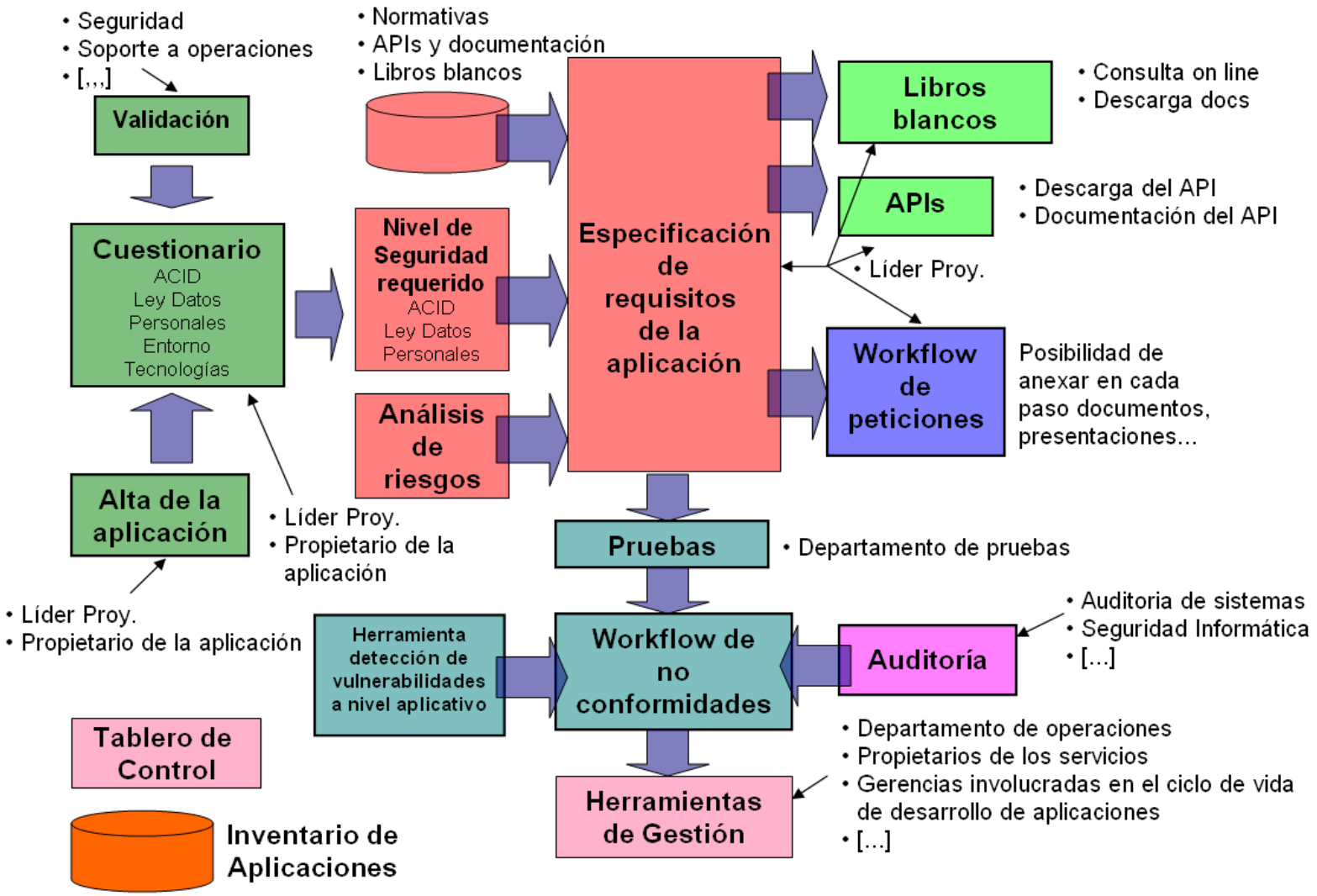
- Validación de la entrada y salida de información
- Diseños simples
- Utilización y reutilización de componentes de confianza
- Defensa en profundidad
- Tan seguros como en eslabón más débil
- La "seguridad por oscuridad" no funciona
- Verificación de privilegios
- Ofrecer la mínima información

Esquema Normativo de Seguridad

Ciclo de Seguridad en Desarrollo de Aplicaciones



Seguridad en Sistemas



Seguridad en Sistemas Infotmáticos

Conclusiones

- Desde el punto de vista técnico, la seguridad de los sistemas de información se basa en tres pilares:
  - Una red segmentada con una restricción de accesos adecuada.
  - Los sistemas correctamente configurados.
  - Las aplicaciones desarrolladas de forma segura.
- Las aplicaciones deben protegerse:
  - Introduciendo seguridad en todo el ciclo de vida del Desarrollo.
  - Definiendo normas y procedimientos para cada entorno y tecnología empleada.
  - Apoyándose desde el principio en metodologías de análisis y gestión de riesgos.
  - Realizando pruebas de seguridad de la aplicación.
  - Protegiéndola con FW de aplicación, antes del paso final a Producción.
- Una metodología de desarrollo seguro redundará en un beneficio claro del negocio, aumentando notablemente el nivel de seguridad de las aplicaciones desde el principio, disminuyendo drásticamente los riesgos, ahorrando en costos y tiempo.

Accesos

Accesos

Índice

- *Tipos de Control de Accesos y su Implementación*
- *Identificación y Autenticación*
- *Empleo de Contraseñas*
- *Técnicas de Control de Acceso*
- *Administración de Control de Acceso*
- *Monitorización y Detección de Intrusos*

Control de Accesos

2023
SEGURIDAD INFORMÁTICA

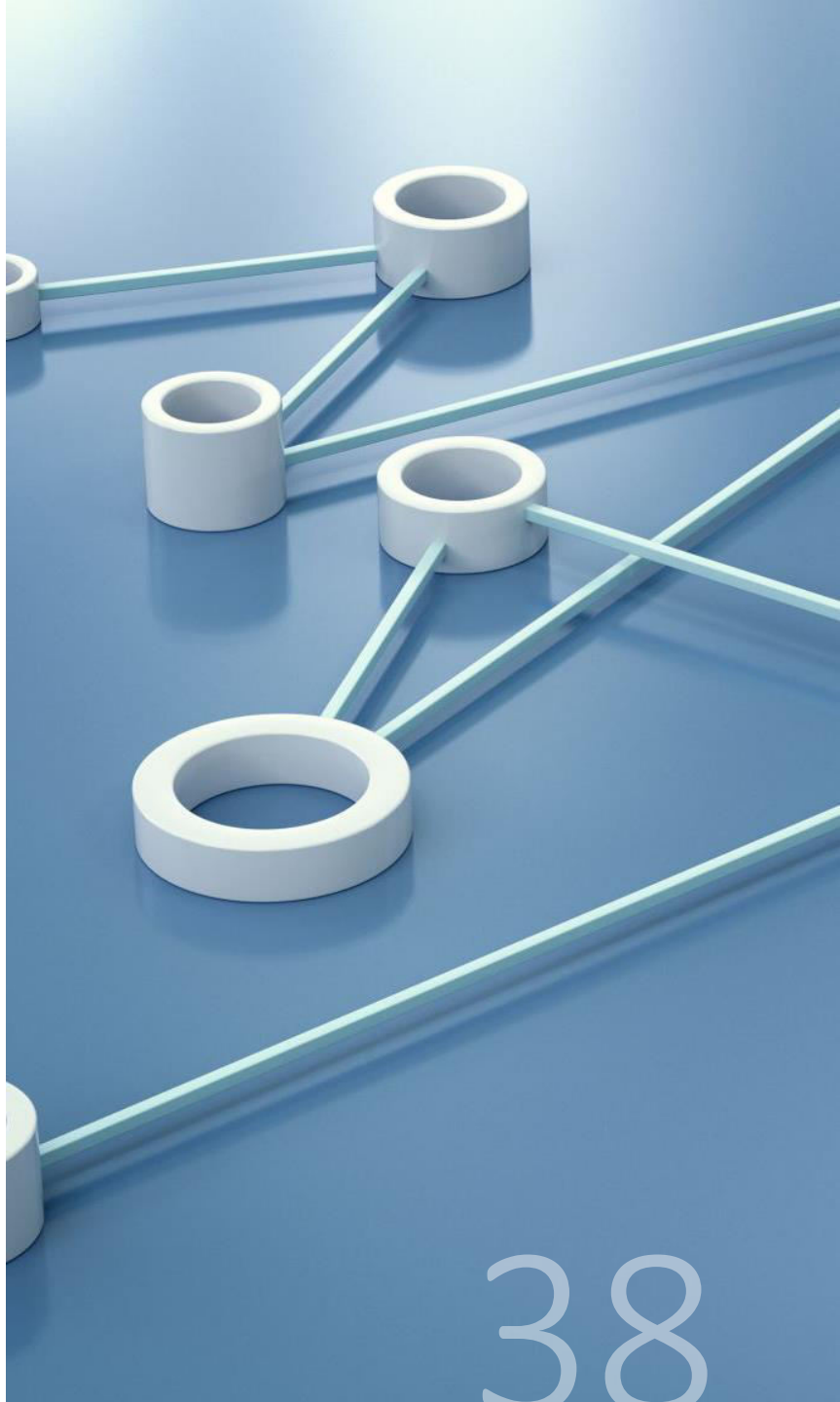
1

Control de Accesos

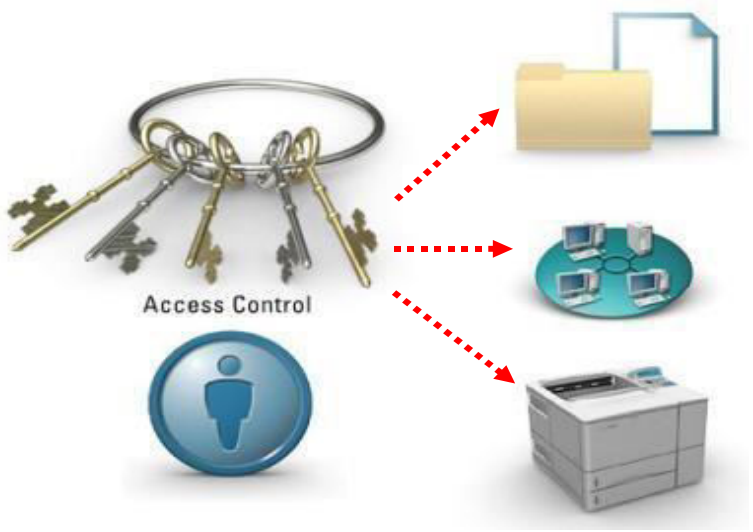
Descripción general

Controlar el acceso a la información y a los recursos de procesamiento de datos es fundamental en cualquier empresa. El profesional debe ser capaz de describir los conceptos de control de acceso y las metodologías utilizadas, así como la forma en que se realicen, ya sea en un entorno centralizado o descentralizado. Los objetivos de este capítulo son:

- Describir las características del control de acceso
- Explicar conceptos de identificación y autenticación
- Explicar la función de las contraseñas
- Definir las técnicas de control de acceso
- Definir la administración de control de accesos
- Explicar los conceptos de monitorización y detección de intrusos

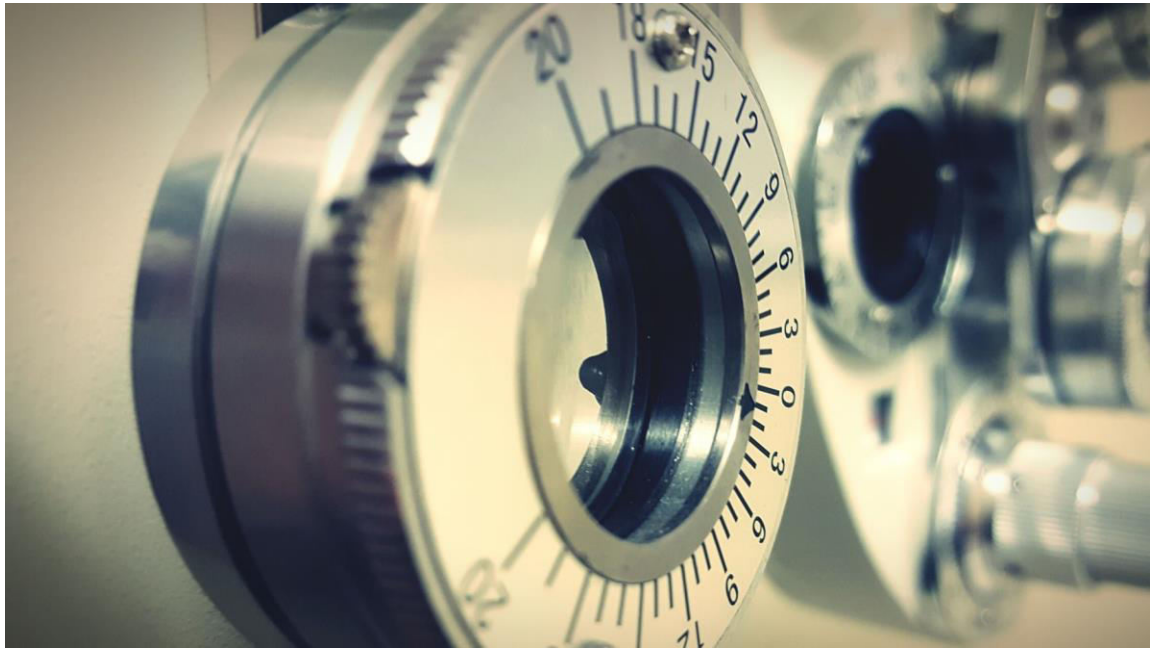


Control de Accesos



Derechos de Acceso y Permisos

- Para proporcionar un nivel de seguridad, los recursos que necesitan un mecanismo de protección, no deben ser vistos o modificados de forma no autorizada. La concesión de derechos de acceso y permisos a los sujetos y los objetos en la red debe ser gestionada eficientemente.
- El control de acceso es el corazón de los derechos de acceso y permisos, especificando lo que los usuarios en un sistema pueden o no pueden hacer.
- El control de acceso incluye las acciones que un usuario puede realizar y los recursos que un usuario puede tener acceso.
- Los controles de acceso son las salvaguardas o contramedidas que garantizan la Triada CID y aseguran que, sólo los usuarios con la necesidad adecuada y la autorización debida pueden acceder a los recursos.



Control de Accesos

Tipos de Control de Acceso

El principal objetivo del establecimiento de controles de acceso, es el de reducir los efectos producidos por las amenazas de seguridad a niveles tolerables.

Estos controles pueden ser:

- **PDC**: Preventivos, Detectivos, o Correctivos.
- **DRC**: Disuasión, Recuperación, o Compensación.

Control de Accesos

Tipos de Control de Accesos

PDC

- Preventivos: actúan antes de que un hecho ocurra y su función es detener agentes no deseados.
  - Política de Seguridad, capacitación, antivirus, clasificación de información, encripción o cifrado, separación de ambientes, Firewalls, etc.
- Detectivos: actúan antes de que un hecho ocurra y su función es revelar la presencia de agentes no deseados
  - Guardias de seguridad, investigación de incidentes, IDS, antivirus, logs de auditoria, CRC, totales de hash, comprobaciones, conciliación.
- Correctivos: actúan luego de ocurrido el hecho y su función es corregir las consecuencias.
  - Política de seguridad, manuales, plan de contingencia, antivirus, backup (restauración), reportes de control.

Control de Accesos

Tipos de Control de Accesos
DRC

- Disuasión: actúan desalentando las violaciones a la seguridad.
  - Cerraduras, rejas, guardias de seguridad, circuito cerrado de TV, separación de funciones, etc.
- Recuperación: actúan restaurando recursos y capacidades.
  - Copias de seguridad, software antivirus, backup (restauración), etc.
- Compensación: actúan brindando alternativas a otros tipos de controles.
  - Monitorización y supervisión, procedimientos de personal, etc.

Control de Accesos

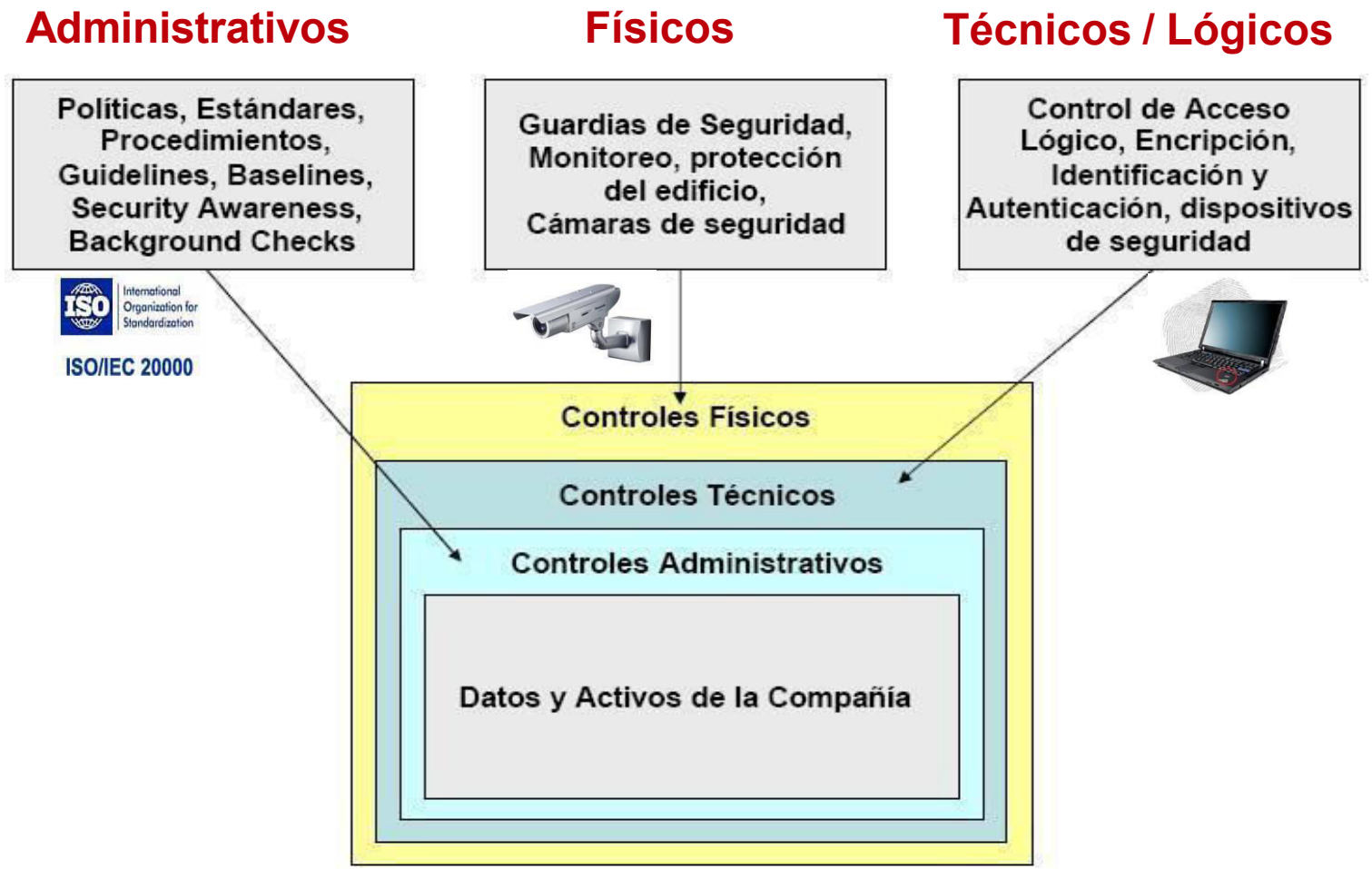
Implementación de Controles de Acceso

La implementación y mantenimiento de un control de acceso puede se categorizada en:

- Administrativos: Comprenden las normas y procedimientos definidos en la Política de Seguridad de la Organización, a fin de implementar y hacer cumplir las medidas de control de acceso. Algunos ejemplos son:
  - Política, normas, procedimientos, revisiones, clasificación de la información, capacitación, etc.
- Lógicos/Técnicos: Comprenden los mecanismos de hardware o software usados para gestionar el acceso a recursos y sistemas de manera de brindar protección a los mismos. Algunos ejemplos son:
  - Contraseñas, técnicas criptográficas, smart cards, sistemas biométricos, ACLs, etc.
- Acceso Físico: Comprenden la distribución de barreras físicas a fin de prevenir el contacto directo con los sistemas. Algunos ejemplos son:
  - Detectores de movimientos, sensores, luces, cerraduras, perros, cámaras, etc.

Control de Accesos

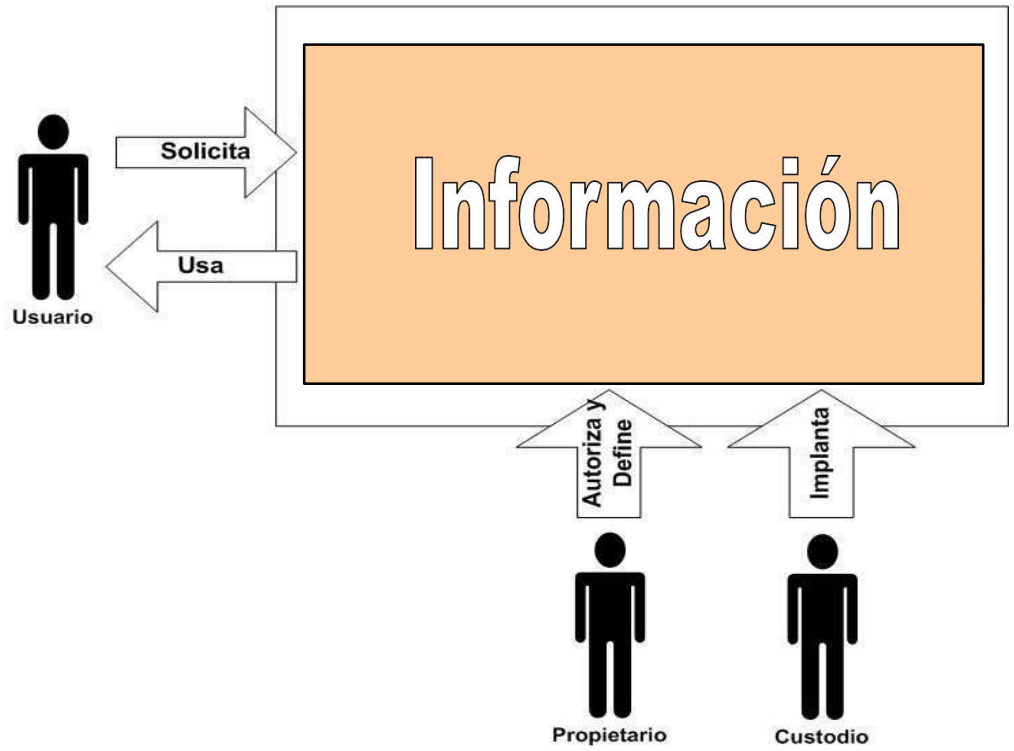
Implementación de Controles de Acceso



Control de Accesos

Esquema de Gestión de Accesos

Asignación de la Propiedad de la Información



Control de Accesos

Propiedad de la Información

Algunos Conceptos

Propietario: Sujeto al que se le ha asignado la responsabilidad de gestión de una información en particular. Pueden ser empleados; preferentemente personal directivo de la organización. Sin embargo, desde el punto de vista legal, la propiedad de la información es siempre de la organización. El propietario de la información tendrá las siguientes funciones:

- Dictar las medidas de acceso a la información.
- Conocer como se usa su información dentro y fuera de la organización, entendiendo también los problemas potenciales asociados al uso de ésta.
- Clasificar la información basándose en su sensibilidad y criticidad. Las escalas de sensibilidad y criticidad no son desarrolladas por el Propietario, sino por el responsable de definir la seguridad.
- Definir los requisitos de resguardo y conservación de la información.
- Aprobar todos los requisitos de acceso a la información que le ha sido asignada.

Control de Accesos

Propiedad de la Información

Algunos Conceptos

Custodio: Sujetos encargados de tener la posesión de la información, y gestionar los sistemas que utilizan esta información. Pueden ser empleados, contratistas, consultores o personal externo. El trabajo del Custodio es comúnmente asignado a los Administradores de Sistemas, Operadores o Especialistas de Control de Datos. El custodio de la información tendrá las siguientes funciones:

- Cumplir las instrucciones del Propietario de la información y los requisitos de la política general de seguridad de la información.
- Gestionar diariamente la información que le ha sido encomendada, a través de las siguientes acciones:
  - Salvaguardar el almacenamiento y procesamiento seguro de la información (Departamento Operativo)
  - Administrar los accesos a la información que le ha sido encomendada para tal fin (Área responsable de la administración de accesos).
  - Informar periódicamente al Propietario sobre todo el que tenga acceso a la información en cuestión (Área responsable de la mejora de procesos).
- Proveer asesoramiento técnico sobre las mejores formas de proteger la confidencialidad, integridad y disponibilidad, así como la autenticación y auditabilidad de la información.

Control de Accesos

Propiedad de la Información

Algunos Conceptos

Usuario: Sujeto que tiene acceso a la información y/o sistemas de la organización, para su uso. Podrán ser empleados, personal temporal, consultores, contratistas o personal externo. Sus privilegios deberán ser revocados cuando cambie o finalice la necesidad de contar con dichos accesos. El usuario de la información tendrá las siguientes funciones:

- Solicitar al correspondiente Propietario los accesos a la información y sistemas.
- Abstenerse de usar la información de la organización para cualquier otro propósito que el autorizado por parte del Propietario o por su superior inmediato.
- Manejar de forma segura la información en su posesión, incluyendo el hecho de mantener en secreto su clave de acceso, tratar de forma segura la información sensible, tanto en papel, forma verbal y formato electrónico.
- Informar al Propietario o a su superior inmediato, los errores o anomalías en la información a la cual tiene acceso.

.

Control de Accesos

Pasos para Acceder a un Objeto

El control de acceso gobierna el acceso de sujetos a objetos.
Existen varios pasos para poder acceder a un objeto:

- Identificación
- Autenticación
- Autorización
- Auditoria / Accounting

Identificación

Control de Accesos

Identificación

Es el proceso por el cual un sujeto proporciona una identidad y una cuenta es iniciada. Un Usuario puede utilizar como identidad:

- Nombre de Usuario
- ID de Logon
- PIN
- Pasaporte
- DNI

Autenticación

Control de Accesos

Autenticación

Es el proceso de verificar que una identidad proporcionada es válida. La autenticación requiere que el sujeto proporcione información adicional que debe corresponder exactamente con la identidad indicada. El método más común, es el empleo de contraseñas.

Los tipos de información más comunes que pueden ser empleados son:

- **Factor de autenticación por Tipo 1**: "Algo que usted conoce", como es una contraseña, un PIN, etc.

- **Factor de autenticación por Tipo 2**: "Algo que usted tiene", como es una smart-card, un token, tarjeta de coordenadas, etc.

- **Factor de autenticación por Tipo 3**: "Algo que usted es", como es una huella digital, análisis de voz, escáner de retina o iris, ADN, etc.

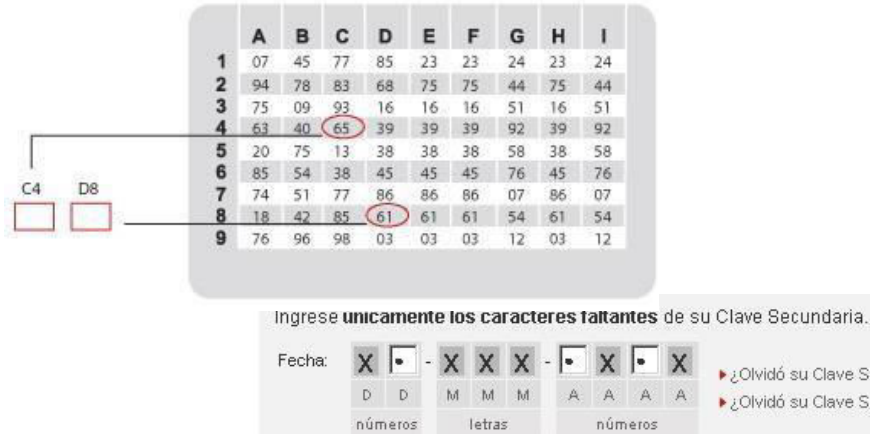
Control de Accesos

Autenticación

Ejemplos:

- **Factor de autenticación por Tipo 1**: “Algo que usted conoce o sabe”.

- **Factor de autenticación por Tipo 2**: “Algo que usted tiene”.



- **Factor de autenticación por Tipo 3**: “Algo que usted es”.

Control de Accesos

Autenticación Multifactor

La Autenticación de múltiples factores utiliza dos o más tipos de autenticación para proporcionar mayor seguridad.

Sistemas de factor de autenticación doble:

- Tarjeta Cajero ATM + PIN
- Tarjeta de Crédito + Firma
- PIN + Huella digital
- Nombre Usuario + Contraseña

Sistemas de factor de autenticación triple (mayor seguridad):

- Contraseña + Token + Huella digital
- PIN + Licencia de conducir + Escaneo de voz
- Contraseña + Llave Mecánica/Electrónica + Escaneo de Iris

Control de Accesos

Autenticación – Otros Factores

En adición a estos, existen otras como:

- "Algo que usted hace", tanto como firmar un documento, escribir una frase ("captcha"), un gesto frente a una cámara, un dibujo en el touchpad, etc., normalmente incluido dentro del Tipo 3.

- "Donde usted se encuentra", como es un equipo específico, una ruta o IP, una línea telefónica determinada, etc., normalmente incluido dentro del Tipo 2.

Control de Accesos
Técnicas de Identificación y Autenticación

Multifactor

Es una parte esencial de las mejores prácticas actuales de gestión de identidad y acceso.

También es uno de los principales requisitos de cumplimiento para la verificación de identidad del usuario.

MFA le permite agregar una capa más de protección a puntos finales críticos, datos y funcionalidades.

La función principal de **MFA** es asegurarse de que la persona o entidad que intenta acceder a los activos protegidos es realmente quien dice ser.

Control de Accesos
Técnicas de Identificación y Autenticación

Multifactor

La autenticación multifactor combina dos o más credenciales independientes: lo que **sabe** el usuario, lo que **tiene** el usuario y lo que **es** el usuario.

La autenticación multifactor, también conocida como autenticación de dos factores o simplemente **2FA**, requiere que el proceso de autenticación incluya la verificación de factores de al menos dos de las tres categorías:

1. Algo que el usuario **sabe** (contraseña, PIN, respuesta a una pregunta secreta, etc.)
2. Algo que el usuario **tiene** (clave, token de seguridad, tarjeta bancaria, teléfono inteligente, etc.)
3. Algo que el usuario **es** / biometría (huella digital, iris, voz, etc.)

Control de Accesos

Técnicas de Identificación y Autenticación

Entre las principales técnicas de mayor utilización, encontramos:

- Contraseñas
- Sistemas Biométricos
- Tokens
- Tickets

Control de Accesos Contraseñas

Es la técnica de autenticación más usada, pero también es considerada la más débil. Las fallas habituales de seguridad en las contraseñas se deben a:

- Son fáciles de escribir, compartir y olvidar.
- Los usuarios frecuentemente las eligen fáciles de recordar y en consecuencia, fáciles de romper.
- Las aleatorias son difíciles de recordar.
- Pueden ser robadas fácilmente, por observación, grabación, etc.
- Algunas se transmiten en texto claro o protegidas por técnicas fáciles de romper.
- Las cortas o débiles son vulnerables a ataques de fuerza bruta.

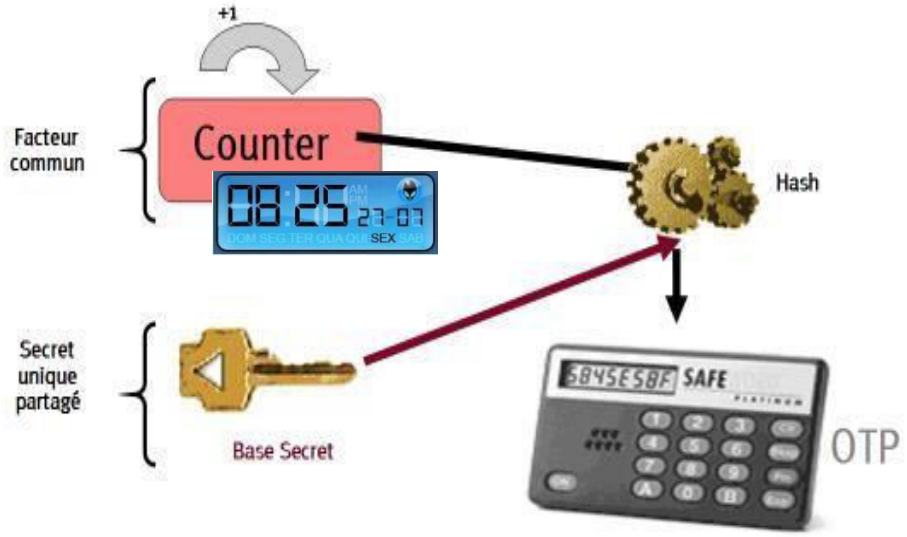
Control de Accesos
Tipos de Contraseñas

Existen dos tipos de contraseñas:

- **Estáticas**: permanecen inalterables y solo cambian cuando expira su tiempo de vida.
- **Dinámicas**: cambian después de un período de tiempo de uso. Las OTP (One-Time Passwords) son una variante de esta categoría.

Tipos de Contraseñas

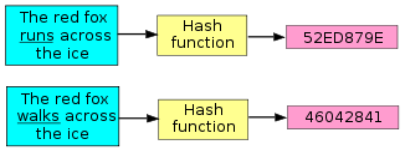
OTP – One Time Passwords



§ Esta técnica utiliza contraseñas que sólo tienen validez para un usuario específico durante una determinada sesión. Ej:. S/Key. El sistema utiliza algoritmos de hashing de una vía con el fin de crear un esquema de contraseñas de única vez .

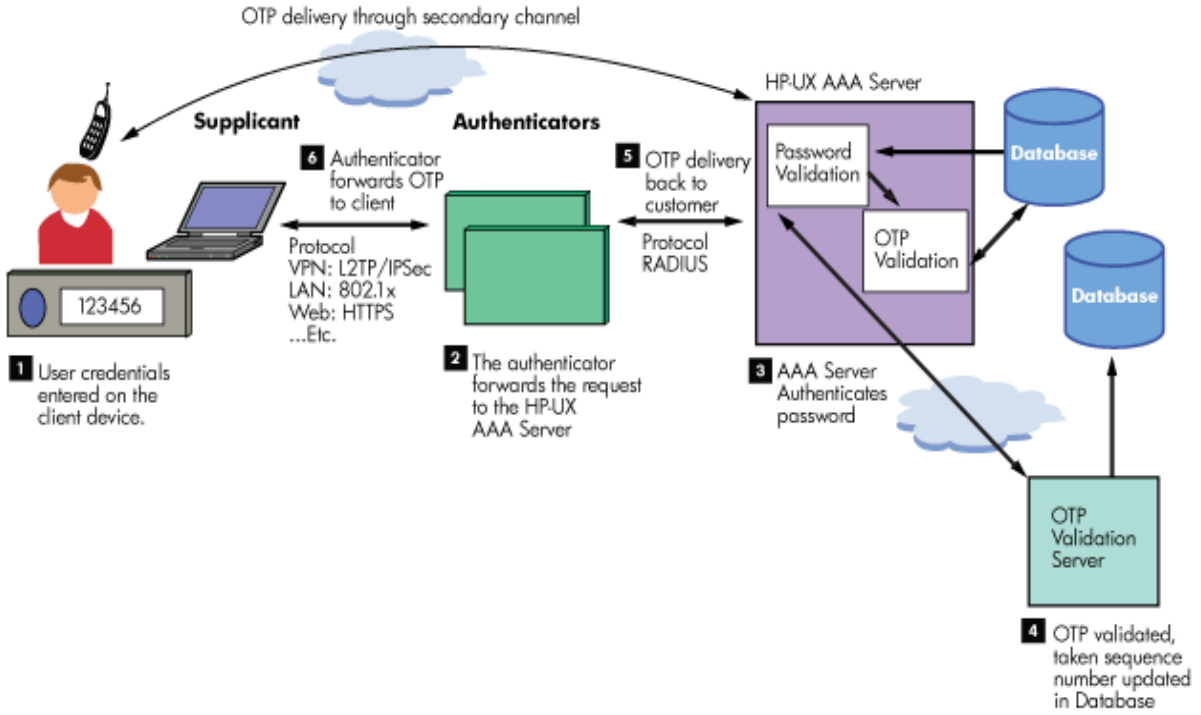
§ La contraseña es enviada a través de la red, y luego de ser empleada, caduca y no es válida para ser utilizada nuevamente.

Hash: se refiere a una función o método (one-way) para generar claves o llaves que representen de manera casi unívoca a un documento.



Tipos de Contraseñas

OTP – One Time Passwords



Este sistema tiene tres componentes fundamentales:

- Cliente: Solicita el login del usuario. No realiza el almacenamiento de contraseñas.
- Host: Procesa la contraseña, almacena la contraseña de única vez y también le provee al cliente el valor inicial para calcular el hash.
- Calculador de Claves: Es la función de hash para la contraseña de única vez.

OTP – One Time Passwords
Métodos de Generación y Distribución

Generación: se realiza a través de algoritmos de funciones random. Esto es necesario para evitar la predicción de la OTP a través del estudio de la generación de una.

Existen dos métodos de generación:

- **Sincronización por tiempo** – normalmente relacionado a hard c/ clock sincronizado (Ej.:token).
- **Algoritmo matemático** - El algoritmo matemático genera la contraseña nueva basada en la anterior (cadena). Si un intruso viese la contraseña, podría tener solo acceso temporal, puesto que la contraseña caduca cuando finaliza la sesión. Para obtener la clave siguiente en la serie, hay que encontrar la manera de calcular la función inversa y esto es extremadamente difícil de lograr debido al hash (one-way).

Distribución: los métodos más empleados de entrega o distribución son:

- **Tokens**: Sincronización temporal. Vulnerable a pérdidas por volatilidad de la memoria o a robos.
- **SMS**: Servicio de mensajes cortos. Vulnerable a man-in-the-middle.
- **Celulares**: Empleados como tokens, brindan gran almacenamiento y potencia de calculo, para la generación de OTP. Vulnerable a pérdidas o robos.
- **OTP Directo**: Se aplica directamente al sistema que el usuario accede. Ideal para organizaciones con gran número de usuarios, pero no es considerado el mas seguro.

Contraseñas
Selección y Empleo

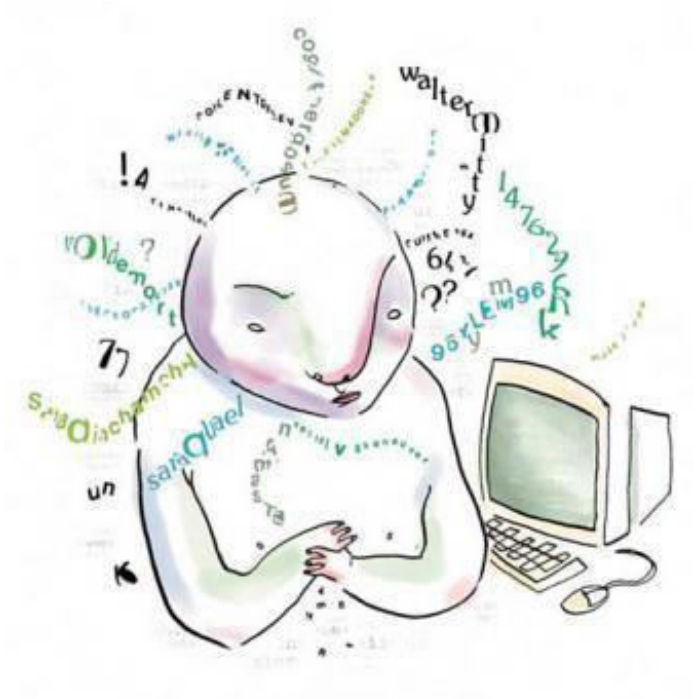
Qué evitar en una contraseña?

- ID de usuario,
- Info. personal (nombre, apellido, DNI, fechas, etc.),
- Secuencias básicas de teclado (qwerty, 1234),
- Palabras del diccionario,
- Utilizar todos números, o todas letras.

Crear una contraseña fuerte no es suficiente. La contraseña debe ser adecuadamente administrada y protegida por su dueño.

- No compartirla con otros,
- No anotarla en ningún lugar,
- No transmitirla en claro por ningún medio,
- No permitir que otros la vean al introducirla.

Contraseñas
Recomendaciones



Parafrase: “Un sol para los chicos”

Contraseña: “1S.xalCH”

Aspectos de seguridad aplicables:

1. Que contenga al menos 8 caracteres,
2. Utilizar dígitos, letras y caracteres especiales,
3. Alternar entre mayúsculas y minúsculas,
4. Cambiar las contraseñas con cierta regularidad,
5. Utilizar signos de puntuación,
6. Emplear reglas mnemotécnicas,

Parafrases y Passwords Cognoscitivos

- Las “parafrases” son frases conocidas por el usuario, que se utilizan para recordar mas fácilmente una contraseña.
- Un “password cognoscitivo”, comprende una serie de preguntas acerca de hechos cuyas respuestas sólo pueden ser conocidas por un sujeto determinado.

Contraseñas
Tipos de Ataques

Cuando un atacante busca obtener las contraseñas, puede utilizar diferentes métodos, como:

- **Análisis de tráfico de red** – Capturar la contraseña mediante el empleo de herramientas de monitorización del tráfico de red.
- **Acceso al archivo de contraseñas** – Poseer permisos para acceder al archivo de contraseñas del sistema.
- **Ataques por fuerza bruta** - Recuperar una contraseña probando todas las combinaciones posibles hasta encontrar la correcta.
- **Ataques por diccionario** - Recuperar una contraseña probando todas las palabras de un diccionario hasta encontrar la correcta.
- **Ingeniería social** - Práctica de obtener información confidencial a través de la manipulación y el engaño de usuarios legítimos.

Comprobadores Proactivos de Contraseñas: Software que al ser instalado evita que se introduzcan contraseñas débiles en la base de datos de contraseñas. Realiza un mini ataque a diccionario con unas ciertas reglas, de forma que si se averigua la contraseña, se imposibilita su uso.

Contraseñas Fortaleza

Longitud en caracteres	26 letras minúsculas	36 letras y dígitos	52 letras (min y may)	96 caracteres
6	50 minutos	6 horas	2,2 días	3 meses
7	22 horas	9 días	4 meses	23 años
8	24 días	10,5 meses	17 años	2.287 años
9	21 meses	32,6 años	881 años	219.000 años
10	45 años	1.159 años	45.838 años	21.000.000 años

Política de contraseñas

Muchas organizaciones poseen políticas de definición de contraseñas, que comprenden una serie de restricciones, como:

- Longitud mínima,
- Duración mínima y máxima,
- No reutilizar el nombre de usuario o parte del mismo,
- Guardar histórico de contraseñas,
- Utilizar mayúsculas, minúsculas, números, caracteres especiales,
- Prevenir su reutilización.

Control de Accesos – Sistemas biométricos

Los sistemas biométricos se basan en características físicas del usuario a identificar o en patrones de conducta.

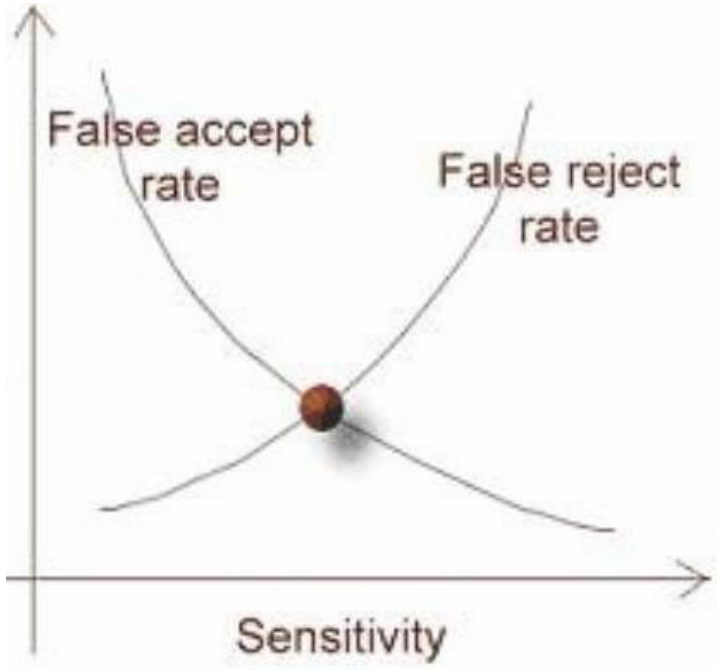
El proceso general de autenticación sigue unos pasos comunes a todos los modelos de autenticación biométrica:

- Extracción de ciertas características de la muestra (por ejemplo, el detalle de una huella dactilar).
- Comparación de tales características con las almacenadas en una base de datos.
- Finalmente la decisión de si el usuario es válido o no.

Sistemas Biométricos - Sensibilidad

La mayoría de los dispositivos biométricos tienen un ajuste de sensibilidad para que puedan ser configurados de manera que operen en forma más sensible o menos sensible.

- Tasa de Falsos Rechazos (FRR): Cuando un dispositivo es demasiado sensible, ocurre un error Tipo 1, es decir, un sujeto válido no es autenticado.
- Tasa de Falsas Aceptaciones (FAR): Cuando un dispositivo no es lo suficientemente sensible, ocurre un error Tipo 2, es decir, un sujeto inválido es autenticado.
- El punto en el cual FRR=FAR es conocido como Crossover Error Rate (CER).
- El nivel CER es usado como un estándar para evaluar la performance de los dispositivos biométricos.

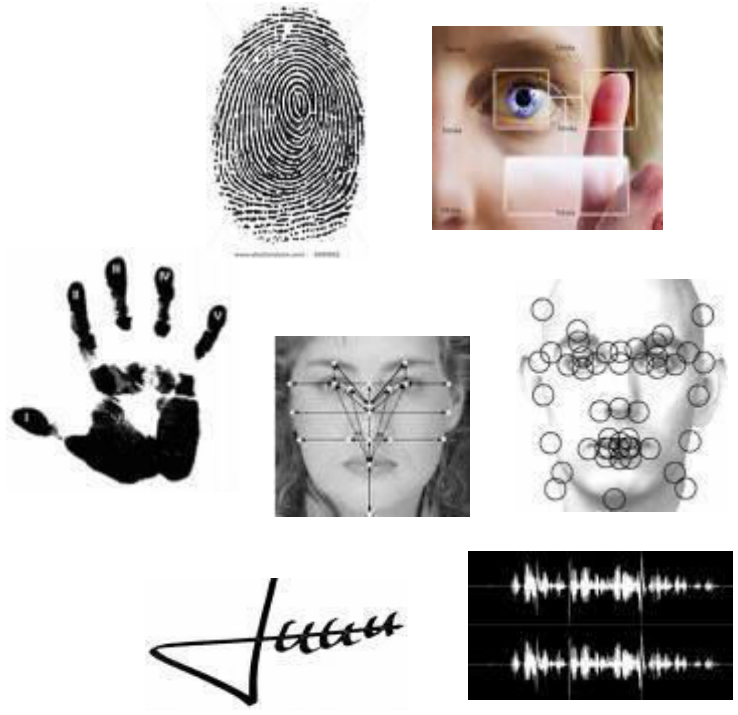


Sistemas Biométricos – los mas utilizados

Fuente: EvaluandoERP.com

Entre los mas utilizados podemos encontrar:

- Huella digital
- Reconocimiento facial
- Geometría de la mano
- Reconocimiento de iris
- Reconocimiento de retina
- Reconocimiento de la palma
- Dinámica de la firma a mano alzada
- Verificación de voz



Sistemas Biométricos – Criterios de Selección

Además de los costos hay puntos críticos a determinar a la hora de elegir un sistema biométrico como método de control de acceso:

- Aceptación del usuario
- Enrollment time (tiempo de registro)
- Throughput time (tiempo de proceso)
- Precisión

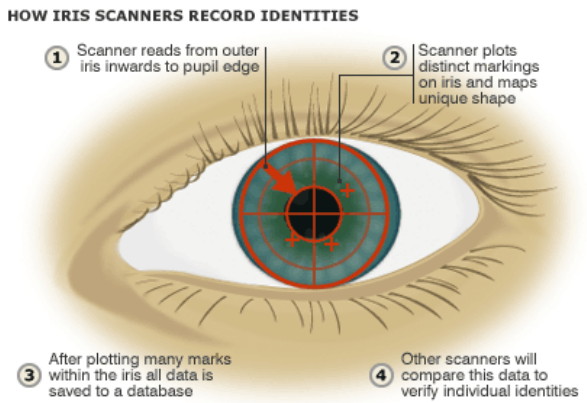
Adicionalmente también son importantes:

- Facilidad de implementación
- Tamaño y manejo de las muestras

Sistemas Biométricos – Criterios de Selección

Los más aceptados por los usuarios, por orden, son:

- Iris Scan
- Keystroke Dynamics (Type Sense)
- Signature Dynamics
- Voice Verification



Iris Scan

- Facial Recognition
- Fingerprint
- Palm Scan
- Hand Geometry
- Retina Scan

Keystroke Dynamics (Type Sense)

Sistemas Biométricos – Criterios de Selección

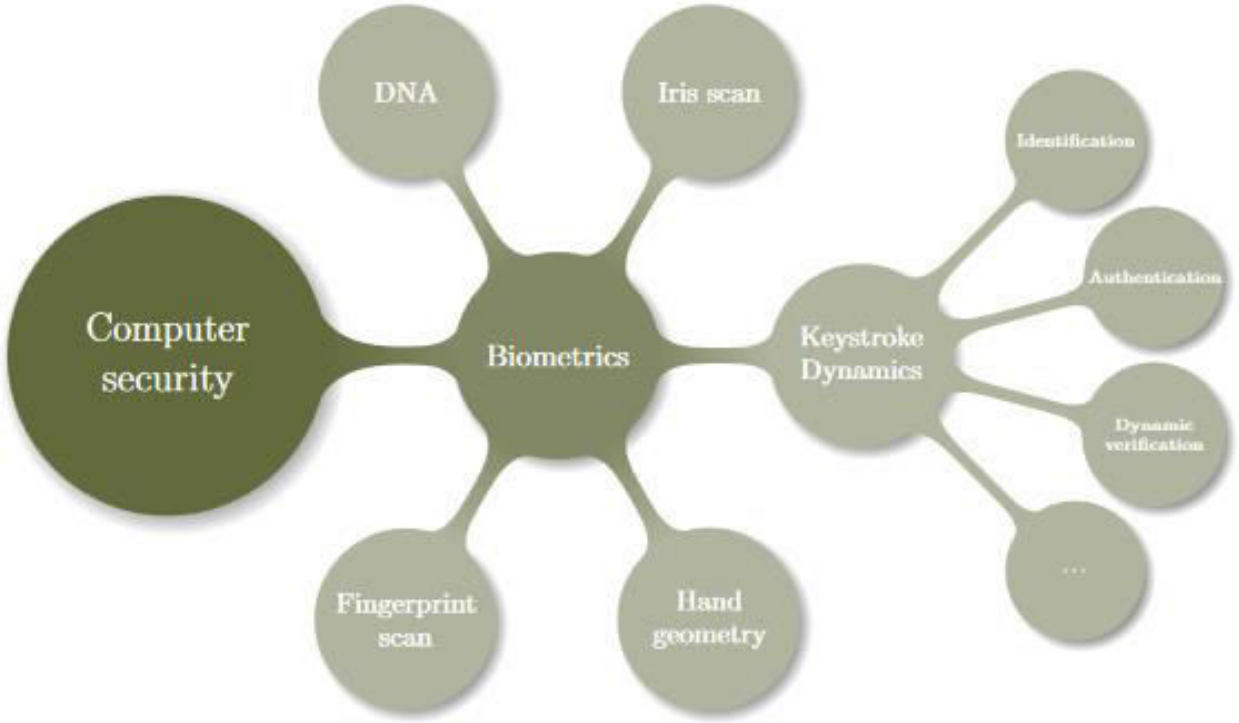


Figure 1.1: Keystroke Dynamics in the field of Computer Security

Sistemas Biométricos – Criterios de Selección

Enrollment (Registro de la Muestra)

- Es el proceso en el cual se toma la muestra del atributo físico del individuo, la cual será almacenada en una base de datos sobre la cual se verificará posteriormente su identidad.
- Muchas veces se necesita tomar repetidas muestras del atributo hasta que se logra finalmente una muestra válida.
- Esto puede hacer que los tiempos de enrollment sean altos y el sistema tenga baja aceptación.

Sistemas Biométricos – Criterios de Selección

Throughput (Proceso de Autenticación)

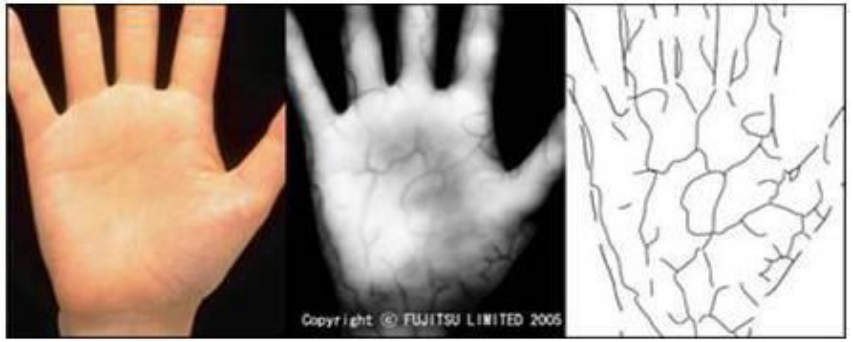
- Comprende el proceso propiamente dicho de identificación o autenticación de una persona.
- Es cuando la persona somete su característica física al dispositivo biométrico, y es comparada con la almacenada en la base de datos.
- Al igual que el proceso de enrollment, puede necesitarse repetir la operación de reconocimiento más de una vez, con lo cual los tiempos de respuesta serán altos, perdiendo funcionalidad.

Sistemas Biométricos – Criterios de Selección

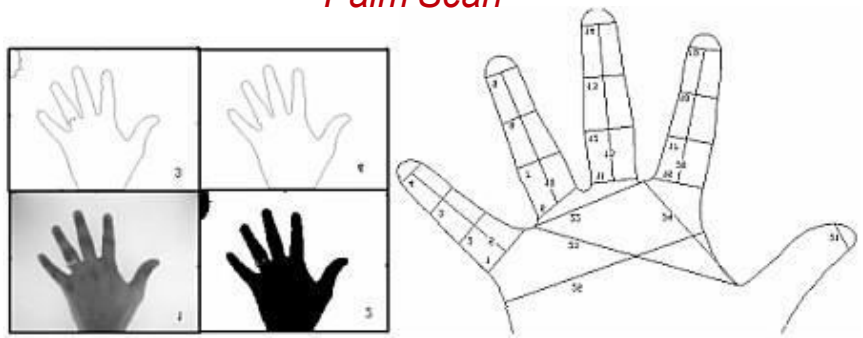
Precisión (Efectividad)

Los más efectivos, por orden, son:

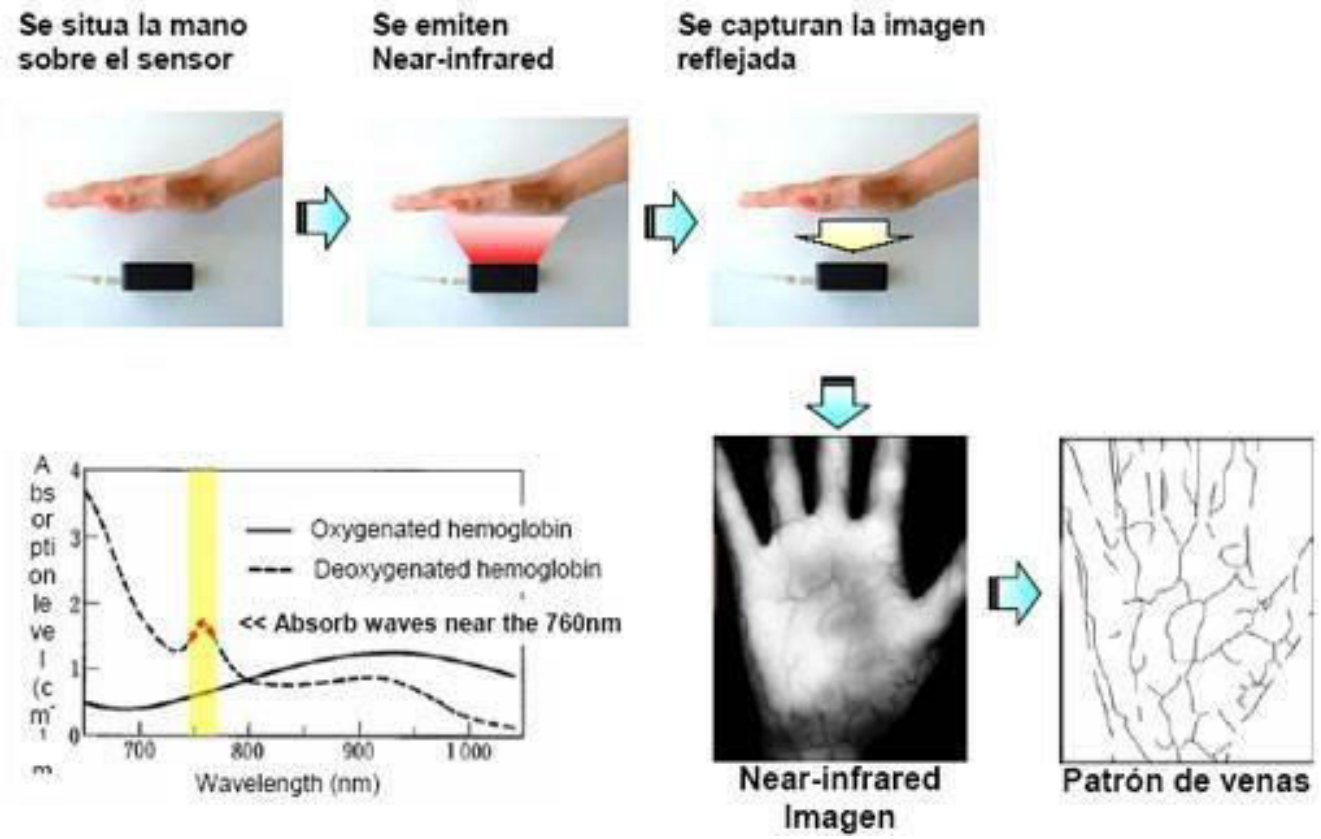
- Palm Scan
- Hand Geometry
- Iris Scan
- Retina Scan
- Fingerprint
- Voice Verification
- Facial Recognition
- Signature Dynamics
- Keystroke Dynamics



Palm Scan



Hand Geometry



Sistemas Biométricos – Ventajas

Entre las ventajas más significativas, encontramos:

- No pueden ser prestados / cedidos, como una llave o token y no se pueden olvidar como una contraseña.
- Buena relación entre facilidad de uso, tamaño de las plantillas, costo y precisión.
- Permiten la identificación única de un individuo, aún en casos de bases de datos de gran tamaño.
- Duran por siempre...
- Logran que los procesos de login y autenticación no requieran esfuerzo alguno.

Sistemas Biométricos – Desventajas

Entre las desventajas más importantes, encontramos:

- Todavía siguen siendo particularmente caros.
- Aún existe cierto rechazo o desconfianza por parte de los usuarios.

Sistemas Biométricos – Pérdida de privacidad

Seguimiento y Vigilancia: Permiten seguir y vigilar los movimientos de una persona.

Anonimicidad: Si la identificación está asociada a una base de datos, se pierde el anonimato al acceder a servicios a través de sistemas biométricos.

Profiling: La recopilación de datos acerca de transacciones realizadas por un individuo en particular, permite definir un perfil de las preferencias, afiliaciones y creencias de ese individuo.

Sistemas Biométricos - ejemplos

Reconocimiento de Rostro

- VeriLook SDK (software development kit)

Motor de identificación de rostros, disponible como SDK para MS Windows y Linux. Posee similares características al Verifinger SDK pero para el desarrollo de aplicaciones de reconocimiento facial.

Motor de identificación de rostros, disponible como SDK para MS Windows y Linux. Posee similares características al Verifinger SDK pero para el desarrollo de aplicaciones de reconocimiento facial.

- Velocidad de comparación: 80.000 rostros por segundo.
- Compara múltiples rostros simultáneamente.
- Fácilmente integrable a cualquier base de datos.
- Funciona con cualquier Webcam.
- No requiere hardware especial.
- Código fuente disponible.
- Puede utilizarse en computadoras con bajo poder de procesamiento.

Veri Finger

Motor de reconocimiento de Huellas Dactilares

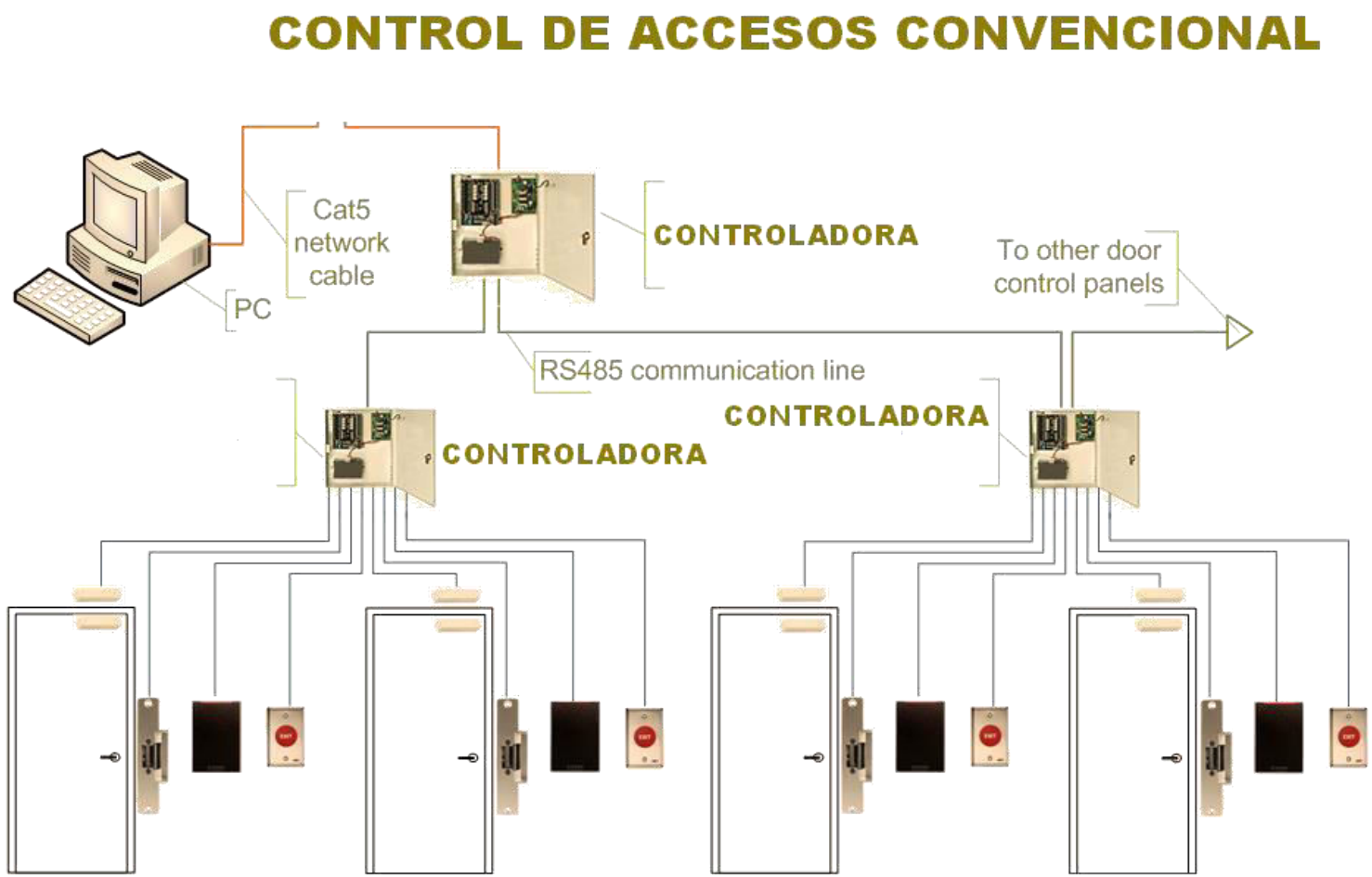
Kit de desarrollo SDK

El motor de identificación de huellas dactilares **VeriFinger** está destinado a desarrolladores e implementadores de sistemas biométricos. **VeriFinger** asegura alta confiabilidad en el reconocimiento de huellas dactilares, modos de comparación 1:1 y 1:N, una velocidad de comparación de hasta 30000 huellas por segundo, y requiere sólo 512 Kb de memoria. Disponible como **SDK** y como código fuente para MS Windows, Windows CE 3.0 y Linux.

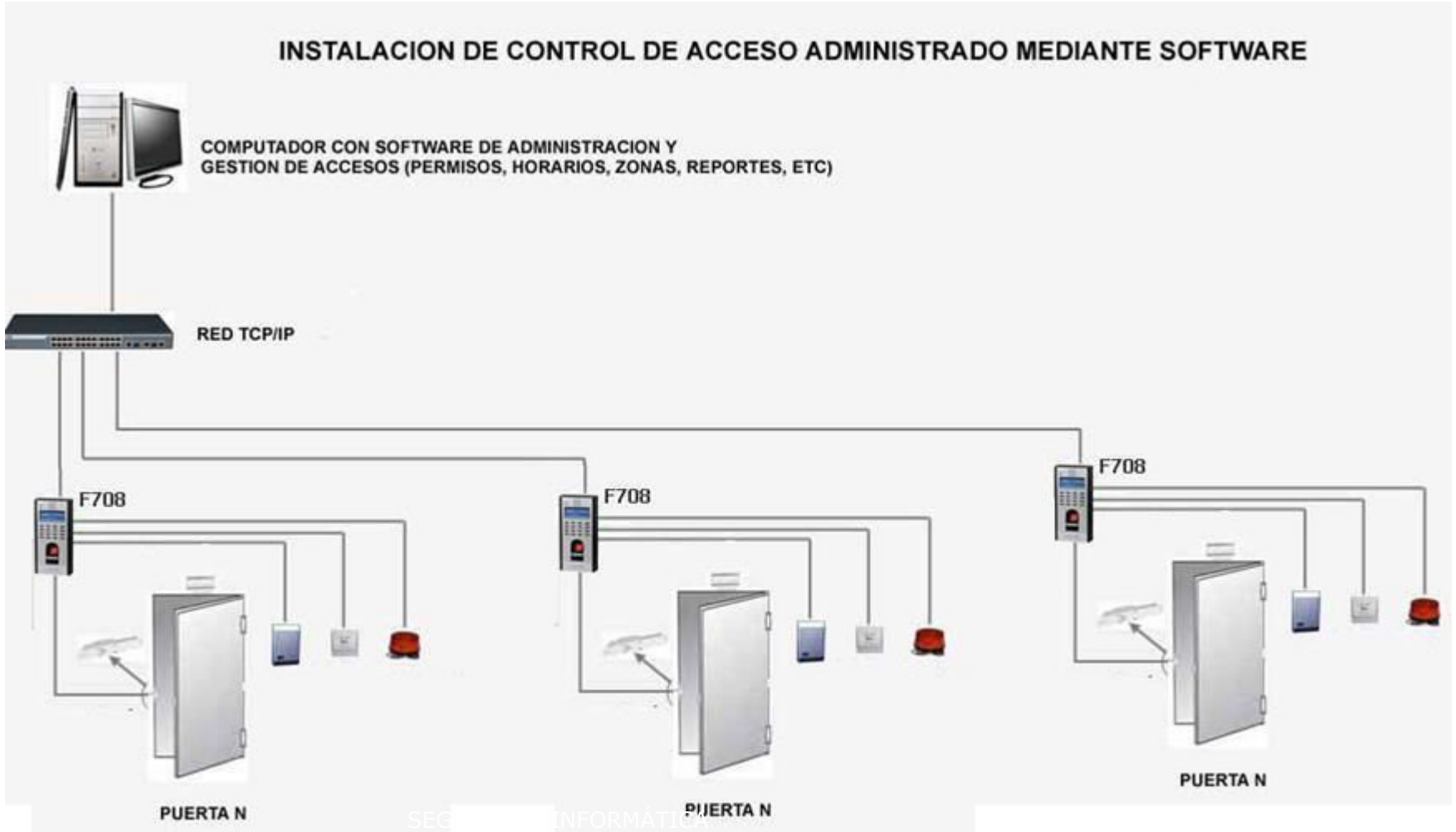
A continuación se puede observar, en dos ventanas, la imagen original de la huella y la misma imagen luego del filtrado y procesamiento por VeriFinger, con la posición y dirección de la minutia marcada por círculos rojos y líneas.

Fuente: http://www.neurotechnology.com
http://www.ex-cle.com.ar

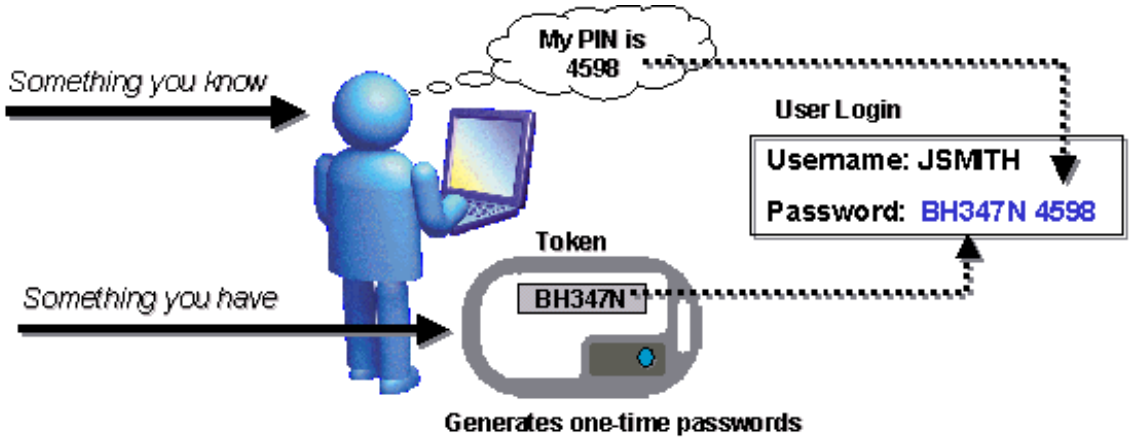
Sistemas Biométricos - ejemplos



Sistemas Biométricos - ejemplos



Control de Accesos - Tokens



Son dispositivos generadores de contraseñas que un sujeto lleva consigo. Los tokens pertenecen a la clase "Algo que usted tiene" (Factor de Autenticación Tipo 2).

Existen cuatro tipos de tokens:

- Estáticos
- Sincrónicos basados en tiempo
- Sincrónicos basados en eventos
- Asincrónicos basados en desafío/respuesta

Control de Accesos - Tokens

Estáticos

Requieren de un factor adicional para brindar autenticación, como ser una contraseña o una característica biométrica.

La mayoría de estos dispositivos almacenan una clave criptográfica como ser, una clave privada, credenciales de logon encriptadas, etc.

Son utilizados principalmente como técnica de identificación en lugar de autenticación.

Algunos ejemplos son:

- Smartcard
- Unidades de almacenamiento portables
- USB devices, etc

Control de Accesos - Tokens

Sincrónicos Basados en el Tiempo

Las tarjetas y el servidor tienen relojes que miden el tiempo transcurrido desde la inicialización.

Cada cierto tiempo se encripta y se obtiene un número que se muestra en la pantalla de la tarjeta; el usuario ingresa su PIN en el servidor junto con el número de su tarjeta.

Como el servidor conoce el momento de inicialización de la tarjeta también puede calcular el tiempo transcurrido; dicho valor encriptado deberá coincidir con el introducido por el usuario, para que éste sea aceptado.

Control de Accesos - Tokens

Sincrónicos Basados en Eventos

Las contraseñas se generan debido a la ocurrencia de un evento, por ejemplo se requiere que el sujeto presione una tecla en la tarjeta.

Esto causa que la tarjeta y el servidor avancen al próximo valor de autenticación.

El usuario debe ingresar su PIN en la tarjeta.

A partir del conjunto formado por el PIN y el nuevo valor de autenticación, se genera una nueva contraseña aplicando una función criptográfica (Ej.: DES, hash, etc.) a dicho conjunto, la que será enviada al servidor para su verificación.

Control de Accesos - Tokens

Asincrónicos Basados
en Desafío-Respuesta

1. El usuario remoto solicita autenticarse contra el servidor.

2. El servidor de token genera una cadena de dígitos aleatoria (desafío) y la envía al cliente remoto que intenta acceder a la red.

3. El usuario remoto ingresa esa cadena de dígitos, más su PIN en la tokencard, la cual le aplica una función criptográfica (Ej: DES) con una llave (key) almacenada, generando la contraseña (respuesta). El resultado de esa función es enviado nuevamente al servidor de token, quien realiza la misma operación.

4. Si el resultado es igual, el usuario es autenticado.

Control de Accesos - Tickets

Este mecanismo emplea una tercera entidad, aparte del cliente y el servidor, la cual brinda el servicio de autenticación.
Es importante aquí citar el concepto de Single Sign On (SSO).

Control de Accesos - Tickets

Overview

Ticket authentication allows remote systems to short-lived URLs that EZproxy will automatically recognize as being authorized to login and permit access to a resource with no need for EZproxy to check back with the program that creates the URL. A sample URL looks like this:

```
http://ezproxy.yourlib.org:2048/login?user=rdoe&ticket=a6911a5d0219f428b33e190a80818625%
24c20041222220203&url=http://www.somedb.com/
```

The ticket parameter on the URL contains a digital signature that EZproxy uses to verify that the URL was created by an authorized program. The ticket contains a time-stamp of when it was created. EZproxy can be configured to determine how old a ticket can be before it is considered expired.

Ticket directives for user.txt/ezproxy.usr

A sample entry in user.txt/ezproxy.usr is:

```
::Ticket
TimeValid 10
MD5 somekey
Expired; Deny expired.html
/Ticket
```

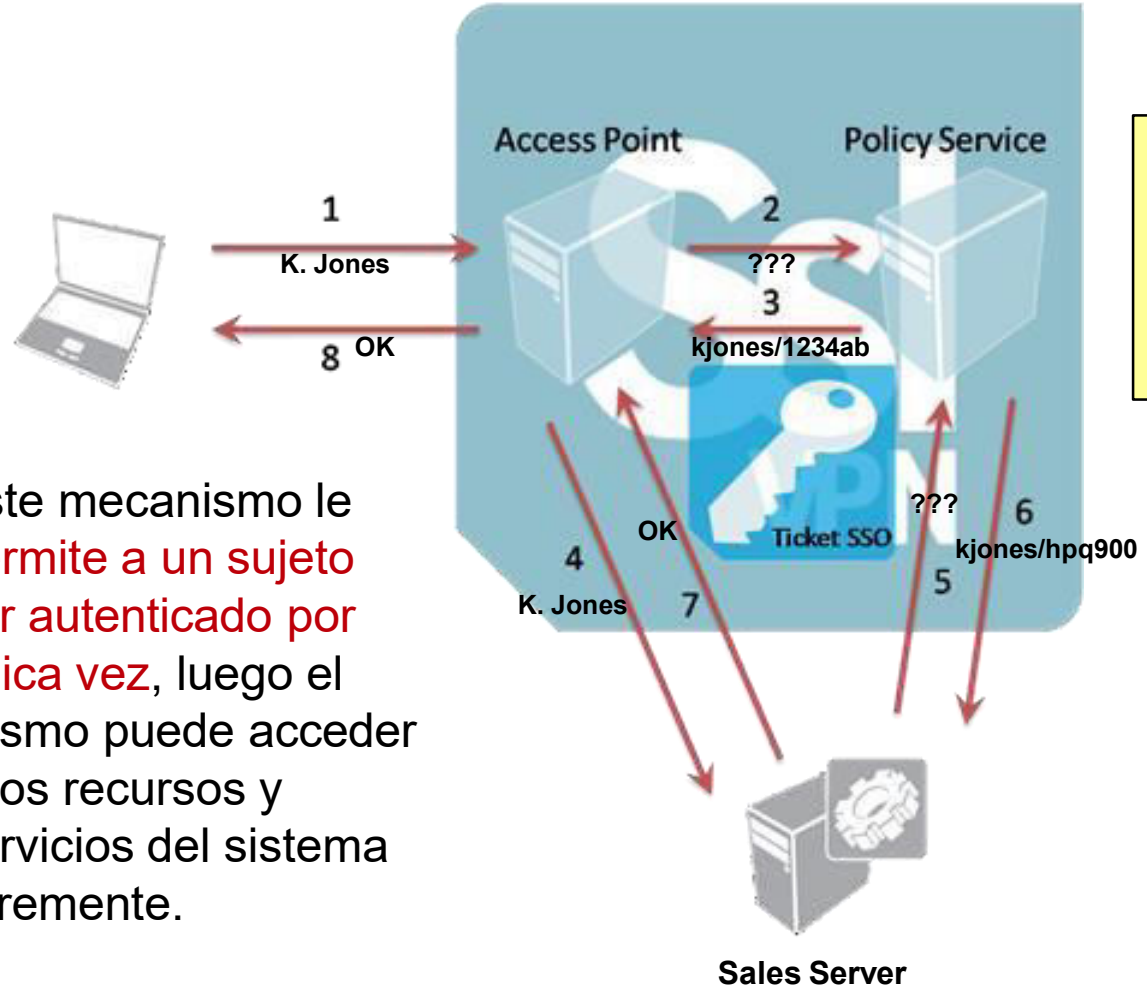
`TimeValid` must appear before `MD5` or `SHA1` and indicates the number of minutes a ticket should be considered valid.

`MD5` or `SHA1` indicate that the MD5 or SHA1 algorithms should be used to check the digital signature. Either must be followed by a string that is also used in the program that generates the ticket.

`Expired` is true if the ticket has expired. The use of a semi-colon in this example links the expired state of the ticket to the `Deny` action which tells EZproxy what file to present to the user if their ticket is expired. If the expired case is not handled, EZproxy ignores the ticket and proceeds on to the next part of user.txt/ezproxy.usr.

Control de Accesos - Tickets

Single Sign On (SSO)



K. Jones – Policy Service

Access Point: kjones / 1234ab
Sales Service: kjones / hpq900
Mail Service: kellyjones / 9876aa
…..
…..
…..

Este mecanismo le permite a un sujeto ser autenticado por única vez, luego el mismo puede acceder a los recursos y servicios del sistema libremente.

Control de Accesos - Tickets

Single Sign On (SSO)

Algunos ejemplos son:

Scripts: Cuando un usuario solicita acceso a un recurso, se corre un script en background que ejecuta comandos para autenticarse contra el recurso.

SESAME: Utiliza criptografía simétrica y asimétrica para proteger el intercambio de datos. Gestiona la identidad del sujeto, capacidades de acceso para cada objeto, tiempo de acceso, tiempo de vida del certificado.

KryptoKnight: Relación P2P. Implementa: administración, autenticación, distribución de llave, confidencialidad, integridad.

Clientes "Delgado": Terminales "bobas" que descargan el sistema operativo, el perfil y la capacidad funcional a utilizar en la sesión establecida.

Servicios de Directorio: BD jerárquica que identifica recursos en una red (nombre, ubicación lógica y física, sujetos que pueden acceder, operaciones que pueden ser realizadas, etc. Algunos ejemplos son: LDAP, NDS y MS Active Directory.

Kerberos: Protocolo de autenticación que permite verificar identidades mutuamente de manera segura. La arquitectura de Kerberos está basada en tres objetos de seguridad: Clave de Sesión, Ticket y Autenticador.

Autorización

Autorización

Pasos para Acceder a un Objeto La autorización determina si una entidad particular, que ha sido autenticada como la fuente de una solicitud, es de confianza para realizar la operación. La autorización podrá asimismo incluir controles (ej.: el momento en que la acción puede tener lugar o la ruta desde donde se solicita). Para que se produzca la autorización se debe dar lo siguiente:

La propiedad de la información – Debe estar asignada la propiedad de la información. Toda la información utilizada será del propietario del recurso. El propietario determina la clasificación adecuada y los controles de acceso. También es responsable de garantizar los controles adecuados para el almacenamiento, la manipulación y distribución de los datos. Los custodios de recibir el permiso de los propietarios y administrar el cuidado diario de los datos, realizando copias de seguridad. Los usuarios son quienes usan los datos (el objeto) para realizar su trabajo.

El principio del mínimo privilegio - Requiere que un usuario no posea mayores privilegios de lo necesarios para realizar su trabajo. Garantizar el mínimo privilegio es limitar al usuario a un dominio, determinando el conjunto mínimo de privilegios requeridos para realizar ese trabajo. Ej.: llave de encendido del auto vs. llave de apertura de puertas.

La segregación de funciones y responsabilidades - Requiere que no se permita la ejecución de operaciones a un único individuo dentro del set de operaciones. Las transacciones pueden ser estáticas o dinámicas.

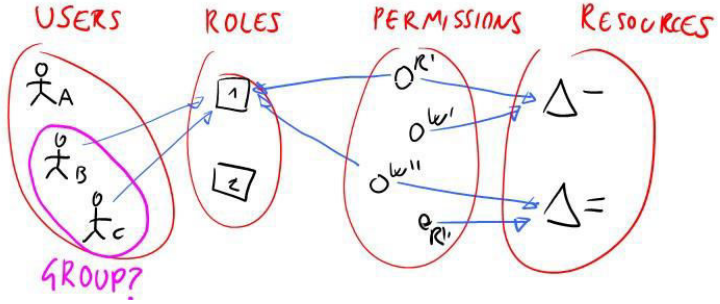
Autorización

Modelos de Control de Accesos

Una vez que el sujeto haya sido autenticado y su registro de actividad iniciado, debe ser autorizado para poder acceder a los recursos disponibles o ejecutar acciones.

Existen tres modelos principales de Control de Acceso, a saber:

1. **Mandatario** (MAC Mandatory Access)
2. **Discrecional** (DAC Discretional Access)
3. **Basado en Roles o No Discreciona** (RBAC Role Based Access)



Autorización

Modelo Mandatorio (MAC)

Se asignan funciones de los usuarios estrictamente de acuerdo a lo que define el administrador del sistema.

Es el método de control de acceso más restrictivo, porque el usuario final no puede establecer controles de acceso en los archivos.

El MAC es muy popular en ambientes/instalaciones altamente secretas, como la industria de defensa donde la perdida de confidencialidad puede afectar la seguridad nacional.

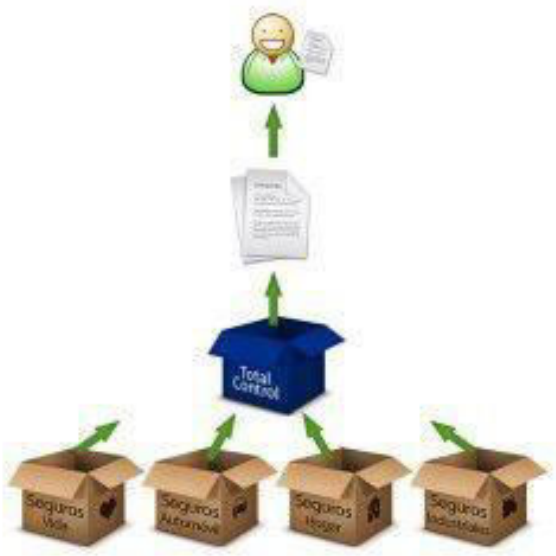
Autorización

Modelo Discrecional (DAC)

El DAC es el otro extremo, es el menos restrictivo de los tres modelos.

El usuario final tiene total libertad (permisos de administrador) para asignar los derechos a los objetos que desea.

Este nivel de control completo sobre los archivos puede ser peligroso porque si un atacante o malware comprometen la cuenta, el usuario malicioso o código tendrá un control completo también.



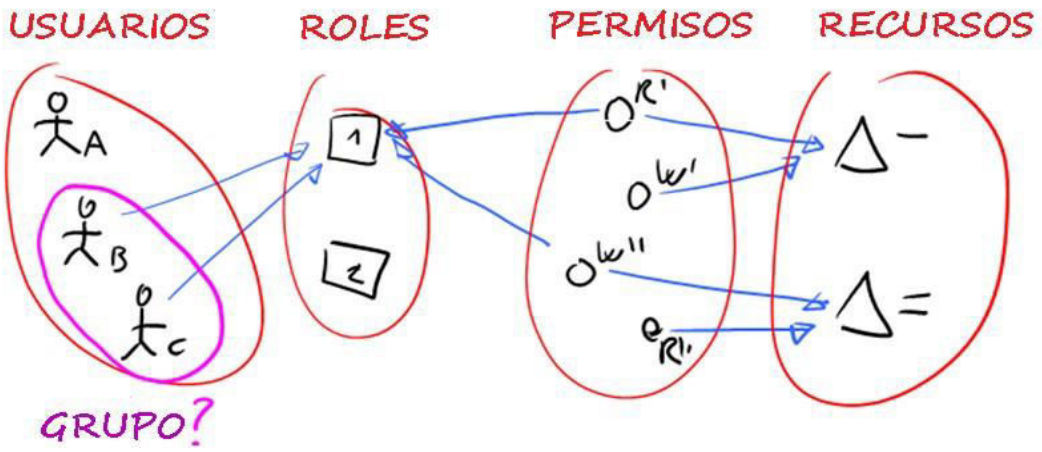
Autorización

Modelo Basado en Roles o No Discrecional (RBAC)

- Incorpora la gestión de arriba hacia abajo.
- Se mapean los permisos (derechos) a recursos dentro de la empresa; con los roles (funciones) de los usuarios, con lo que se les concede privilegios.
- Es el modelo de control de acceso basado en la "necesidad de conocer".

Por ejemplo, un administrador podría otorgar permiso de acceso a los recursos para los gerentes solamente.

Entonces al usuario se le tendría que asignar el rol de gerente para utilizar ese acceso.



Auditoría

Auditoría/Accounting

Pasos para Acceder a un Objeto Es el proceso de registrar eventos, errores, accesos e intentos de autenticaciones en un sistema.
Existen varias razones para que un administrador habilite esta funcionalidad:

- Detección de intrusiones,
- Reconstrucción de eventos y condiciones del sistema,
- Obtener evidencias para acciones legales,
- Producir reportes de problemas, etc.

El conjunto de acciones a ser auditadas esta formado por:

- **Eventos de Sistema**: Monitoreo de performance, Intentos de logon (exitosos y fracasados), ID Logon, Fecha y hora de cada intento de logon, Bloqueos de cuentas de usuario, Uso de herramientas administrativas, Uso de derechos y funciones, Modificación o eliminación de archivos críticos, etc.
- **Eventos de Aplicaciones**: Mensajes de error, Apertura y cierre de archivos, Modificación de archivos, Violaciones de seguridad en la aplicación, etc.
- **Eventos de Usuarios**: Identificación e intentos de autenticación, Archivos, servicios y recursos utilizados, Comandos ejecutados, Violaciones de seguridad.

AAA

Authentication/autenticación

Authorization/Autorización

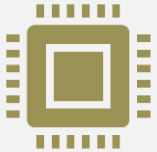
Accounting/Auditoría

RADIUS

Remote Authentication Dial-In User Service

RADIUS

Sistema de autenticación y cuentas.



Comprueba que la información transferida al servidor RADIUS, como el nombre de usuario y la contraseña, sea correcta, para autorizar luego el acceso al sistema.

Este método de autenticación se puede utilizar con un token, tarjeta inteligente, etc., para proporcionar autenticación de dos factores

RADIUS

El servidor Radius se encarga de verificar que la información del usuario que intenta acceder a la red es la correcta.

Si la solicitud es válida, el servidor completa la autenticación y envía la información de autorización requerida al cliente.

Si la solicitud no es válida, el servidor envía la información de error de autorización al cliente.

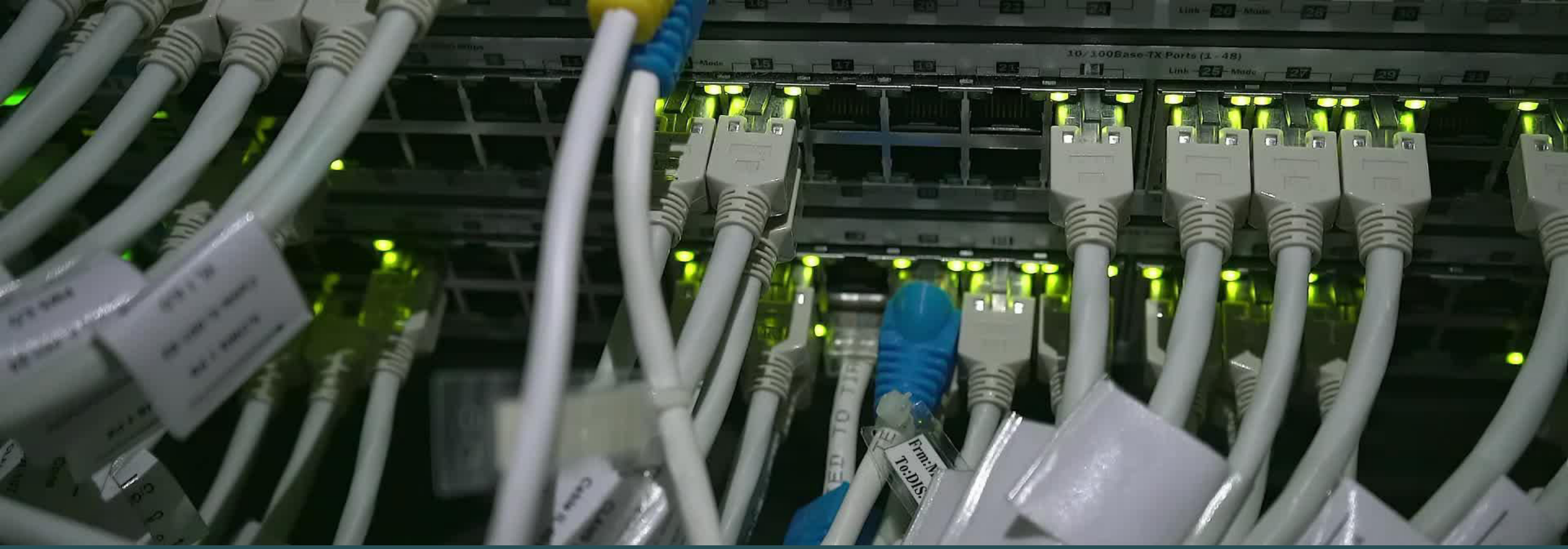
RADIUS

- La solicitud de autenticación y las credenciales se envían desde el dispositivo del usuario por medio del suplicante a un dispositivo de red avalado por RADIUS —piense en un punto de acceso WiFi o un servidor VPN.
- Después, el dispositivo de red avalado por RADIUS envía la solicitud de autenticación al servidor RADIUS para llevar a cabo la autenticación.
- Una vez recibida la solicitud de autenticación del usuario y las credenciales, el servidor RADIUS valida las credenciales del usuario contra la base de datos de los servicios de directorio asociados.
- Si las credenciales del usuario coinciden con la información almacenada en la base de datos del directorio asociado, se envían autorizaciones válidas al cliente de RADIUS para inicializar la conexión a la red.
- Si no, se envía una notificación de negación.
- En caso de que la autenticación resulte exitosa, el servidor RADIUS puede colocar al usuario en un **VLAN** determinado o solicitar un factor adicional de acceso vía **MFA**.

RADIUS

¿Qué ventajas tiene usar Radius?

1. Mejora la seguridad de la red.
2. Mejora el seguimiento de los accesos a la red basado en los nombres de usuarios de clientes.
3. Permite aplicar restricciones a un usuario concreto.
4. Los accesos a la red individuales están encriptados.
5. Es posible desconectar a un único usuario o dispositivo sin afectar al resto, sin cambiar la clave del resto.



TACACS

terminal access controller access control system

2023
SEGURIDAD INFORMÁTICA

TACACS

Protocolo de autenticación remoto propiedad de Cisco que se utiliza generalmente en redes que se comunican entre un servidor de acceso remoto y un servidor de autenticación para determinar los derechos de acceso del usuario a la red.

Este método de autenticación se puede utilizar con un token, tarjeta inteligente, etc., para proporcionar autenticación de dos factores.

TACACS+ vs. RADIUS: Differences Table

RADIUS	TACACS+
RADIUS stands for Remote Authentication Dial-In User Service.	TACACS+ is an abbreviation of Terminal Access Controller Access-Control System Plus.
Documented in RFC 2865.	Described in RFC 1492.
RADIUS uses User Datagram Protocol (UDP) as Transport Layer Protocol.	TACACS+ uses Transmission Control Protocol (TCP) as Transport Layer Protocol.
RADIUS uses UDP port 1812 or 1645 for authentication and port 1813 or 1646 for accounting.	TACACS uses TCP port 49 to communicate between the client and server.
RADIUS provides no support for the external authorization of commands.	TACACS+ provides control over the authorization of commands, allowing granular control.
RADIUS encrypts passwords only, leaving other information unencrypted.	TACACS+ encrypts all packets.
RADIUS bundles authentication and authorization, making it impossible to perform them separately. Accounting can be used separately.	TACACS+ separates Authentication, Authorization, and Accounting, making it possible to use different protocols for authentication and authorization or accounting.
RADIUS does not support command accounting.	TACACS+ supports command accounting.
RADIUS is an open-standard protocol that works with virtually all modern devices.	TACACS+ is Cisco's proprietary protocol and works with Cisco devices only.
RADIUS supports only one privilege level (limited to privilege mode)	TACACS+ supports multiple privilege levels.
RADIUS supports 802.1x. port-based network access control	TACACS+ does not support 802.1x port-based network access control.
RADIUS is mainly a network access protocol.	TACACS+ is mainly used for device administration using Access Control Server (ACS) servers.
RADIUS has no multiprotocol support – IP only.	TACACS+ has multiprotocol support (IP, Novell, NetBIOS, Apple, X.25).
RADIUS cannot authenticate network devices.	TACACS+ can authenticate network devices.

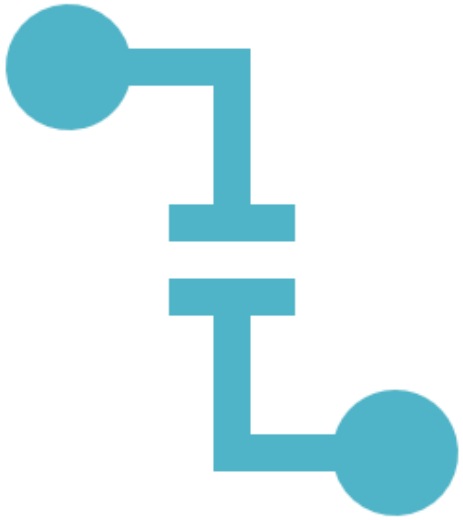
RADIUS Vs TACACS

La principal diferencia entre RADIUS y TACACS+ es que RADIUS es principalmente un protocolo de acceso a la red para la autenticación de usuarios, mientras que TACACS+ se utiliza sobre todo para administrar dispositivos de red como routers y switches.

Ventajas de RADIUS sobre TACACS+

- RADIUS funciona prácticamente con todos los routers y switches, mientras que TACACS+ sólo funciona con dispositivos Cisco.
- RADIUS es compatible con el control de acceso a la red basado en puertos 802.1x, mientras que TACACS+ no.
- RADIUS es mejor para fines de auditoría.

Ventajas de TACACS+ sobre RADIUS



- TACACS+ cifra todos los paquetes, lo que garantiza una mayor seguridad que RADIUS, que sólo cifra las contraseñas.
- TACACS+ proporciona control sobre la autorización de comandos, lo que permite un control granular de la autorización.
- TACACS+ permite utilizar distintos protocolos para la autenticación y la autorización, lo que mejora la flexibilidad.
- TACACS+ admite la auditoría de comandos y múltiples niveles de privilegios.

DIAMETER

DIAMETER

¿Qué es el protocolo Diameter?

Los servicios de AAA proporcionados por el protocolo Diameter constituyen la base de la administración de servicios en el sector de las telecomunicaciones, ya que deciden a qué servicios puede acceder un usuario, con qué calidad de servicio (QoS) y a qué coste.

El protocolo Diameter se centra en la capa de aplicación. Los nodos de AAA reciben un reconocimiento positivo o negativo por cada mensaje intercambiado entre los nodos y el TCP y el SCTP aseguran la fiabilidad.

Distintas funciones de las redes LTE e IMS hacen uso del protocolo Diameter, como la función de política y normas de cobro (PCRF), el servidor de abonados domésticos (HSS) y el sistema de cobro online (OCS).

DIAMETER

¿Por qué es importante el protocolo Diameter?

Desde la introducción de la tecnología basada en IP en las redes de telecomunicaciones, se ha elegido el protocolo Diameter como protocolo de AAA para todas las redes fijas y móviles. Diameter tiene una ventaja competitiva sobre las soluciones AAA anteriores (por ejemplo, RADIUS) y es la base de la red central del EPS (núcleo de paquetes evolucionado) compatible con la tecnología LTE (evolución a largo plazo).

El protocolo Diameter ha sido adoptado por muchos organismos de normalización, como 3GPP y ETSI NFV, como base para todas las funcionalidades de AAA en las redes de nueva generación. El protocolo Diameter es el único que admite mejoras en 4G, como la funcionalidad de transacciones en tiempo real. Otras ventajas son:

- Escalabilidad ilimitada para permitir el crecimiento
- Tolerancia a fallos para garantizar la entrega de mensajes
- Apoyo a agentes para definir claramente los agentes proxy, de redireccionamiento, de retransmisión o de traducción
- Transmisión segura de paquetes de mensajes en Diameter
- Transmisión fiable a través de TCP o SCTP (Stream Control Transmission Protocol)

DIAMETER

¿Cómo funciona el protocolo Diameter?

Cada host que implementa el protocolo Diameter puede actuar como cliente o servidor dependiendo de la arquitectura de la red.

El nodo de Diameter que recibe la petición de conexión del usuario actuará como cliente de Diameter.

Tras recibir las credenciales del usuario (nombre de usuario y contraseña), el nodo cliente envía un mensaje de petición de acceso a otro nodo de Diameter.

Este nodo servidor de Diameter autentifica al usuario en función de la información proporcionada.

Si la información se acepta, el usuario recibirá una respuesta de permiso de acceso a través del nodo cliente de Diameter correspondiente. Si se rechaza, el usuario recibirá un mensaje de denegación de acceso.

El protocolo Diameter también aumenta la seguridad del sistema de nombres de dominio (DNS) rastreando los servicios y recursos que se utilizan. En los entornos de nube, los servicios de AAA desempeñan un papel importante en la atención eficaz a las comunidades globalizadas de abonados.

LDAP

Lightweight Directory Access Protocol

LDAP

¿Qué es LDAP y para qué sirve?

LDAP (Lightweight Directory Access Protocol) o también conocido como «Protocolo Ligero de Acceso a Directorios» es un protocolo de la capa de aplicación TCP/IP que permite el acceso a un servicio de directorio ordenado y distribuido, para buscar cualquier información en un entorno de red.

LDAP

- Generalmente un servidor LDAP se encarga de almacenar información de autenticación, es decir, el usuario y la contraseña, para posteriormente dar acceso a otro protocolo o servicio del sistema.
- Además de almacenar el nombre de usuario y la contraseña, también puede almacenar otra información como datos de contacto del usuario, ubicación de los recursos de la red local, certificados digitales de los propios usuarios y mucho más.
- LDAP es un protocolo de acceso que nos permite acceder a los recursos de la red local, sin necesidad de crear los diferentes usuarios en el sistema operativo, además, es mucho más versátil.
- Por ejemplo, LDAP permite realizar tareas de autenticación y autorización a usuarios de diferentes softwares como Docker, OpenVPN, servidores de archivos como los usados por QNAP, Synology o ASUSTOR entre otros, y muchos más usos.

LDAP

- LDAP puede ser utilizado tanto por un usuario al que se pide unas credenciales de acceso, como también por las aplicaciones para saber si tienen acceso a determinada información del sistema o no.
- Generalmente un servidor LDAP se encuentra en una red privada, es decir, redes de área local, para autenticar las diferentes aplicaciones y usuarios, pero también podría funcionar sobre redes públicas sin ningún problema.

AD

Active Directory

2023
SEGURIDAD INFORMÁTICA

121

AD

Qué es Active Directory

Active Directory o también llamado AD o **Directorio Activo**, es una herramienta **perteneciente a la empresa de Microsoft** que proporciona **servicios de directorio** normalmente en una red LAN.

Lo que es capaz de hacer este directorio activo es proporcionar un servicio ubicado en uno o varios servidores **capaz de crear objetos como usuarios**, eq**uipos o grupos para administrar las credencias durante el inicio de sesión de los equipos que se conectan a una red**.

Pero no solamente sirve para esto, ya que también podremos administrar las políticas de absolutamente toda la red en la que se encuentre este servidor. Esto implica, por ejemplo, la **gestión de permisos de acceso de usuarios, bandejas de correo personalizadas**, etc.

Fundamentalmente **está orientada al uso profesional**, en entornos de trabajo con importantes recursos informáticos en donde se necesario administrar gran cantidad de equipos en cuanto a actualizaciones o instalación de programas o la creación de archivos centralizados para poder acceder a los recursos de forma remota desde las estaciones de trabajo.

Como entenderás, **es la forma ideal de centralizar muchos de los componentes típicos de una red LAN** sin necesidad de ir equipo por equipo y evitando que los usuarios puedan hacer lo que quieran en una red.

AD

Cómo funciona Active Directory

Los **protocolos** de red que utiliza Active Directory son principalmente **LDAP, DHCP, KERBEROS y DNS**.

Básicamente tendremos una especie de base de datos en la que se almacena información en tiempo real acerca de las credenciales de autenticación de los usuarios de una red.

Esto permite que todos los equipos estén sincronizados bajo un elemento central.

AD
Ejemplo

Veamos por ejemplo que hace Active Directory cuando un usuario de esta base de datos se registra en un equipo:

En el servidor Active Directory tendremos un usuario (objeto) compuesto por los típicos atributos que denotan su presencia, como son, el campo “Nombre”, el campo “Apellido”, “Email”, etc.

Pero es que además **este usuario pertenecerá a un grupo determinado**, el cual tiene determinados privilegios como el acceso a impresores de red que están almacenadas con un campo “Nombre”, “Fabricante”, etc.

El equipo cliente, está en comunicación con este servidor, así que el usuario, cuando arranca el equipo encontrará una pantalla de bloqueo como si de cualquier sistema se tratase.

Cuando ponga su usuario y contraseña, este no estará físicamente en el equipo, sino que estará ubicado en este servidor.

El cliente solicitará las credenciales al servidor Active Directory para que este las verifique, y si existen, enviará la información relativa al usuario al equipo cliente.

En este momento el usuario iniciará sesión de forma aparentemente normal en su equipo. tendrá sus archivos personales típicos almacenados en el disco duro. Pero según el grupo al que pertenezca, también tendrá acceso a recursos de la red como la impresora.

Seguridad en Informática - Módulo 3

Docente: Carlos Cagnani

*Este documento fue realizado en concepto de capacitación en Formación Profesional y dictada para el **Sindicato CePETel** a contar del mes de mayo del año 2023.*

Hacking Ético

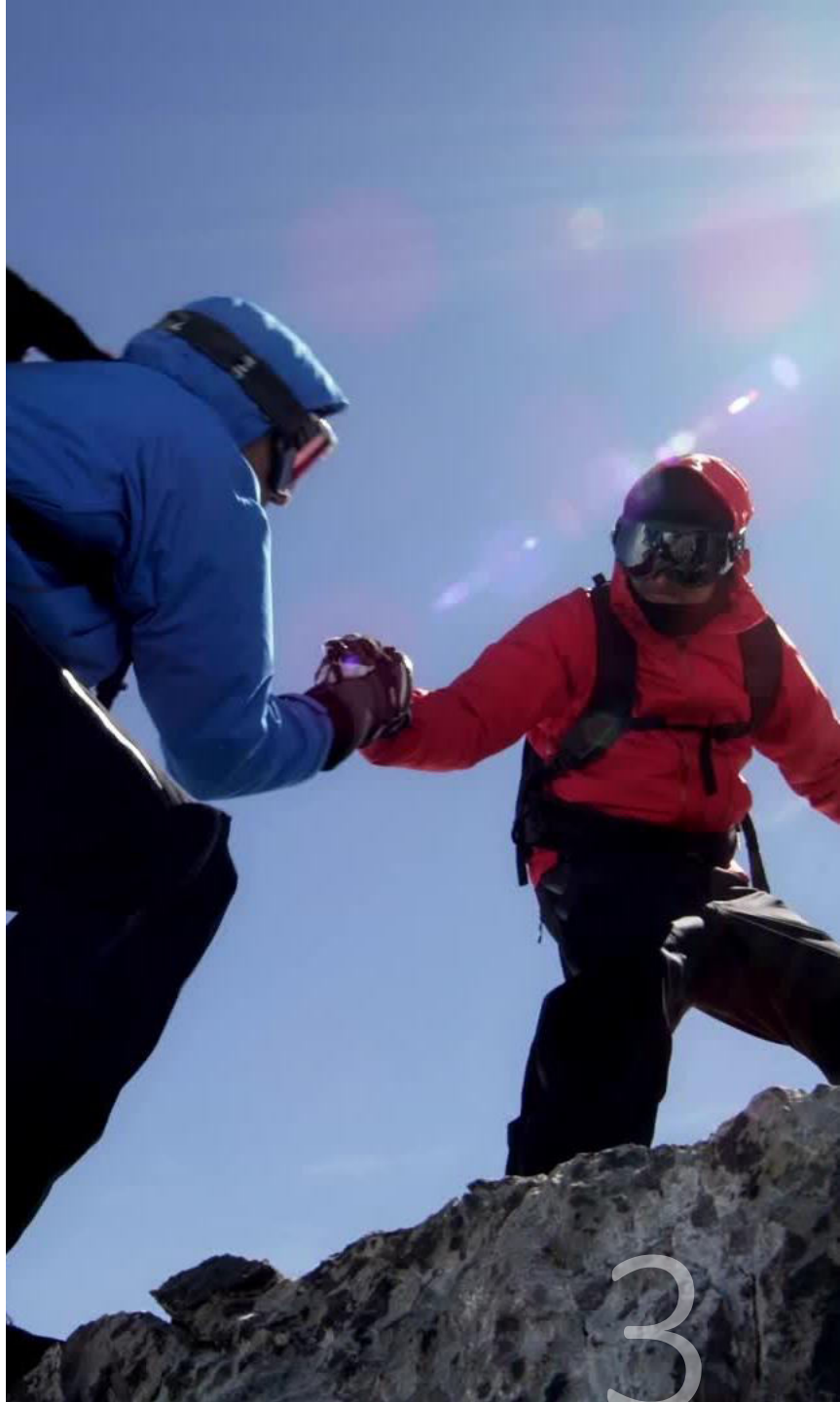
Índice de temas

1. Hacking Ético
2. Tipos
3. Hacker
4. Tipos de Hackers
5. Pen Testing
6. SIEM
7. NOC
8. SOC
9. Informática Forense

Hacking ético

Durante el paso de los años se ha evidenciado el crecimiento que han tenido las diferentes herramientas tecnológicas que se han desarrollado con el objetivo de brindar mayores facilidades y comodidades en las labores que desarrolla el hombre en su día a día.

Con el desarrollo de estas herramientas se generó un gran conocimiento tanto en su uso como aplicabilidad (una orientada a aprovechar y sacar utilidad de las herramientas creadas y otras personas poco éticas orientadas a aprovecharse de las vulnerabilidades de esas herramientas con fines poco éticos y fraudulentos de aquí es donde nacen dos conceptos Hacker y Cracker.



Cracker	*Hacker*
Robo de identidad	Accesos por conocimiento
Acciones fraudulentas	Fines pedagógicos
Cyber-Crimen	Hacking Ético
Cyber-Guerra	

Hacking ético

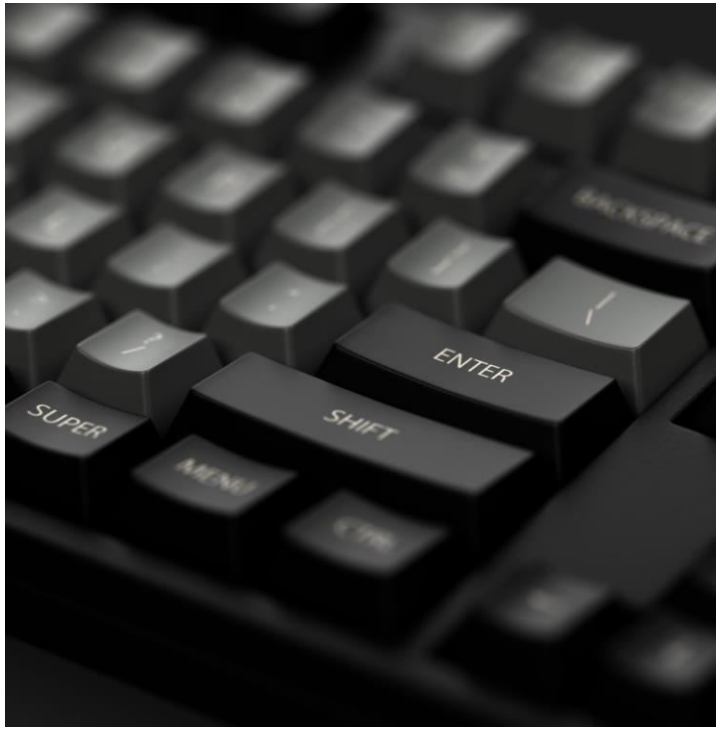
Metodología del hacking

Hacking ético

Definición de Hacking

Consiste en acceder desde algún lugar del ciberespacio a un ordenador valiéndose de deficiencias en los sistemas de seguridad aprovechando su vulnerabilidad u obteniendo contraseñas de acceso, haciéndose pasar por usuarios legítimos .

El hacking es una intromisión maliciosa que trata de hurgar entre datos buscando información válida, en conclusión, se trata de una intromisión ilegal a sistemas de computación ajenos.



Hacking ético

Definición de Hacking ético

- Es el término que se usa para hacer análisis de las vulnerabilidades de los sistemas para evitar o prevenir que un hacker los irrumpa o ataque
- Tiene como objetivo evaluar la seguridad.
- El hacking ético tiene dos significados:

  Un hobby de una persona que esta se interesa en el campo de seguridad vulnerabilidad.

  La otra es la persona que vive de esa profesión y que trabaja para empresas que contratan servicios de seguridad.

Hacking ético

Motivos del porqué del Hacking

- Por cuestiones de seguridad: para demostrar vulnerabilidades o debilidades de un sistema.
- Por inactividad del sistema: porque no se explota totalmente su capacidad
- Con fines de aprendizaje: para entrar a un sistema con el fin de instruirse.
- En pro de la sociedad: irrumpen para descubrir casos de abusos o delitos en contra de la sociedad.

Tipos de Hacking ético

1) **Hacktivistas**

Es una forma de protesta realizada por aficionados o profesionales de la seguridad informática (Hackers) con fines reivindicativos de derechos, promulgación de ideas políticas o quejas de la sociedad en general, haciendo uso de los fallos de seguridad de las entidades o sistemas gubernamentales.

Es decir, surge como un nuevo fenómeno cuya base ideológica es el intercambio y apertura del conocimiento y la vulneración de derechos de propiedad intelectual que aprisionan el desarrollo del conocimiento.

Así, motivados por un fin político o social aparecen los hacktivistas, que de forma personal o colectiva llevan a cabo acciones contra la seguridad de los sistemas para escribir códigos que promuevan ideologías políticas, libertad de expresión, derechos humanos y ética de la información, es decir pretenden producir resultados similares a los de cualquier otra forma de activismo social, como las protestas o la desobediencia civil.

Tipos de Hacking ético

1) **Hacktivistas**

Es una forma técnica mediante la cual un hacker informático está ingresando ilegalmente a cualquier sistema informático por cualquier motivo, ya sea social o político.

Esta actividad, un hacker informático puede dejar un mensaje muy grande en la página principal de cualquier sitio web conocido o cualquier otro mensaje importante para que el visitante vea ese mensaje y reaccione en consecuencia.

Puede mostrar cualquier tipo de discurso o cualquier mensaje social que pueda atraer a los usuarios.

Esto puede llevar a ingresar al sistema sin el consentimiento del objetivo.

Puede tener cualquier mensaje social, como el hacker ético es ético o no, lo que puede atraer a muchos usuarios

Tipos de Hacking ético
grupo hactivista

Tipos de Hacking ético grupo hactivista - lema

“El conocimiento es libre.

Somos anónimos.

Somos legión.

No perdonamos.

No olvidamos.

¡Esperadnos! “

Tipos de Hacking ético grupo hactivista – “logros”

A este grupo se les ha atribuido ataques a:

Webs oficiales del gobierno chino

Web de la justicia británica

Instituto Tecnológico de Massachusetts

Robo de perfiles de SonyPictures.com en 2011

Declararon la guerra al estado Islámico, después del atentado a Charlie Hebdo y Paris

Tipos de Hacking ético

2) **Cyber-Warrior**

Un cyber-warrior es una persona que participa en la guerra cibernética, ya sea por razones personales o por creencias patrióticas o religiosas.

La guerra cibernética puede perseguirse para defender los sistemas informáticos y de información, o para atacarlos.

Los guerreros cibernéticos vienen en diferentes formas, dependiendo de sus roles, pero todos se relacionan con la seguridad de la información de una forma u otra.

Tipos de Hacking ético

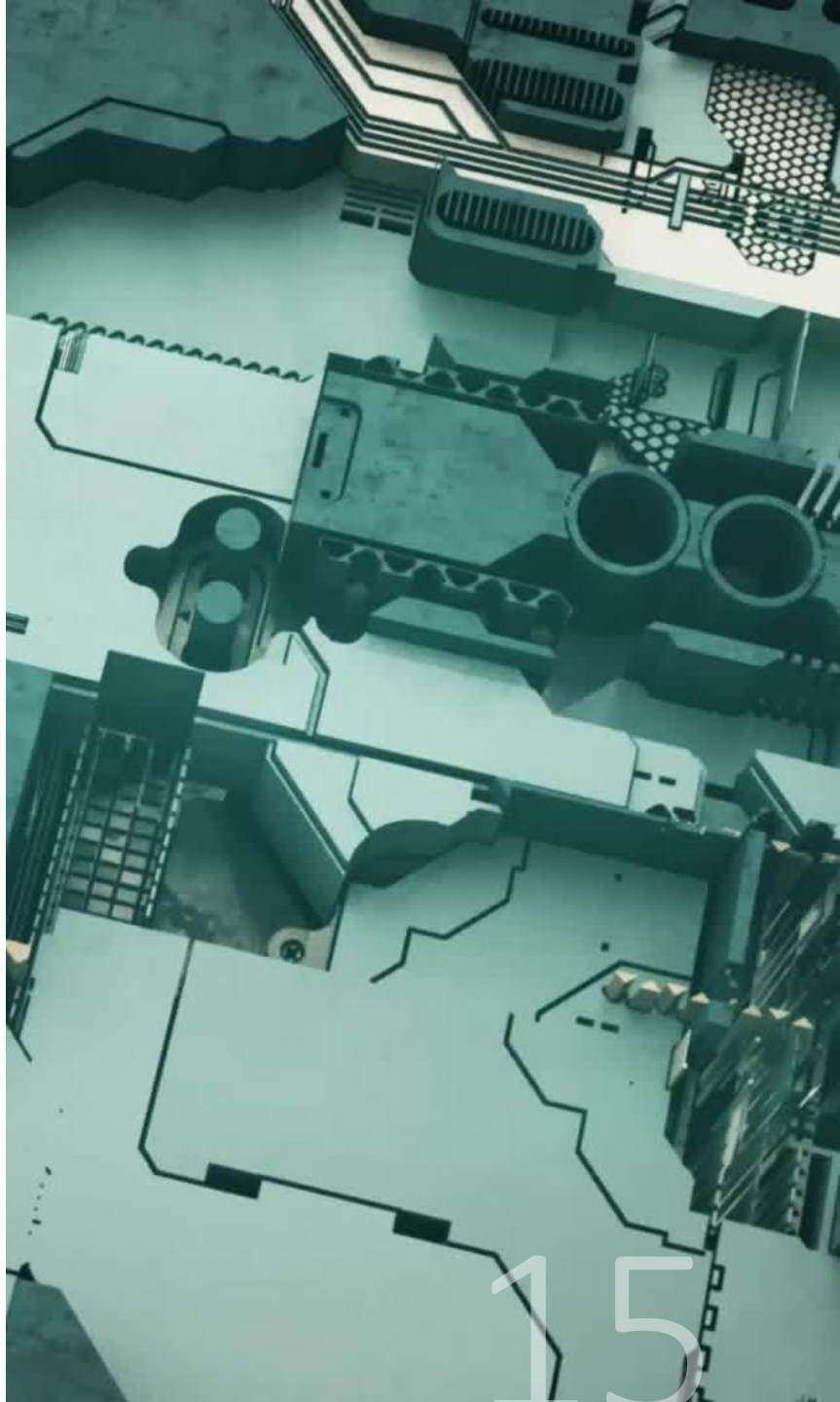
2) **Cyber-Warrior**

Los países que no pueden igualar a los EE. UU. En términos de tecnología militar han recurrido a la guerra cibernética, un método que todavía puede hacer mucho daño en términos de costo económico.

Varias agencias en los Estados Unidos están bajo ataque constante de numerosos países.

En respuesta, el ejército de Estados Unidos entrenando a veteranos de guerra y soldados heridos que ya pueden luchar en el campo en el arte de la guerra cibernética para convertirse en guerreros cibernéticos y continuar defendiendo el país en otro plano.

Esta interpretación del término se asemeja al hackeo ético.



Tipos de Hacking ético

2) **Cyber-Warrior**

La misión del grupo es:

- Evitar ataques a nuestra creencias y valores morales
- Nuestras acciones contra el estado y nuestro país
- Eventos que afecten adversamente a la conciencia pública.

ciberyihadistas.

- El **hacktivismo yihadista o ciberyihadismo** se retroalimenta con las **organizaciones yihadistas**.

Tipos de Hacking ético

3) **Pruebas de penetración** de caja blanca

Una prueba de penetración (prueba de pluma) a menudo se confunde con un análisis de vulnerabilidad, una auditoría de cumplimiento de una evaluación de seguridad.

Tipos de Hacking ético

3) Pruebas de penetración (Pen-Test) de caja blanca

Las pruebas de penetración de caja blanca también se denominan hackers de caja blanca.

Son los empleados contratados por la organización para ingresar a su sistema o red de computadoras actual.

Son los probadores legales de penetración. Están irrumpiendo legalmente el sistema o en la red de computadoras de la organización o de un individuo para ayudarlos, explicando las vulnerabilidades y las debilidades del sistema actual.

Las pruebas de caja blanca funcionan de la misma manera que los Cyber-Warrior. La única diferencia es que los Cyber-Warrior no tienen conocimiento del sistema o la red de Computadoras de la organización o del individuo, mientras que los hackers informáticos de caja blanca tienen pleno conocimiento del sistema, red o là computadora.

También se puede considerar que el ataque está siendo simulado por un interno de la organ1zación.

Tipos de Hacking ético

3) Pruebas de penetración de caja blanca

La penetración va más allá de las comprobaciones del sistema y hace lo siguiente:

- Lleva la información de exploración de vulnerabilidad a un nivel más alto.
- Si descubre vulnerabilidades durante un pen-test puede explotar esas vulnerabilidades para probar o refutar el potencial ataque del mundo real.
- Se enfoca en el individuo o equipo de evaluadores.
- Es importante tratar de entender los posibles motivos sobre las modalidades sofisticadas en este tipo de pruebas
- Busca información sobre la efectividad real de su sistema de seguridad
- Se trata de determinar si el sistema puede hacer frente a un hacker sigiloso e implacable
- Considera múltiples vectores de ataque contra el mismo objetivo

Tipos de Hacking ético

4) **Hacker ético o certificado**

Son profesionales con licencia o certificado en el campo de seguridad que los avala a realizer pruebas de vulnerabilidad.

Desempeñan funciones de hacker ético de caja negra o de caja blanca.

Son responsables de la seguridad y/o vulnerabilidad de las redes

Estas certificaciones o licencias son otorgadas por el Consejo Internacional de Consultores de Comercio Electrónico

Otras certificaciones

Certified Ethical Hacker por el EC-Council, CEH

Gerente de Certificado de Seguridad de la Información (CISM Certified Information Security Manager) por ISACA.

Profesional Certificado de Sistemas de Información de Seguridad (CISSP por ISC2)

Tipos de Hacking ético Hackers

- Hacker blanco White hat
- Hacker negro Black hat
- Hacker Gris Grey hat

WHITE HAT

Hace referencia a un hacker de sombrero blanco, el cual se rige por su ética, esta se centra en analizar, testear, proteger y corregir vulnerabilidades (bugs) en los sistemas de información y comunicación

Estos suelen trabajar en empresas de seguridad informática. De donde proviene la definición de hackers éticos o pentesters (test de penetracion)

BLACK HAT

Es una clase de hacker dedicado a la obtención y explotación de vulnerabilidades en sistemas de información, bases de datos, redes informáticas, sistemas operativos, etc. Para su propio beneficio, por ello, desarrollan programas como malware, virus, troyanos, crack`s, etc. que les ayuden a lograr sus objetivos.

GRAY HAT

Son hackers que están en el límite de lo que se puede considerar bueno y lo malo. Usualmente se infiltran en un sistema o servidor (que va en contra de la ley) para poner sus nombres o cambiar los nombres de las empresas. También pueden avisar a los administradores que su sistema ha sido ganado por ellos para que en un futuro puedan cubrir esos huecos y fallas y los arreglen para que otros hackers maliciosos no puedan entrar.

ETHICAL HACKING

DEFINICION

- Es el proceso por el cual, se utilizan las mismas técnicas y herramientas que un black hat para atacar a una organización y descubrir las vulnerabilidades de la misma.
- Para tal finalidad los ethical hackers han desarrollado las denominadas pruebas de penetración, (PEN-TEST por sus siglas en inglés).

Ethical Hacking

"para atrapar a un ladrón debes pensar como un ladrón".

Pentesting

Pruebas de penetración

PENTESTING

Conjunto de métodos y técnicas para la realización y simulación de un ataque en un escenario controlado, al cual se le practica un test de intrusión, para evaluar la seguridad de un sistema o de una red informática, y así encontrar los puntos débiles y vulnerables en dichos sistemas o redes.

PENTESTING
Porque realizar pruebas de penetración

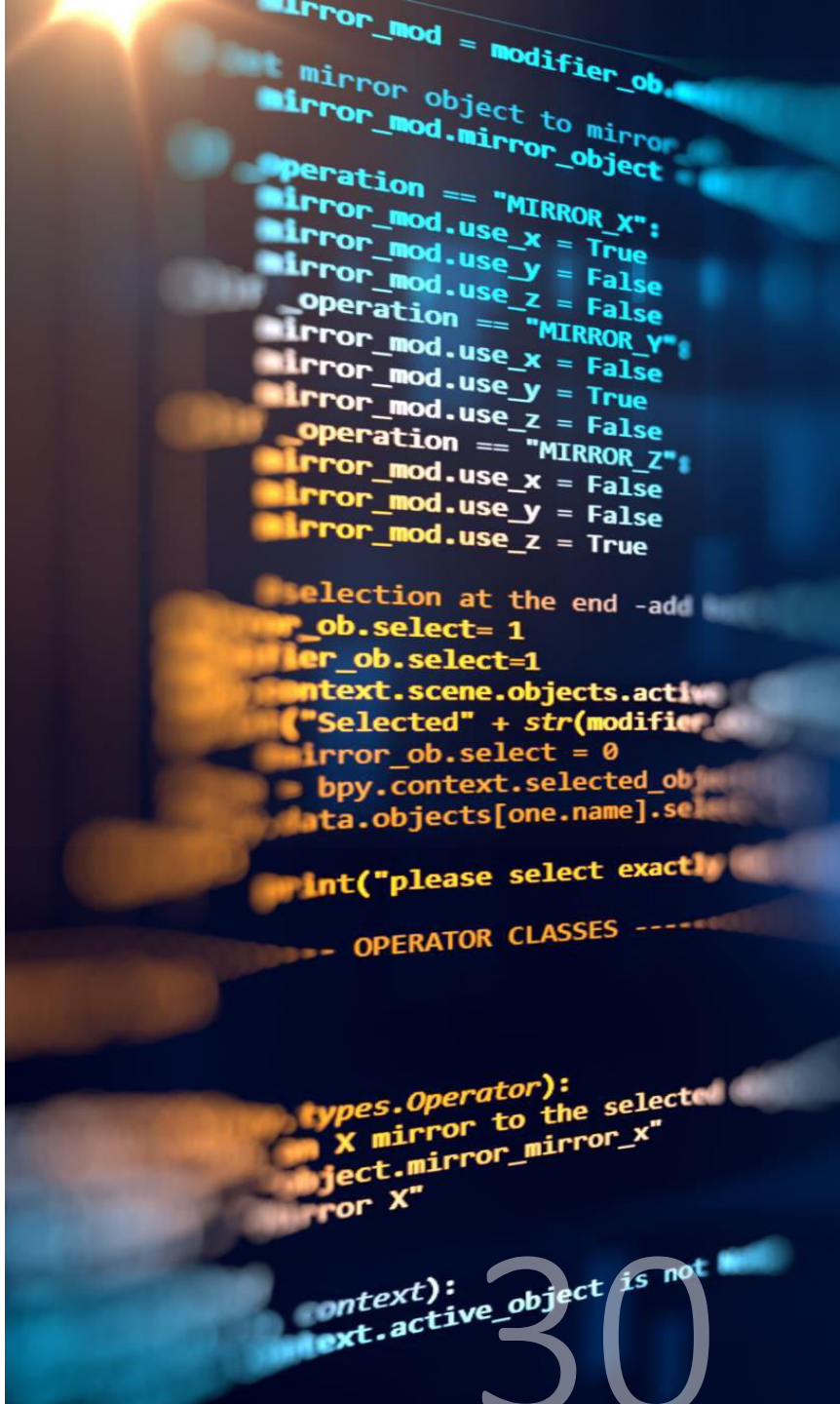
La seguridad de una organización es un aspecto cambiante. Una empresa puede alcanzar un nivel de protección óptimo en un momento determinado y ser totalmente sensible poco después, luego de realizar cambios en la configuración de un servidor o realizarse la instalación de nuevos dispositivos de red.

Asi mismo, continuamente aparecen nuevos fallos de seguridad en software existentes, que previamente se creían seguros.

TIPOS DE ATAQUES

ACTIVOS: Estos alteran y comprometen la disponibilidad, integridad, autenticidad de la información, afectando a los sistemas, redes y aplicaciones informáticas objetivo. Ejemplo: Sql injection/ alteración de la aplicación web, robo de información.

PASIVOS: Estos no alteran, ni modifican al sistema o red objetivo, solo se obtiene y compromete la confidencialidad de la información. Ejemplo: un sniffing de red.



ATAQUE INTERNO: es realizado desde el interior de la organización, por lo general suelen ser perpetrados por personal propio de la empresa, empleados inconformes o clientes que tienen accesos. Colaborados por malas configuraciones. Ejemplo, robo de información, instalación de software malicioso, etc

ATAQUE EXTERNO: es el que se realiza desde una fuente externa a la organización. Ejemplo internet o conexiones remotas, etc.

TÉCNICAS PARA UTILIZAR EN UN ATAQUE

- Denegación de servicio DoS
- Crackeo de contraseña por fuerza bruta
- Explotacion de vulnerabilidades
- Phising/ scam
- Secuestro de secciones en redes wifi
- Hijacking (secuestro), dominio, seccion, ip, entre otras
- Spoofing (suplantación), ip, DNS etc.
- Ingeniería social

TIPOS DE PRUEBAS PENTESTING

Pruebas de penetración con objetivo: se buscan las vulnerabilidades en partes específicas de los sistemas informáticos críticos de la organización.

Pruebas de penetración sin objetivo: consisten en examinar la totalidad de los componentes de los sistemas informáticos pertenecientes a la organización.

Pruebas de penetración a ciegas: en estas pruebas sólo se emplea la información pública disponible sobre la organización.

TIPOS DE PRUEBAS PENTESTING

- **Pruebas de penetración informadas:** Se utiliza información privada, otorgada por la organización acerca de sus sistemas informáticos. Se trata de simular ataques realizados por individuos internos de la organización que tienen acceso a información privilegiada.

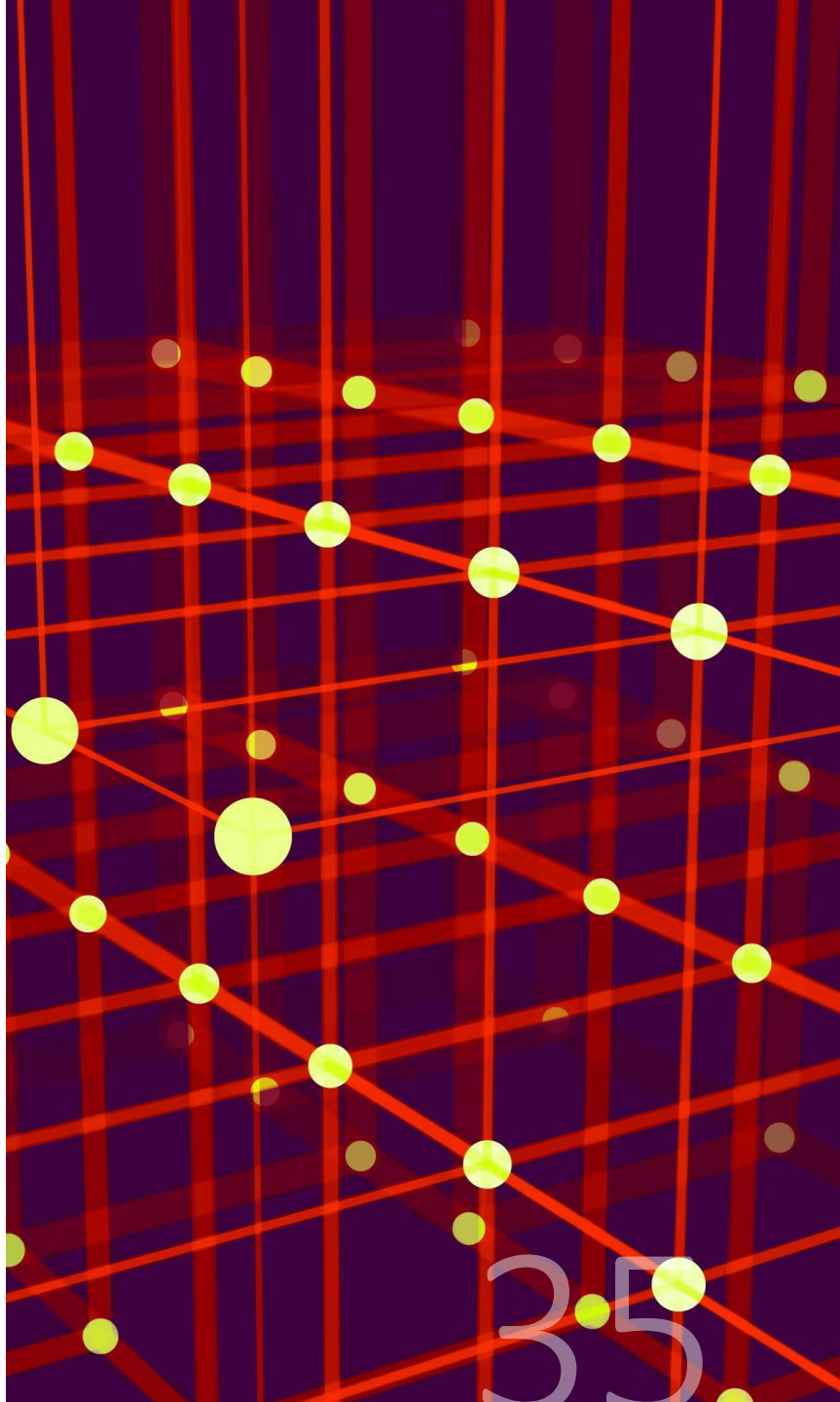
- **Pruebas de penetración externas**: son realizadas desde lugares externos a las instalaciones de la organización. Su objetivo es evaluar los mecanismos de seguridad perimetrales de la organización.

- **Pruebas de penetración internas**: son realizadas dentro de las instalaciones de la organización con el objetivo de evaluar las políticas y mecanismos internos de seguridad de la organización.

MODALIDADES DE LAS PRUEBAS

Red teaming: Prueba encubierta, es donde sólo un grupo selecto de directivos sabe de ella. En esta Modalidad son válidas las técnicas de "ingeniería social" para obtener información que permita realizar Ataque. Ésta prueba es la más real y evita se realicen cambios de última hora que hagan pensar que hay un mayor nivel de seguridad en la organización.

Blue teaming: El personal de informática conoce sobre las pruebas. Se aplica cuando las Medidas tomadas por el personal de seguridad de las organizaciones ante un Incidente, repercuten en la continuidad de las operaciones críticas de la organización, por ello es necesario alertar al personal para evitar situaciones de pánico y fallas en la continuidad de la actividad.



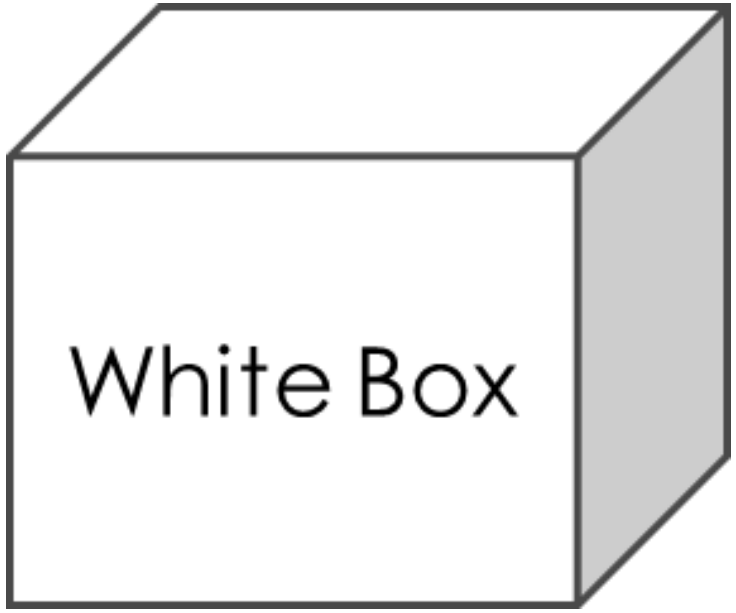
FASES DE LAS PRUEBAS DE PENETRACION

- Recopilación de información
- Descripción de la red
- Exploración de los sistemas
- Extracción de información
- Acceso no autorizado a información sensible o crítica
- Auditoría de las aplicaciones web
- Elaboración de informes
- Informe final

TIPOS DE PRUEBAS DE PENETRACIÓN

CAJA BLANCA

Se cuenta con el código fuente de la aplicación y la documentación. Se simula el ataque y el daño que podría ocasionar un trabajador interno enojado o desleal. En éste tipo de prueba, se encuentran cuestiones relacionadas a fallas lógicas, caminos mal estructurados en el código, el flujo de entradas específicas a través del código, funcionalidad de ciclos y condiciones, hoyos de seguridad interna y permite probar cada objeto y función de manera individual.

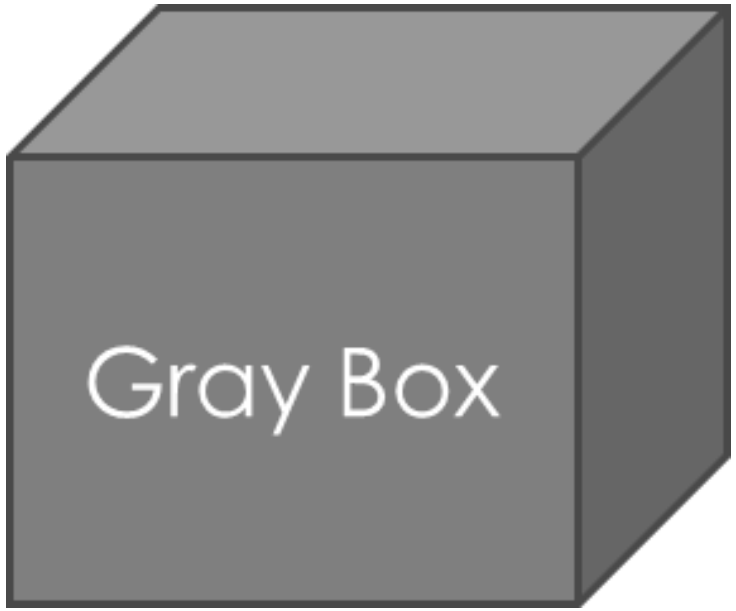


Caja Negra

Aquí, el tester no tiene acceso al código, ni a la documentación. Lo único con lo que cuenta para trabajar es con la versión descargable de manera pública de la aplicación. Se simula un ataque lanzado por un hacker; el vector de ataque más común, es la intercepción de tráfico y la inyección de contenido malicioso para obtener información. Éste tipo de pruebas, trata de explotar vulnerabilidad de tipo Cross Site Scripting(XSS), inyección de link e inyección de comandos SQL.

CAJA GRIS

Es una combinación de ambas, se realiza un análisis con la ventaja que se cuenta con el código y documentación, que sirven como guía.



BENEFICIOS DE UN ETHICAL HACKING

Ofrecer un panorama acerca de las vulnerabilidades halladas en los sistemas de información.

Deja al descubierto configuraciones no adecuadas en las aplicaciones instaladas en los sistemas que pudieran desencadenar problemas de seguridad en las organizaciones.

Identificar sistemas que son vulnerables a causa de la falta de actualizaciones.

Disminuir tiempo y esfuerzos requeridos para afrontar situaciones adversas en la organización.

HABILIDADES QUE DEBE TENER UN HACKER ÉTICO PENTESTER

- Tener conocimientos avanzados en programación (php, python, ruby, C, C++, .Net, java, etc.)
- Poseer conocimientos profundos de diversas plataformas como Linux, Windows, Unix, etc.
- Manejo de redes y protocolos, arquitecturas, etc.
- Dominio de hardware y software
- Ser experto en técnicas, metodos y herramientas de hacking
- Capacidad de análisis e investigación para proveer soluciones

HERRAMIENTAS PENTESTING

SAMURÁI PENTEST

Samurai Web Testing Framework es un entorno de trabajo basado en GNU/Linux Ubuntu, que ha sido pre-configurado para llevar a cabo test de penetración a aplicativos Web.

BACK TRACK

es una distribución GNU/Linux en formato Live CD pensada y diseñada para la auditoría de seguridad y relacionada con la seguridad informática en general.

WIFISLAX

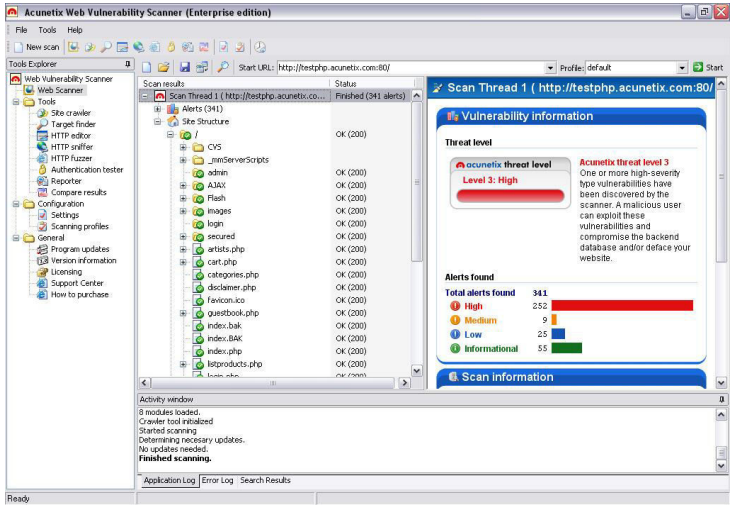
Incluye una larga lista de herramientas de seguridad y auditoría listas para ser utilizadas, entre las que destacan numerosos escáner de puertos y vulnerabilidades, herramientas para creación y diseño de exploits, sniffers, herramientas de análisis forense y herramientas para la auditoría wireless, además de añadir una serie de útiles lanzadores.

MATRIUX

Es una distribución de seguridad que consiste en un poderoso conjunto, de herramientas libres y de código abierto que pueden ser utilizadas para varios propósitos incluyendo, pero no limitado a penetration testing, hacking ético, administración de sistemas y redes, investigaciones forenses, pruebas de seguridad, análisis de seguridad, y mucho más.

ACUNETIX

Potente herramienta para MS Windows que detecta un gran número de vulnerabilidades, entre ellas Cross-Site Scripting, SQL Injection, CRLF injection, Code execution, Directory Traversal, File inclusion, busca vulnerabilidades en formularios de subida de archivos (file upload) y muchísimas más.



Mas Herramientas de Pentesting

Kali Linux

No es la primera vez que hablamos de Kali Linux en MuySeguridad. Ya os contamos que más que una herramienta de intrusión, lo que Kali Linux nos ofrece es una distribución de Linux completa orientada a la auditoría de seguridad informática y el hacking ético. No es la única por supuesto (ahí están ejemplos como el de Parrot OS) pero sin duda es la más conocida.

En su última versión, Kali Linux incluye novedades como la actualización del kernel Linux 4.19 y la suite de pentesting Metasploit 5.0, además de mejoras específicas de la edición ARM y dispositivos concretos como Raspberry Pi. Más allá de lo anterior, el conjunto de herramientas que ofrece es realmente completo.

En su versión «out of the box», Kali Linux ofrece a los usuarios más de 300 herramientas de pentatesting y seguridad, si bien está más pensado para atacar antes que defender una red informática.

https://www.kali.org/

nmap

nmap (network mapper) es una de las grandes veteranas del sector. Este escáner de puertos es una de esas herramientas que forman parte del ABC de cualquier auditor de sistemas. Algunas de las respuestas que proporciona son las siguientes: ¿qué puerto están abiertos en una máquina? ¿qué es lo que hay detrás de esos puertos?

Acceder a esa información es clave en las primeras fases de trabajo de cualquier pentatester. Utilizarla equivale a llamar a la puerta de una máquina que nos interesa y preguntar…¿hay alguien ahí? ¿quién es? En este sentido, tiene soporte para llamadas ping, es capaz de detectar protocolos de servicio y las versiones de las aplicaciones que se encuentran detrás de cada puerto o acceder al ID de un dispositivo.

https://nmap.org/

Metasploit

Metaploit es otra de esas navajas suizas que tiene que tener a mano cualquier pentatester que se precie de serlo. Su objetivo no puede ser más sencillo: encontrar agujeros de seguridad en todo tipo de redes, aplicaciones y dispositivos.

Para ello la herramienta permite en primer lugar cargar el código (o el destino) que se quiere «explotar» para a continuación, someterlo a uno o varios de los más de 900 exploits conocidos que hay registrado en su base de datos.

El uso de Metasploit suele seguir al de nmap (o similar), una vez el investigador ha accedido a más información sobre tipo de sistema operativo, aplicación o dispositivo de hardware que se encuentra «al otro lado». En caso de querer defender una red corporativa, el uso de Metasploit puede ser fundamental a la hora de entender dónde se encuentran los eslabones más débiles.

https://www.metasploit.com/

Wireshark

Wireshark es probablemente, en analizador de protocolos y tráfico de red más utilizado en el mundo. La herramienta captura tráfico en tiempo real y analiza a nivel «microscópico» qué es lo que está pasando.

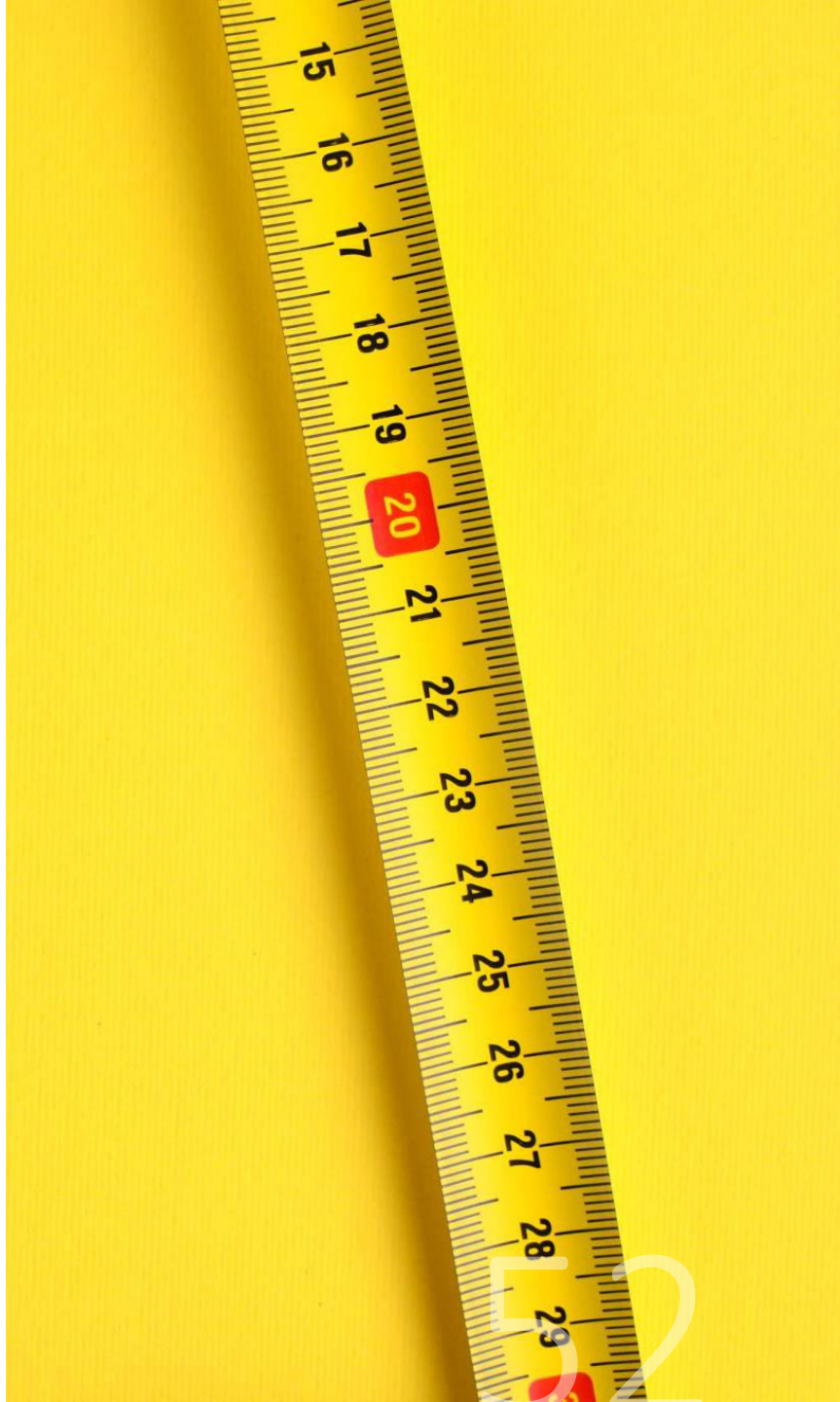
Aunque los pentatesters lo utilizan fundamentalmente para analizar el tráfico a nivel TCP/IP, la herramienta es capaz de analizar cientos de protocolos, de modo que el investigador pueda conocer qué es exactamente lo que se está moviendo dentro de una red.

https://www.wireshark.org/

sqlmap

No hay nada que le «siente mejor» a una base de datos que una inyección de código SQL. Y para demostrar que estamos en lo cierto, nada mejor que utilizar sqlmap. Si esta herramienta es tan interesante es porque automatiza el proceso de detectar y explotar fallos y brechas de seguridad en servidores BBDD basados en SQL. Es decir, casi todos.

En este sentido, sqlmap tiene soporte para MySQL, Oracle, PostgreSQL, Microsoft SQL Server, Microsoft Access, IBM DB2, SQLite, Firebird, Sybase, SAP MaxDB, Informix, HSQLDB y H2.



John the Ripper

Si quieres desencriptar ese archivo que «misteriosamente» ha llegado a tus manos, una buena forma de empezar es con John the Ripper.

Aunque siempre dependerá de la potencia de tu GPU, este proyecto open-source no debería de tener demasiados problemas a la hora de «reventar» la mayoría de las «contraseñas populares», realizando un ataque de «fuerza bruta» que se puede prolongar hasta el infinito si tienes paciencia. Evidentemente, no es lo ideal para contraseñas complejas o si el archivo ha sido encriptado con una buena herramienta.

https://www.openwall.com/john/

Hydra

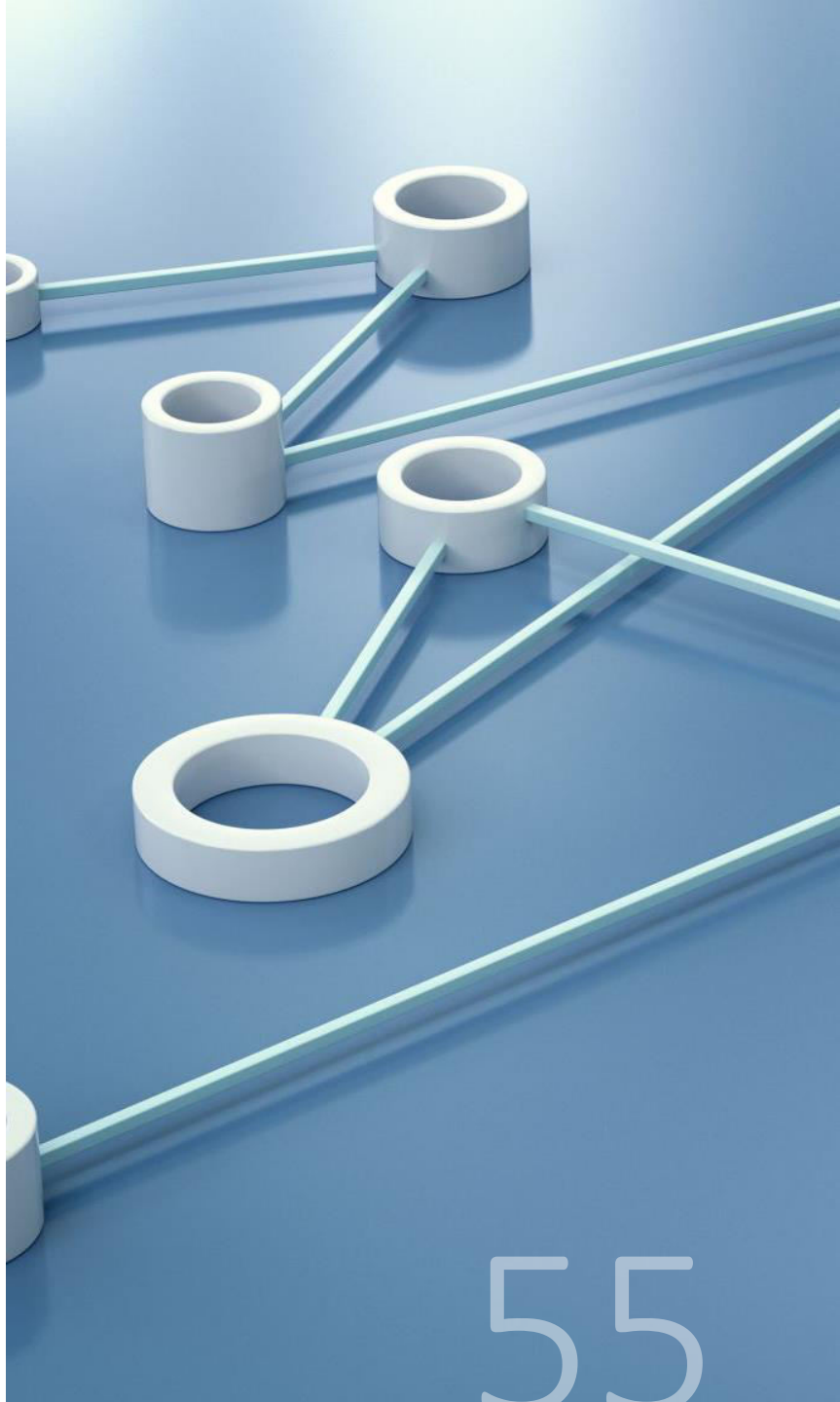
Mientras que John de Ripper intenta averiguar la contraseña de ese archivo que de alguna forma has obtenido, Hydra hace lo propio con cualquier servicio on-line. Para ello tiene soporte para protocolos como SSH, FTP, IMAP, IRC entre otros.

Para conseguir que funcione correctamente deberemos seleccionar el servicio que queremos «crackear», poner el nombre de usuario y subir un archivo que contenga las contraseñas que queremos probar.

aircrack-ng

¿Sabes cómo es de segura la red inalámbrica de la empresa? Si quieres descubrirlo y detectar si tiene alguna vulnerabilidad, nada mejor que probar con la herramienta aircrack-ng.

En muchos casos descubrirás que las principales vulnerabilidades se encuentran en una mala configuración de la red, el uso de contraseñas débiles o la falta de actualización del firmware de los dispositivos.



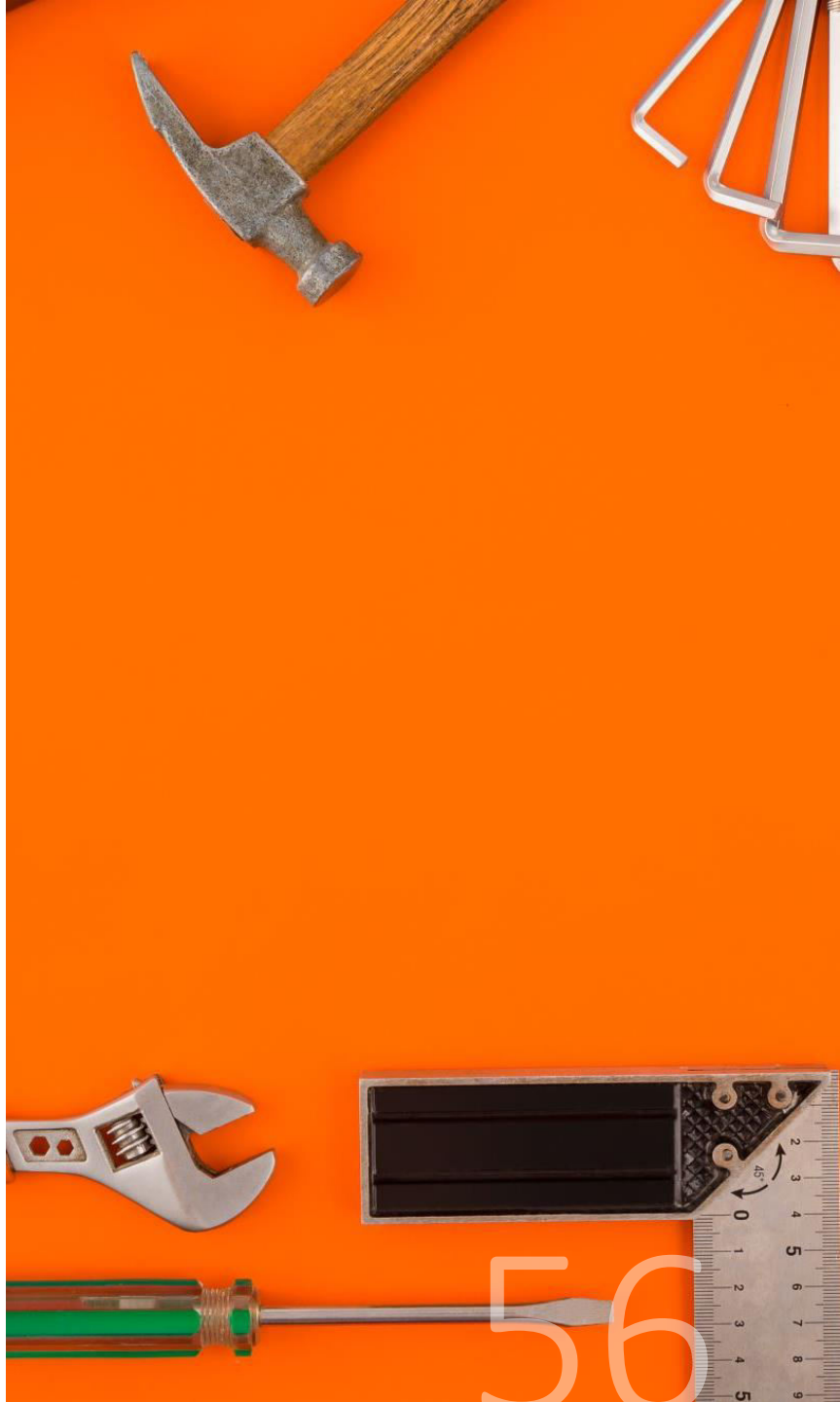
Burp Suite

Ninguna colección de herramientas de pentatesting está completa si no contamos con Burp Suite, uno de los analizadores de vulnerabilidades web más completo. A diferencia de las herramientas de las que hemos hablado hasta ahora, Burp Suite ni es un proyecto *open* source ni es gratuito.

Más bien todo lo contrario. Hablamos de una herramienta cara (3.999 euros) al año, y que se encuentra solo al alcance de aquellos que hacen de la auditoría de seguridad, su medio de vida. Es cierto que existe también una versión gratuita de la suite (la conocida como community edition), pero carece de la mayoría de los servicios que convierten a Burp Suite en un producto realmente interesante.

Si resulta tan caro es que existe una razón realmente válida. Basta apuntar una página web, para al soltar la «artillería» descubrir en unos segundos si resulta vulnerable ante alguno de los ataques que han sido reportados.

https://portswigger.net/burp

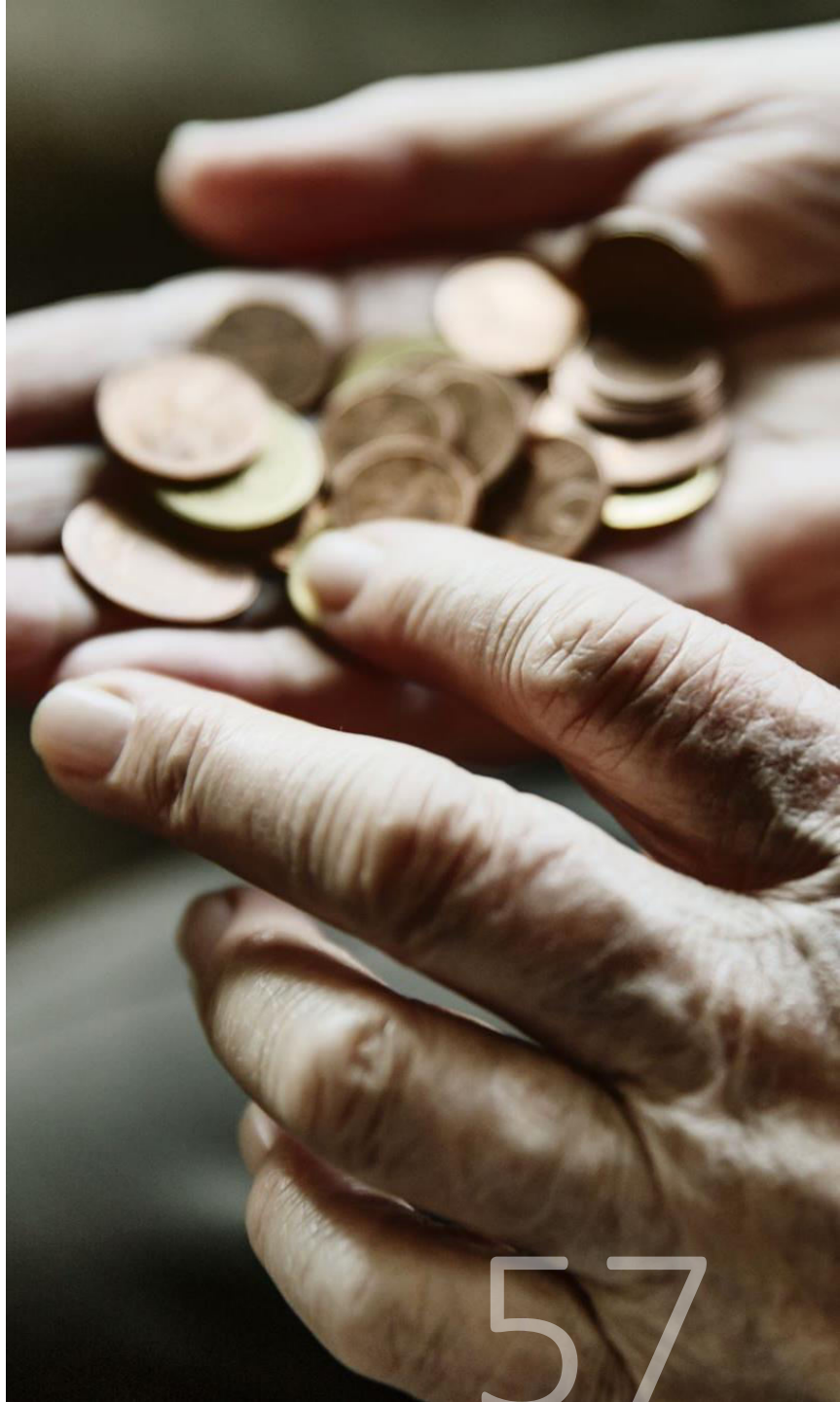


Zed Attack Proxy

Aquellos que no tengan o no quieran invertir 4.000 dólares anuales en Burp Suite, pueden «conformarse» con el gratuito Zed Attack Proxy (ZAP). No es ni tan completo ni tan fácil de utilizar, pero dispone de herramientas que lo convierten en un arma de intrusión igualmente efectiva.

ZAP se configura como un «man in the middle» que se sitúa entre nuestro navegador y la web que nos interesa inspeccionar, capturando el tráfico, para que a continuación podamos inspeccionarlo o modificarlo si descubrimos que reporta alguna vulnerabilidad.

https://www.zaproxy.org/



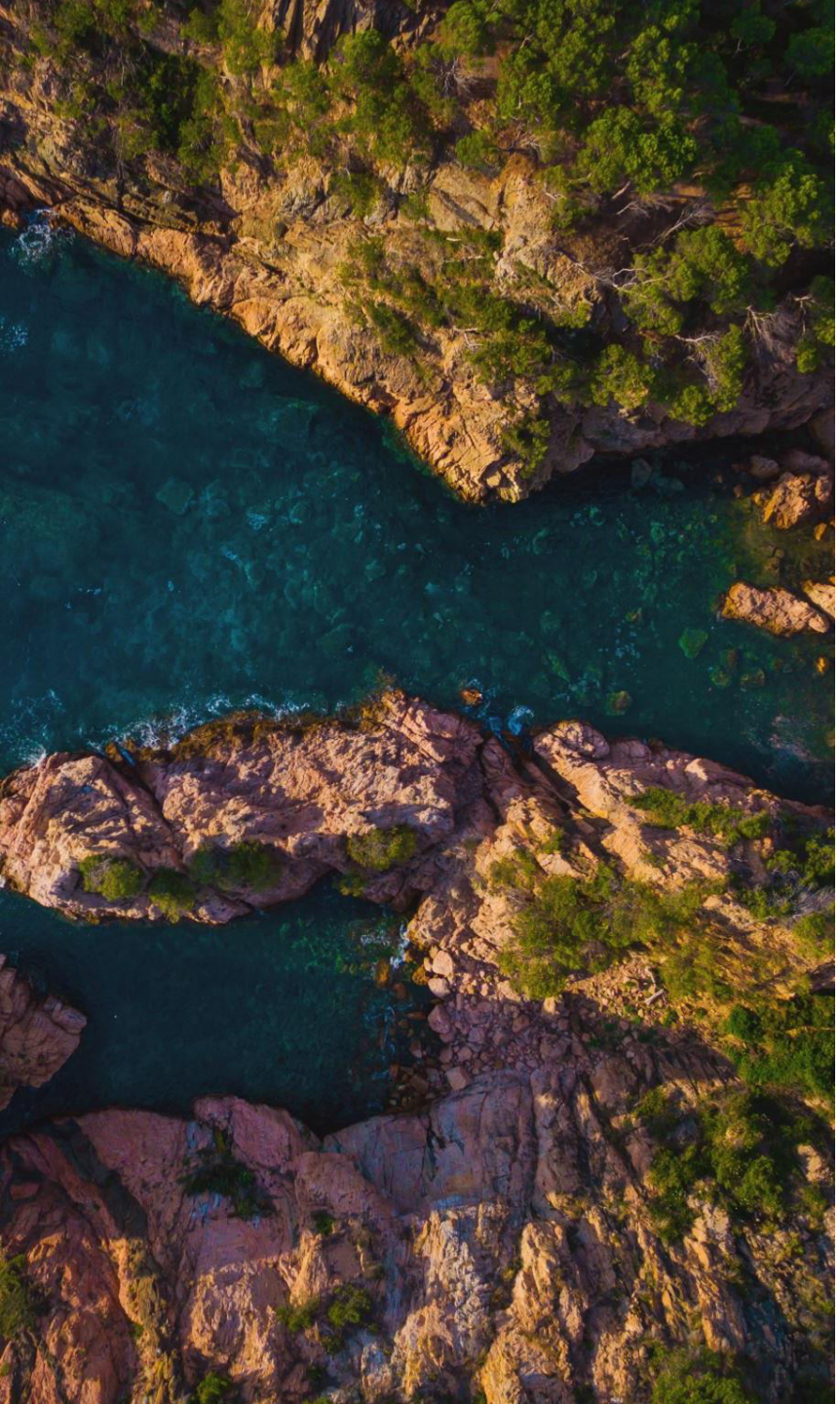
Seguridad en Informática - Módulo 5

Docente: Carlos Cagnani

*Este documento fue realizado en concepto de capacitación en Formación Profesional y dictada para el **Sindicato CePETel** a contar del mes de mayo del año 2023.*

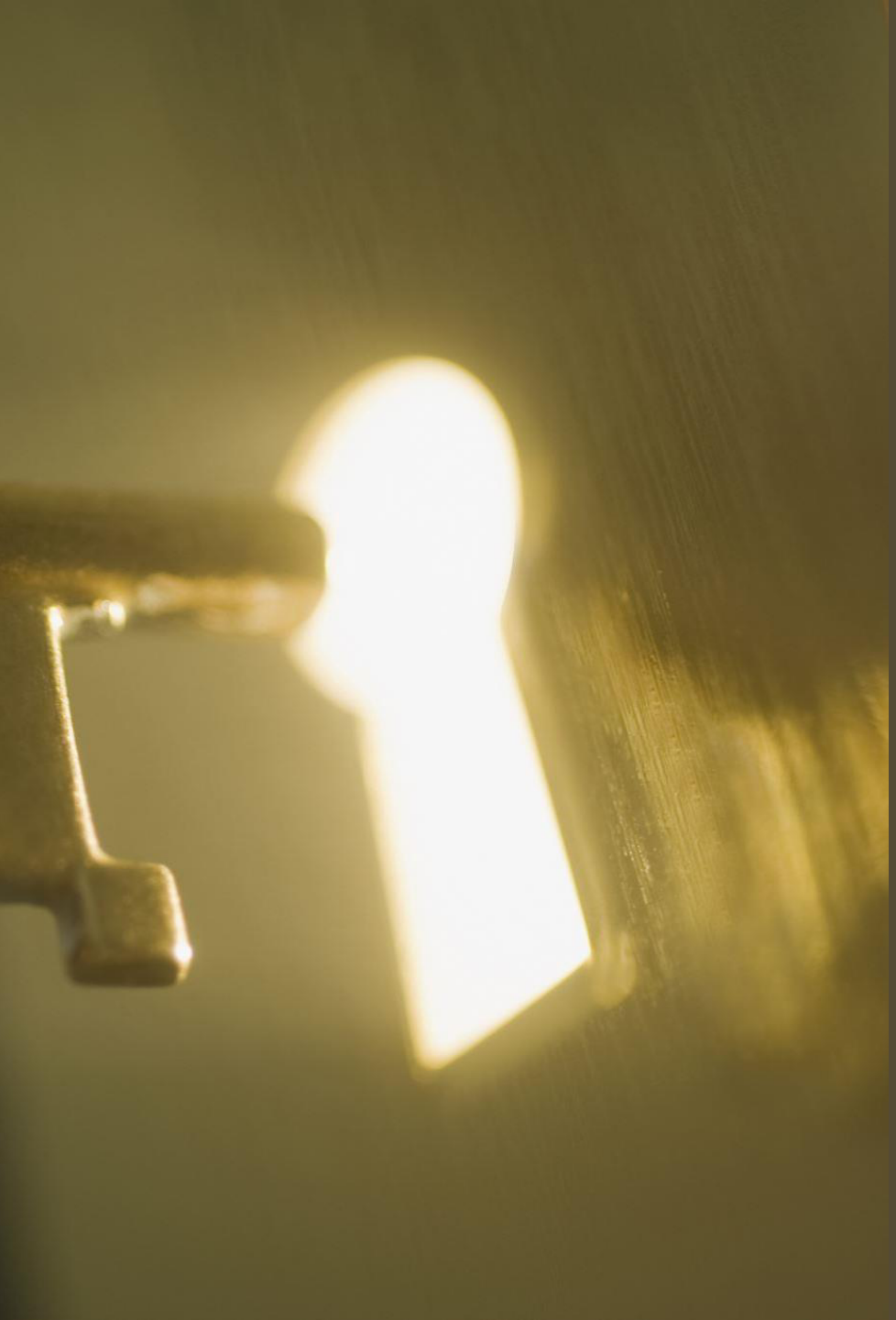
Redes Informáticas

CLASE 5 Seguridad en Redes

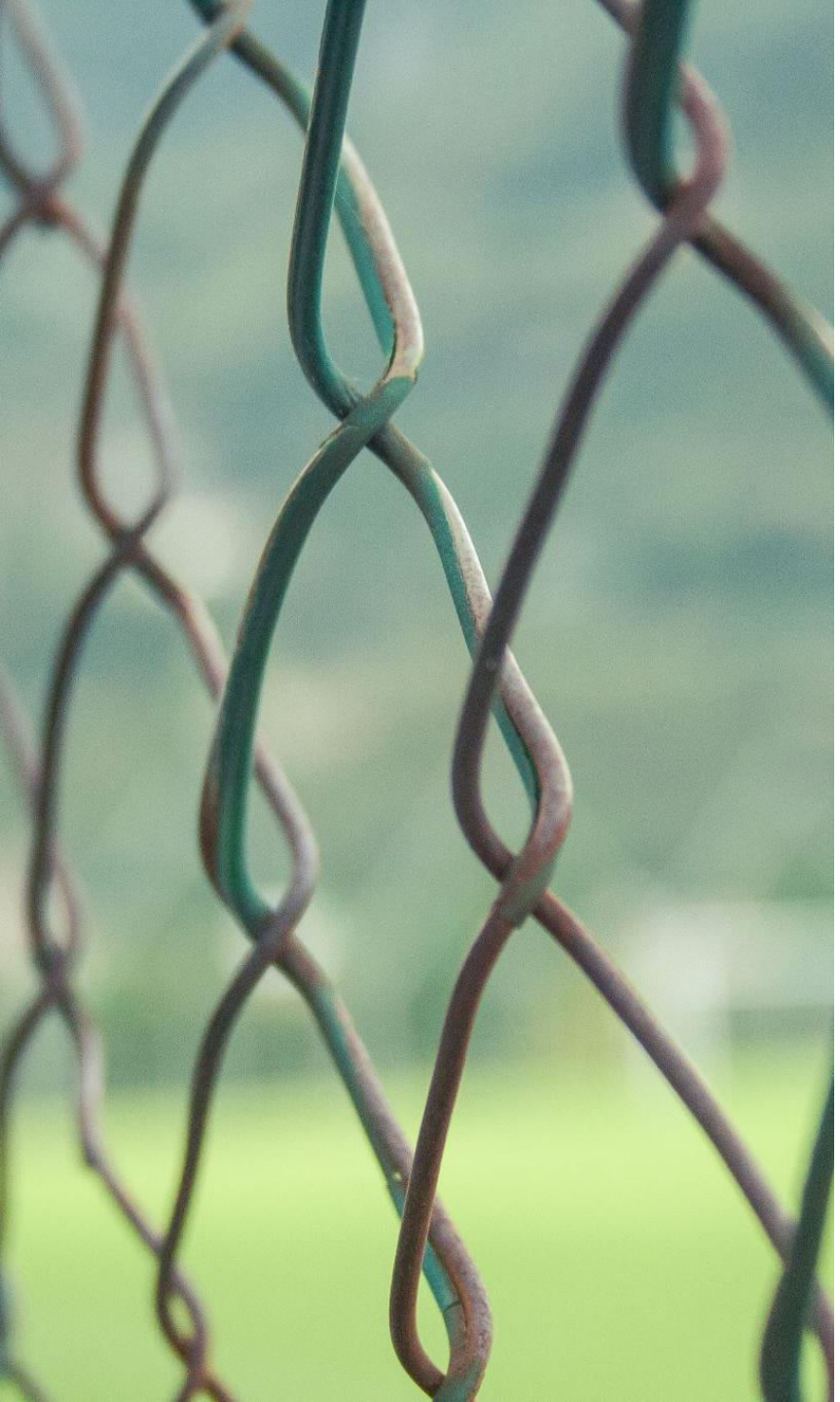


Índice de temas

- Seguridad Perimetral
- Zero Trust
- SASE
- Firewalls
- IPS
- IDS
- WAF
- NGFW
- Cisco Umbrella
- Fortinet
- F5
- McAfee
- ARBOR
- Juniper
- Sophos



Seguridad Perimetral

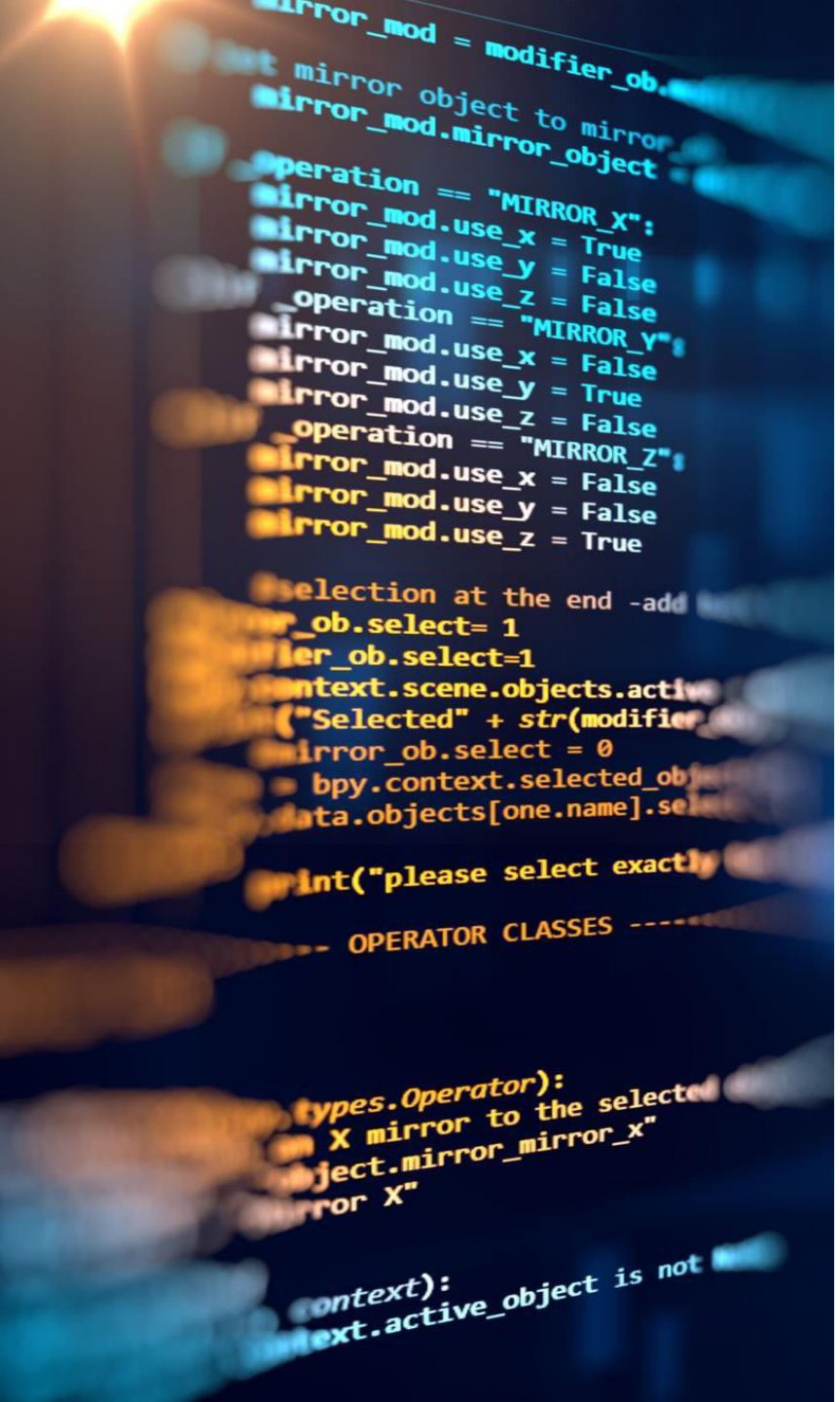


Seguridad perimetral

- El concepto de **seguridad perimetral o perímetro de seguridad** es uno de los más relevantes dentro del campo de la seguridad de la información.
- Y es que, la unión de la red local y confiable de una organización con otras redes externas, como puede ser Internet, donde existen numerosos agentes de amenaza que pueden comprometer la infraestructura, presenta un riesgo elevado.
- Por ello, es importante que las compañías apliquen controles de seguridad específicos que garanticen el control de acceso sobre la información sensible de la organización.

Seguridad Perimetral
idea o concepto

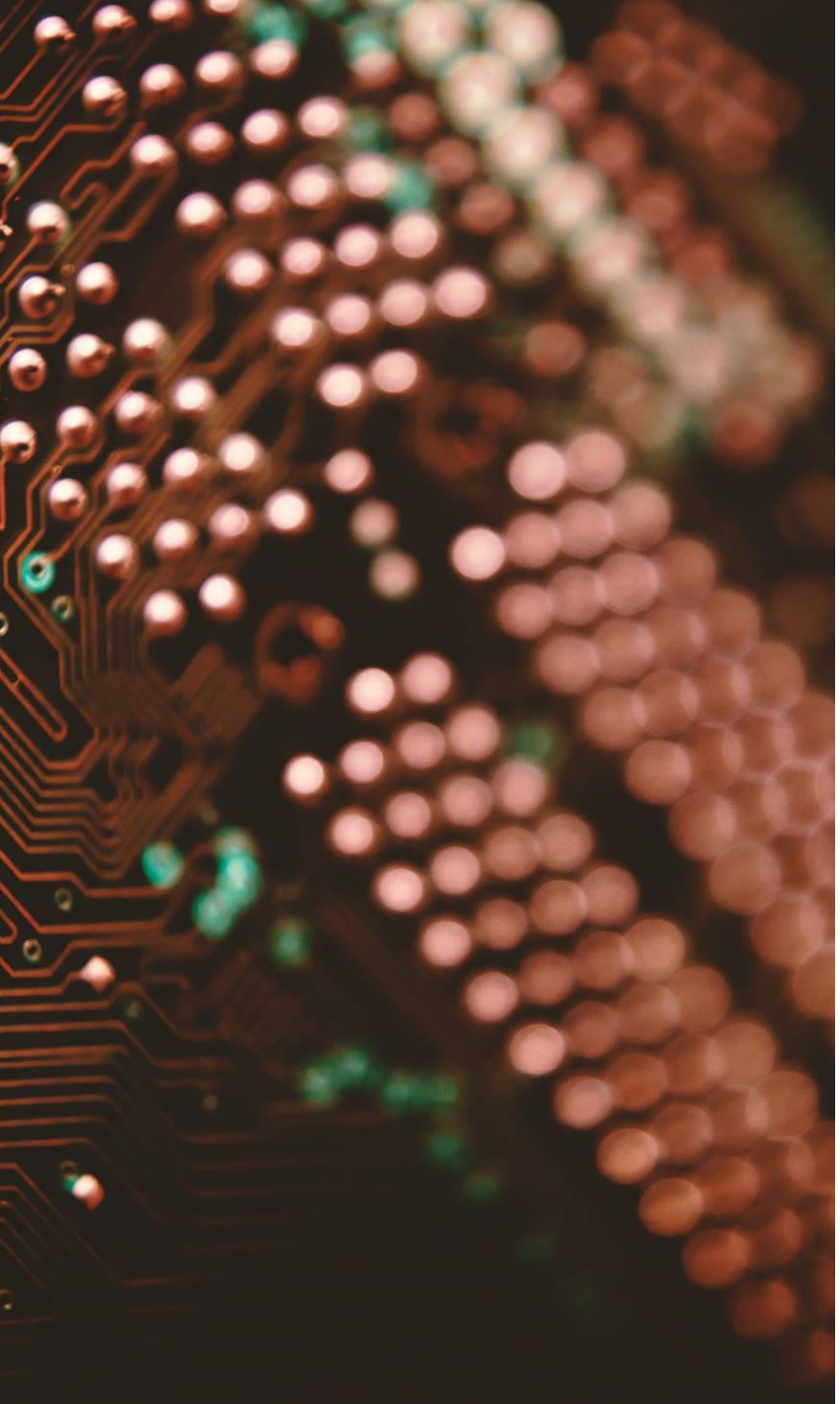
- El modelo perimetral es un modelo de seguridad de red en el que nadie de fuera de la red puede acceder a los datos de dentro, pero sí que pueden todos los que están dentro.
- Imaginemos que la red de una organización es un castillo, y el perímetro de red un foso.
- Una vez que se baja el puente levadizo y alguien lo cruza, puede moverse con libertad por el interior del castillo.
- Del mismo modo, una vez que un usuario se conecta a una red en este modelo, puede acceder a todas las aplicaciones y datos de esa red.



Seguridad Perimetral

En que consiste

- Podemos establecer una **definición de seguridad perimetral informática** como aquel conjunto de controles de seguridad que se establecen alrededor de una infraestructura tecnológica.
- De ahí que la palabra “perímetro” juegue un papel importante en este concepto.
- La necesidad de paliar riesgos de ciberseguridad con controles perimetrales surge cuando los ordenadores comienzan a intercambiar información con otros ordenadores.
- Esto implicaba que controlar la información que entraba y salía de los ordenadores fuera cada vez más complejo.



Seguridad Perimetral

En que consiste cont.

- Hoy en día, debido a la evolución tecnológica, los ordenadores están al alcance de cualquier persona.
- Además, estos ya no se conectan solo con otros ordenadores por una red local, sino también a través de redes de Internet. Y, por otro lado, están conectados con Smartphones, Smart tvs o tablets.
- Por ello, el perímetro de seguridad de estos sistemas puede interpretarse de manera diferente en función del contexto.
- Si bien, por lo general, el perímetro de una organización se establece en el punto en el que la infraestructura tecnológica de la compañía (redes, ordenadores, teléfonos…) se interconecta con Internet.
- De esta forma, **la seguridad perimetral consiste en establecer controles de seguridad con el fin de garantizar que la información y los sistemas que se encuentran dentro de la infraestructura tecnológica de la organización no sufran ataques** ni accesos procedentes de redes no confiables, como puede ser Internet, que estén fuera de su perímetro.
- Gracias a ello se controla, por ejemplo, el acceso a los recursos corporativos, la confidencialidad y la integridad de la información que se intercambia o la disponibilidad de los sistemas. Se trata por tanto de un factor clave de la Ciberseguridad en las compañías.

Seguridad Perimetral

Sistemas

Existen distintos **tipos de sistemas de seguridad perimetral**. Si bien, los más comunes en la actualidad son los siguientes:

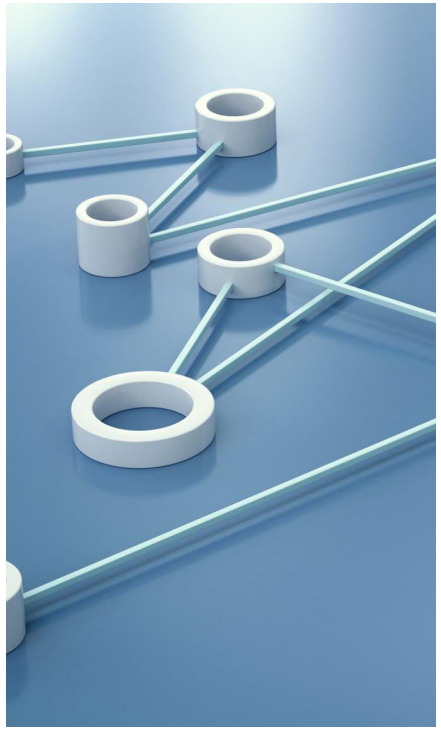
- **Sistemas de cortafuegos**: Son los llamados firewall, que filtran el tráfico que se intercambia entre una red confiable y otras redes no confiables. Todo ello, en función de unas reglas establecidas previamente.
- **Zonas desmilitarizadas (DZM):** Se trata de uno de los conceptos más usados para añadir seguridad al perímetro cuando se establece una arquitectura de red para una organización de cualquier dimensión. Es una red que se sitúa entre la red interna (confiable) de la organización y las redes externas (no confiables).
- **Sistemas de prevención y detección de intrusiones**: Son algo más complejos. Pretenden una identificar una posible actividad maliciosa con el fin de detener una posible intrusión (IPS / IDS).

Seguridad Perimetral
Problemas

- En la actualidad, el enfoque perimetral se está quedando **obsoleto**.
- En la mayoría de las empresas, los datos están repartidos entre varios proveedores de la nube, en lugar de permanecer detrás de un perímetro de red local.
- En el ejemplo del castillo. No tiene sentido poner todos los recursos defendiendo el castillo, si la reina y su corte están fuera del mismo.
- En la actualidad, hay algunas organizaciones que siguen manteniendo sus datos en las redes locales, y otras enrutan todo el tráfico con destino a Internet a través de la red corporativa central para controlar el acceso a los proveedores de la nube.
- Pero este uso del modelo perimetral sigue teniendo fallos de seguridad inherentes.
- El mayor fallo de seguridad es que si un atacante consigue acceder a la red (es decir, si cruza el "foso"), también puede acceder a los datos y sistemas que haya dentro.
- Pueden penetrar en la red al robar las credenciales de usuario, aprovechar una vulnerabilidad de seguridad, introducir una infección de malware, o llevar a cabo un ataque de ingeniería social, entre otros métodos.
- Los firewalls y otras herramientas de prevención de intrusiones pueden detener algunos de estos ataques, pero si uno de ellos consigue pasar, el coste es muy alto.

Seguridad Perimetral

Como se implementa



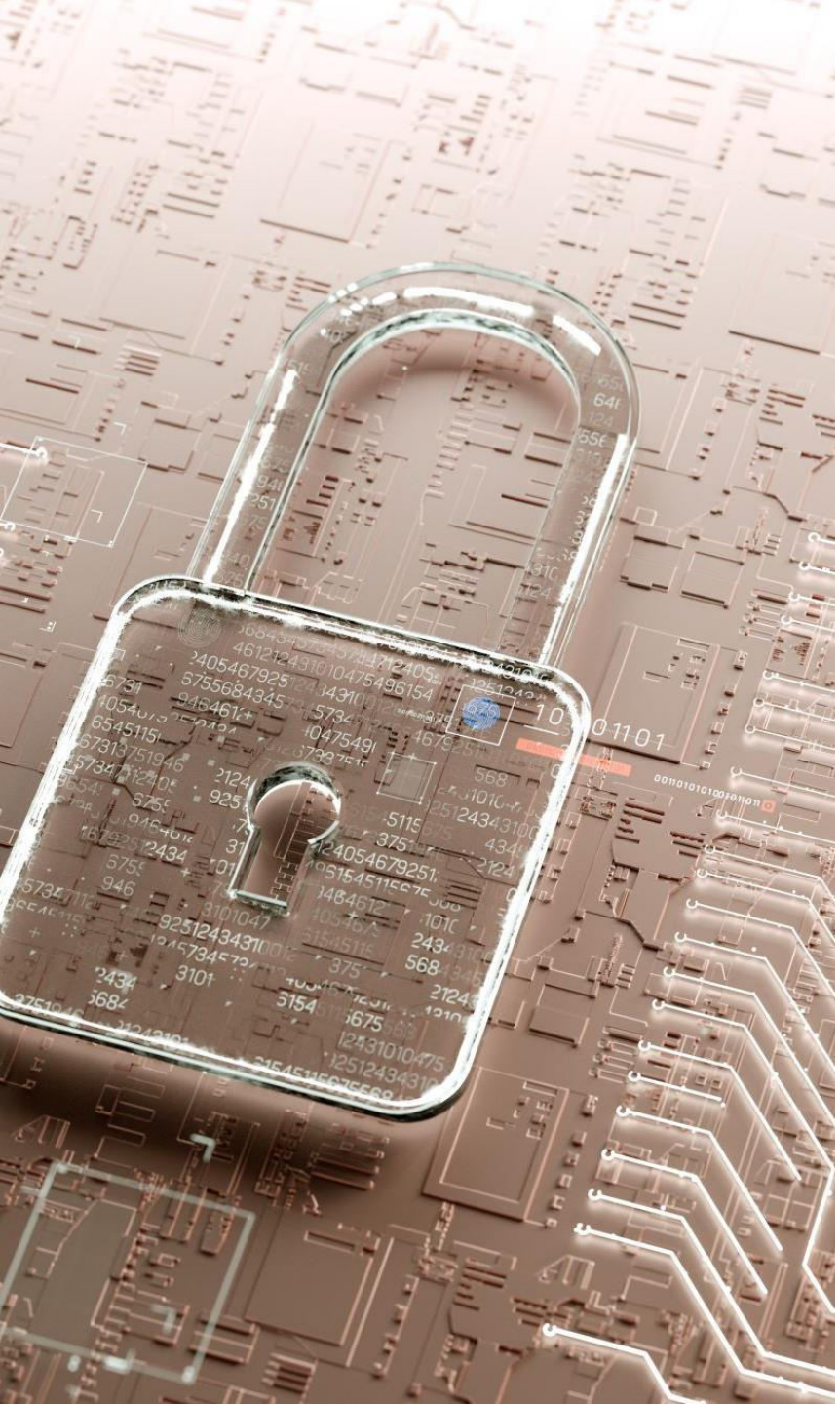
Una de las formas en que las organizaciones controlan el acceso cuando utilizan el modelo perimetral son las redes privadas virtuales, o VPN. Las VPN establecen una conexión encriptada entre los usuarios conectados (que suelen trabajar en remoto) y un servidor VPN. Para determinados niveles de acceso, un usuario debe conectarse al menos a una VPN. Una vez conectado, puede acceder a los recursos que necesite.

Ya que los diferentes usuarios de una misma empresa suelen requerir diferentes privilegios de acceso, los equipos de TI configuran varias VPN. Cada VPN puede considerarse como su propio "castillo", lo que proporciona un nivel de acceso diferente.

Este enfoque tiene algunos inconvenientes:

- **Vulnerabilidad a los ataques:** una VPN actúa como un único punto de fallo para las aplicaciones y los datos que protege. Solo hace falta una cuenta o un dispositivo en riesgo para que un atacante cruce el perímetro y acceda a los datos protegidos por la VPN.
- **Rendimiento más lento:** las VPN encriptan todo el tráfico, lo que puede añadir una ligera latencia a la red, en función del tipo de encriptación utilizado (comparar IPsec vs. SSL). Para los empleados en remoto, una VPN enruta todo el tráfico a través del servidor VPN, que podría estar lejos del empleado, ralentizando todavía más el tráfico de la red.
- **Escalabilidad:** si el uso de la VPN excede la capacidad del servidor VPN para gestionar el tráfico, se tiene que actualizar el servidor, un proceso que requiere mucho trabajo.
- **Mantenimiento:** las VPN requieren mucho tiempo y recursos para su mantenimiento. Los equipos de TI deben instalar el cliente VPN adecuado en el ordenador de cada empleado en remoto, asegurarse de que los empleados mantienen ese software actualizado, y actualizar o sustituir el hardware de la VPN con regularidad.

ZERO TRUST

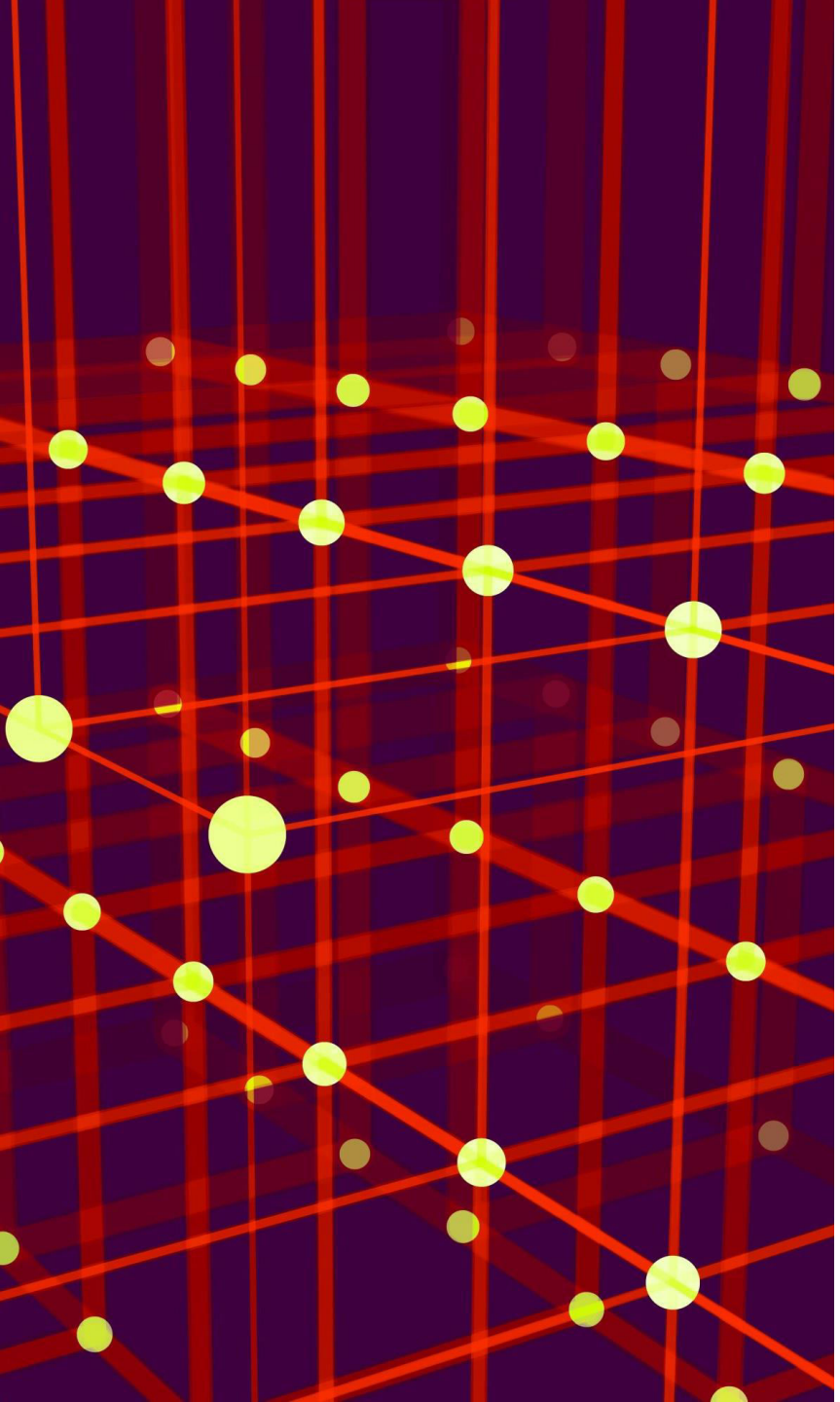


Zero Trust

- La seguridad de confianza cero es un modelo de seguridad informática que requiere una estricta verificación de identidad para cada persona y dispositivo que intenta acceder a recursos en una red privada, independientemente de si se encuentran dentro o fuera del perímetro de la red.
- ZTNA (acrónimo en inglés de Acceso de Confianza Cero) es la principal tecnología asociada con la arquitectura de confianza cero; pero la confianza cero es un enfoque holístico de seguridad de red que incorpora varios principios y tecnologías diferentes.
- En términos más simples: la seguridad tradicional de red confía en cualquier persona y cualquier cosa dentro de la red. Una arquitectura de confianza cero no confía en nadie ni en nada.
- La seguridad tradicional de red se basa en el concepto de castillo y foso.
- En la seguridad de castillo y foso, es difícil obtener acceso desde fuera de la red, pero se confía en todos los que están dentro de la red por defecto.
- El problema con este enfoque es que una vez que un atacante obtiene acceso a la red, tienen pleno control sobre todo lo que hay dentro.

Zero Trust

- Esta vulnerabilidad en los sistemas de seguridad de castillo y foso se ve agravada por el hecho de que las empresas ya no tienen sus datos en un solo lugar.
- Hoy en día, la información se encuentra a menudo dispersa en diferentes proveedores de servicios en la nube, lo que dificulta tener un control de seguridad único para toda la red.
- La seguridad **Zero Trust** significa que nadie es confiable por defecto, ya sea desde dentro o fuera de la red, y se requiere verificación de todos aquellos que intenten acceder a los recursos de la red.
- Esta capa adicional de seguridad ha demostrado prevenir las violaciones de datos.
- Estudios han demostrado que el costo promedio de una sola violación de datos supera los $3 millones de dólares.
- Teniendo en cuenta esta cifra, no es sorprendente que muchas organizaciones estén ansiosas por adoptar una política de seguridad de confianza cero.



Zero Trust

Principios

1. Monitoreo y validación continua: La filosofía detrás de una red de confianza cero asume que existen atacantes tanto dentro como fuera de la red, por lo que ningún usuario o dispositivo debe ser automáticamente confiable.

La seguridad Zero Trust verifica la identidad y los privilegios de los usuarios, así como la identidad y seguridad de los dispositivos. Las sesiones de inicio y las conexiones expiran periódicamente una vez establecidas, lo que obliga a los usuarios y dispositivos a ser verificados de manera continua.

2. Verificación estricta de identidad: La seguridad de confianza cero enfatiza la necesidad de una sólida verificación de identidad de los usuarios y dispositivos. Esto implica la autenticación multifactor (AMF), donde los usuarios deben proporcionar múltiples pruebas para demostrar su identidad, como contraseñas, biometría o tokens de seguridad.

3. Acceso con privilegios mínimos: La seguridad de confianza cero sigue el principio de otorgar el menor nivel de privilegios necesario para que un usuario o dispositivo realice sus tareas autorizadas. Los derechos de acceso se basan en un nivel granular, permitiendo solo los recursos y datos específicos requeridos para el rol o función del usuario.

4. Microsegmentación: La seguridad de confianza cero promueve la segmentación de la red en segmentos más pequeños y aislados para contener posibles amenazas. Al dividir la red en zonas y aplicar controles de acceso estrictos entre ellas, se puede limitar el movimiento lateral de los atacantes, reduciendo la superficie de ataque general.

Zero Trust

Principios cont.

5. Monitoreo y análisis continuos: Las redes de confianza cero emplean el monitoreo y análisis continuos del comportamiento de usuarios y dispositivos. Al recopilar y analizar datos de diversas fuentes, como registros, tráfico de red y patrones de comportamiento de los usuarios, se pueden detectar de manera rápida cualquier anomalía o actividad sospechosa, permitiendo una respuesta y mitigación oportuna.

6. Automatización y orquestación de la seguridad: La seguridad de confianza cero enfatiza el uso de herramientas y procesos de seguridad automatizados para aplicar políticas de seguridad consistentes, detectar y responder rápidamente a las amenazas, y agilizar las operaciones de seguridad. La automatización ayuda a reducir los errores humanos y mejora la eficiencia y efectividad de las medidas de seguridad.

Estos principios conforman colectivamente la base de un enfoque de confianza cero, con el objetivo de mejorar la seguridad de la red al minimizar la confianza depositada en los usuarios y dispositivos, y validar continuamente sus privilegios de acceso.

SASE

SECURE ACCESS SERVICE EDGE

SASE

El nuevo panorama requiere una solución moderna que ofrezca conectividad sin problemas desde cualquier lugar y al mismo tiempo brinde seguridad en todas partes.

Secure Access Service Edge, o SASE, es una poderosa solución de TI que puede ayudar a tu organización a proteger mejor sus datos y tecnologías que usan tus empleados, ya sea que estén en el sitio o de forma remota.

SASE (perímetro de servicio de acceso seguro)

SASE (Secure Access Service Edge) es una arquitectura de red que unifica las soluciones de red y seguridad en un servicio basado en la nube para mejorar la accesibilidad, la eficiencia y la ciberseguridad.

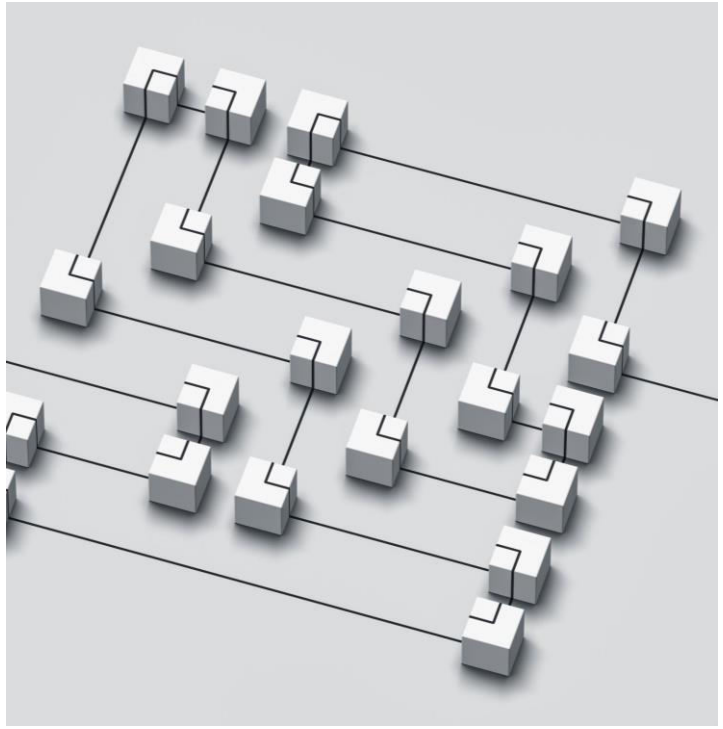
SASE

En pocas palabras, SASE combina capacidades de

SD-WAN con **seguridad** y las ofrece como un servicio. Las políticas de seguridad aplicadas en las sesiones de los usuarios se adaptan a cada una de ellas en función de cuatro factores:

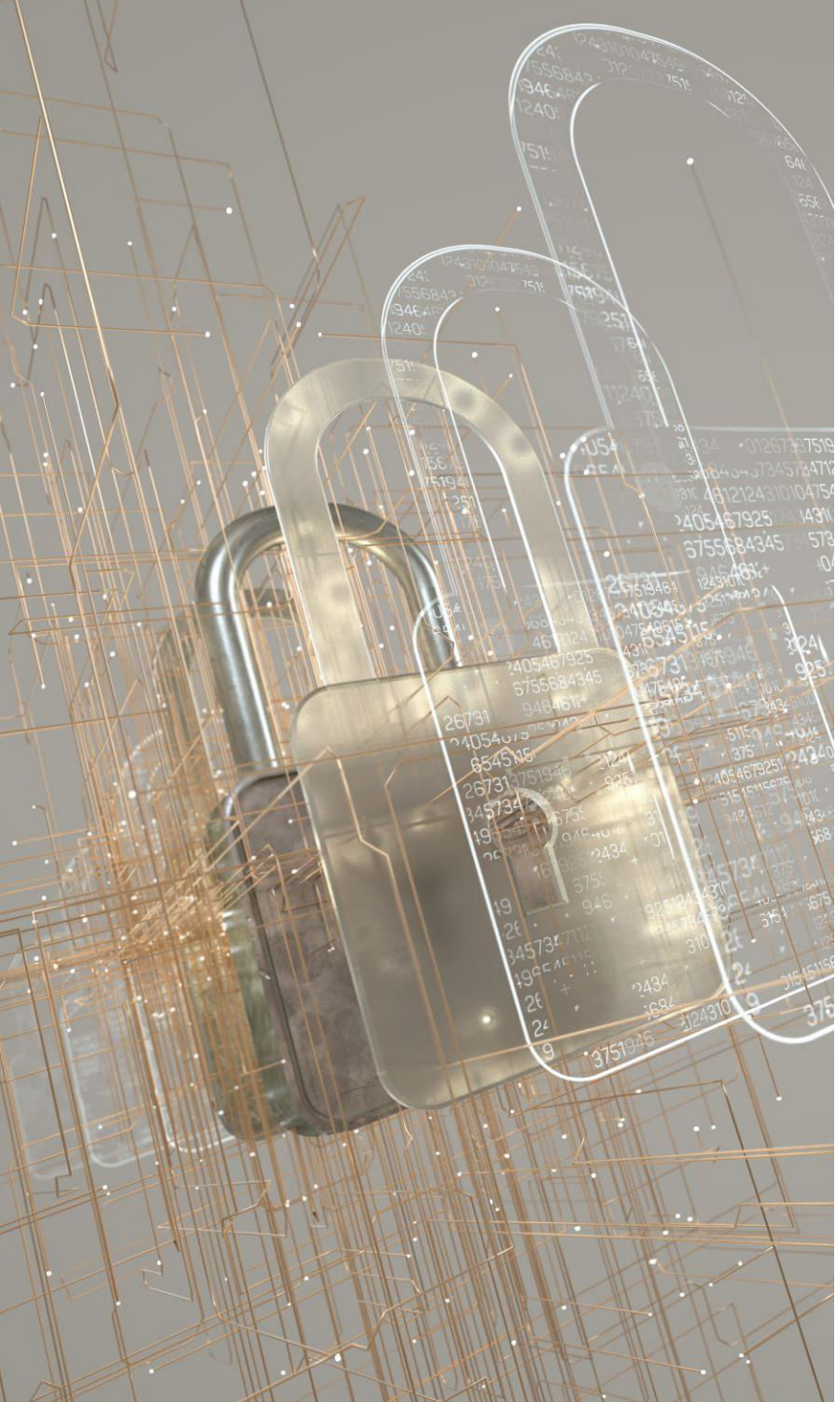
- Identidad de la entidad que conecta.
- Contexto (salud y comportamiento del dispositivo, sensibilidad de los recursos a los que se accede).
- Políticas de seguridad y cumplimiento.
- Evaluación continua del riesgo durante cada sesión.

SASE



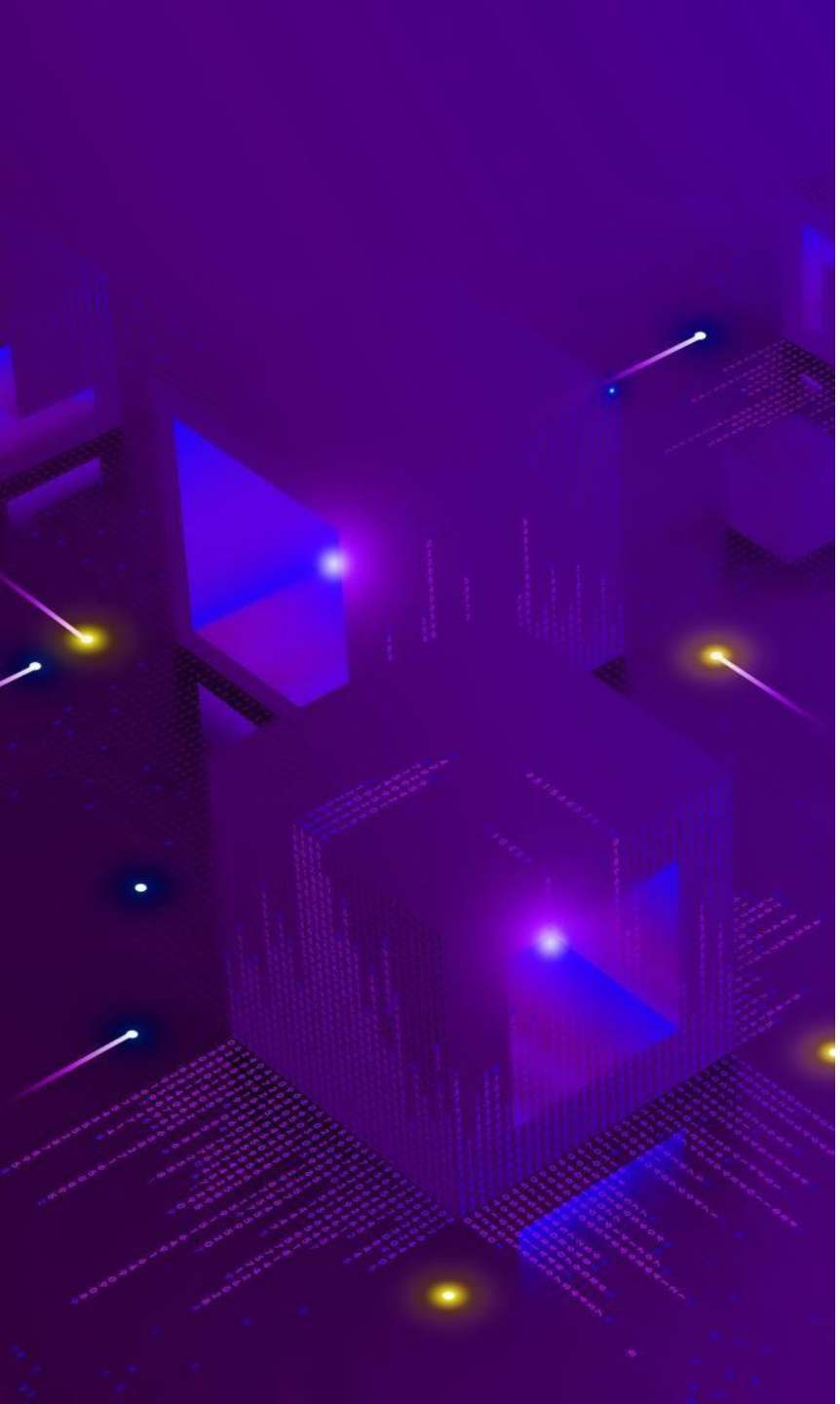
El lado WAN de SASE se basa en las capacidades por entidades que incluyen proveedores de **SD-WAN**, operadores, redes de entrega de contenido, proveedores de red como servicio, agregadores de ancho de banda y proveedores de equipos de red.

El lado de la seguridad se basa en agentes de seguridad de acceso a la nube, puertas de enlace web seguras en la nube, acceso a la red de confianza cero, firewall como servicio, protección de API web como servicio, DNS y aislamiento de navegador remoto.



SASE Componentes

- SASE combina la protección de Security Service Edge (el conjunto de capacidades necesarias para lograr las características de seguridad de SASE) con múltiples tecnologías de red y seguridad en una única solución.
- Cada componente contribuye a construir una red segura y confiable sin sacrificar la calidad o la velocidad.



SASE Agente de seguridad de acceso a la nube (CASB)

CASB (**C**loud **A**ccess **S**ecurity **B**roker) funciona como puente entre los usuarios/dispositivos y las aplicaciones en la nube.

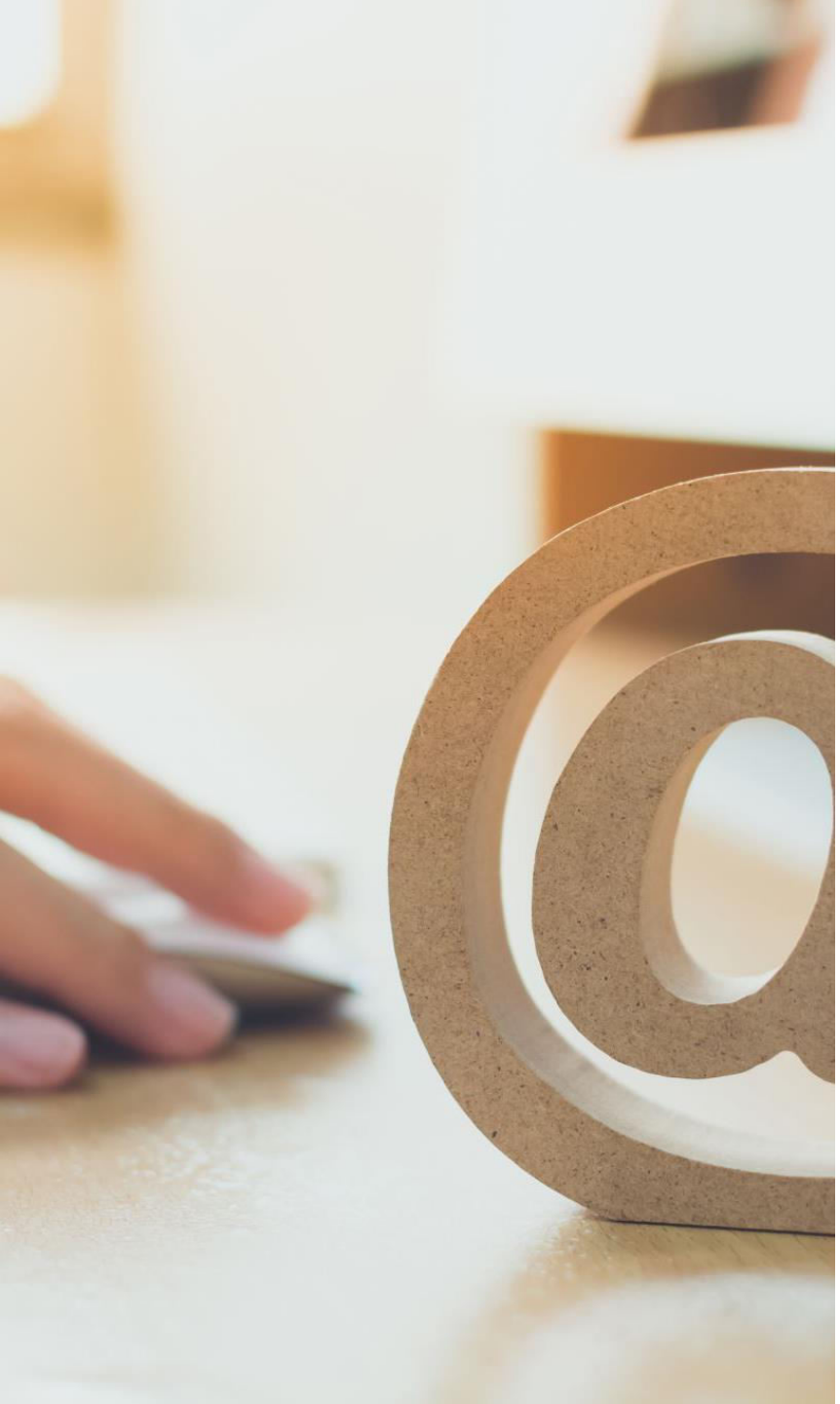
Si sus aplicaciones fueran un club nocturno, los CASB serían los gorilas o patovicas de la puerta.

Son una forma clave de seguridad. Permite a la organización aplicar políticas de seguridad, autenticación de dos factores e inicio de sesión único en todas las aplicaciones en la nube que se supone que las personas deben usar, manteniendo los dispositivos no autorizados y las personas fuera de los activos críticos sin restringir el acceso a quienes lo necesitan.

SASE Firewall como servicio (FWaaS)

El firewall como servicio (FWaaS) puede funcionar en las instalaciones, pero a menudo se aprovecha a través de la nube en una configuración SASE.

FWaaS ofrece las mismas soluciones que un firewall con estado: monitorización de red, filtrado de paquetes y mapeo de IP, con capacidades adicionales de firewall de última generación (NGFW).



SASE Acceso a la red de confianza cero (ZTNA)

ZTNA significa acceso a la red de confianza cero.

- Requiere que los usuarios/dispositivos proporcionen un permiso explícito para acceder a las aplicaciones.
- Es como si el usuario estuviera físicamente en la oficina y necesitara escanear su tarjeta para acceder a áreas restringidas; tendrían que escanear la placa cada vez que quisieran entrar.
- Este es un componente de seguridad muy importante porque permite ocultar las aplicaciones privadas internas a los usuarios que no deberían tener acceso, pero que son visibles y funcionales para quienes sí lo tienen.
- También permite un mayor acceso remoto mediante la autenticación por capas. ZTNA brinda seguridad ágil que es increíblemente adaptable y capaz de manejar las necesidades de seguridad modernas.

SASE Puerta de enlace web segura (SWG)

SWG significa Secure Web Gateway, y funciona como un tamiz en la red para filtrar lo que no debería estar allí.

- También permite a las organizaciones hacer cumplir sus políticas de usuarios aceptables, manteniendo alejados a los atacantes y conservando los datos confidenciales.
- SWG incluye otras funciones que garantizan una funcionalidad más segura sin sacrificar la experiencia del usuario.
- Por ejemplo, el Aislamiento de navegador remoto (RBI) aísla a los usuarios de los sitios web que pueden haberse visto comprometidos.
- Y Content Disarm and Reconstruction (CDR) asegura automáticamente los archivos descargados, lo que permite a los usuarios usar contenido de la web de manera segura, incluso si se ha visto comprometido.
- Además, SWG inspecciona el tráfico encriptado y se asegura de que los usuarios solo ingresen a áreas a las que tienen autorización de acceso y que se consideran seguras.
- Debido a que está integrado en toda la plataforma SASE, permite esta función a escala de la nube.

SASE SD-WAN

SD-WAN significa red de área amplia definida por software.

- Proporciona una conexión segura y directa a Internet, generalmente para sucursales y sitios remotos.
- Al combinar esto con las técnicas de seguridad de SSE, SD-WAN permite a los usuarios conectarse a todas las aplicaciones y datos que necesitan para ser productivos.
- SD-WAN también elimina el trabajo pesado de las redes.
- Por lo tanto, tu organización no necesitará redes dedicadas, como las antiguas líneas MPLS basadas en telecomunicaciones, ya que utiliza un enfoque de red completamente basado en la nube.
- Esto permite una red rápida y de calidad porque se ha eliminado la necesidad de enviar todo el tráfico de vuelta a través de un cuello de botella central.
- En su lugar, ofrece capacidades de exploración de tráfico profundas para detectar tráfico sospechoso o patrones de comportamiento inusuales.

FIREWALL

¿Qué es un firewall?

- Un firewall es un dispositivo de seguridad de la red que monitorea el tráfico de red -entrante y saliente- y decide si permite o bloquea tráfico específico en función de un conjunto definido de reglas de seguridad.
- Los firewalls han constituido una primera línea de defensa en seguridad de la red durante más de 25 años.
- Establecen una barrera entre las redes internas protegidas y controladas en las que se puede confiar y redes externas que no son de confianza, como Internet.
- Un firewall puede ser hardware, software o ambos.

¿Qué es un firewall de una red informática de empresa?

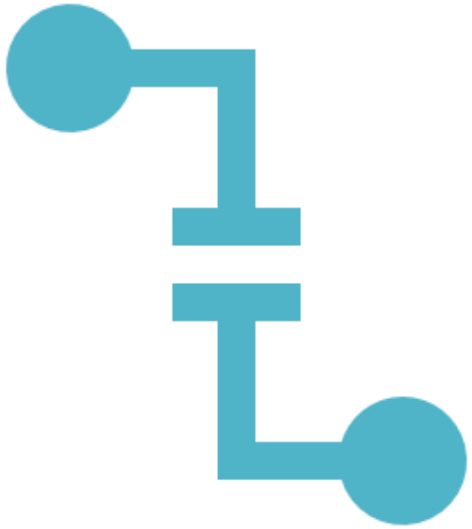
- Si nos fijamos en su significado desde el punto de vista de las redes informáticas, un firewall es un equipo de seguridad que separa la red privada de una empresa, de la red pública (Internet).
- En la actualidad, los firewalls son equipos importantísimos debido a la gran cantidad de ataques que reciben todas las empresas.

¿Qué tipos de firewalls existen?

Los firewalls de red se pueden diferenciar dependiendo de varios criterios:

- Firewall físico o virtual
- Firewall nivel de red: Capa 3, Capa 7.
- Firewall por funcionalidad: UTM, NGFW
- Otras: Firewall Aplicación, Web, PC, Windows…

¿Firewall físico vs virtual?



Si nuestro firewall es físico, tendremos un equipo o hardware dedicado a esta función.

En cambio si nuestro cortafuegos es virtual, lo tendremos integrado dentro de nuestra infraestructura virtual.

Dependiendo de la función que queramos y de las características o infraestructura de nuestra red, nos interesará utilizar un cortafuegos físico o virtual.

¿Qué es un firewall físico?

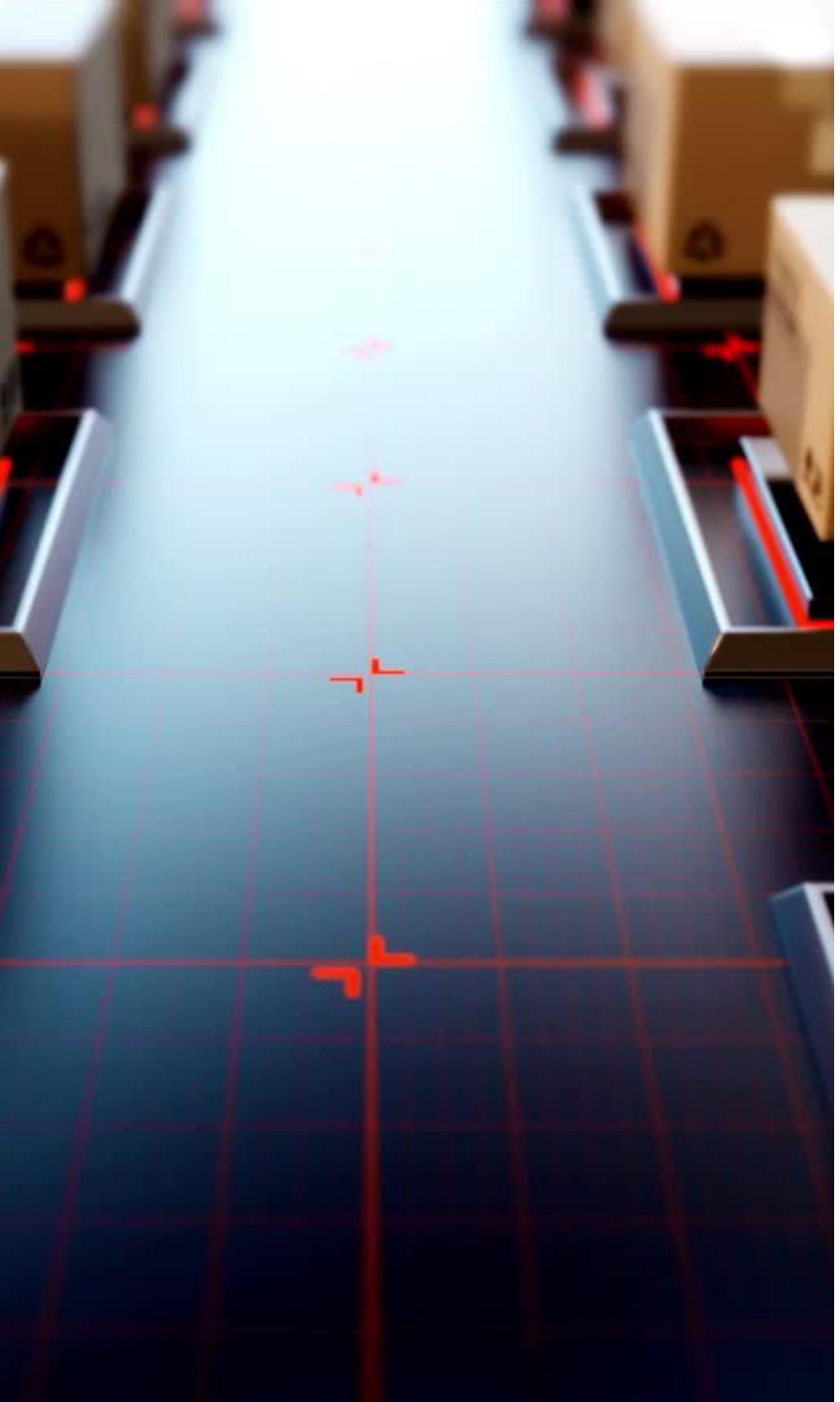
Un firewall físico, consiste en un equipo dedicado exclusivamente a las funciones de firewall.

Es un hardware más en nuestra infraestructura de red.

Normalmente se utilizan para firewalls de red que separan la red privada de Internet.

Los firewalls físicos pueden ser pequeños como un router, para empresas pequeñas y medianas.

Los operadores o grandes empresas tienen firewall muy grandes y pueden ser particionados para distintas áreas o servicios.



¿Qué es un firewall virtual?

Un firewall virtual es una máquina virtual que realiza las funciones de firewall a través de un software específico.

Muchos fabricantes, han desarrollado máquinas virtuales o softwares para poder integrar la función de firewall dentro de nuestro entorno virtual.

Así aprovechar la infraestructura de red, procesamiento y almacenaje que ya disponen para agregar una funcionalidad más.

Casi todos los proveedores o fabricantes de equipos como Cisco, Fortinet, Palo Alto o Watchguard, disponen de licencias para integrar un firewall virtual.

Firewall Capa 3 o 4

Un firewall de capa 3 o 4, es aquel que solo realiza funciones de las capa 3 o 4 de la separación del modelo OSI.

Las principales funciones de un cortafuegos de capa 3, son básicamente a nivel de Routing, ACLs o a nivel IP.

Solo podrá tomar decisiones a base de la información que obtenga de la capa 3.

Algunas de las funciones son:

Filtrado de paquetes dependiendo de:

- Origen
- Destino
- Protocolo

Descarte de paquetes malformado

Si el firewall realiza funciones de capa 4, será un firewall con “Stateful Inspection”.

Esto significa que podrá controlar o filtrar dependiendo del estado de las conexiones.

Por ejemplo podría descartar todas las conexiones SYN, REPLY o cualquier tipo de información de estado que contenga las cabeceras de un paquete IP.

Firewall capa 7

Los firewalls de capa 7, realizan funciones a nivel de aplicación.

Esto significa que podrán realizar funciones en los protocolos de red más arriba del modelo OSI.

Con un firewall de capa 7 o de aplicación, podríamos inspeccionar los protocolos HTTP, HTTPS entre otros.

Actualmente estos firewalls son los más utilizados. Nos permiten monitorizar muy bien el tráfico y realizar reglas para permitir o denegar el tráfico dependiendo de muchos factores.

Además de las funciones de un firewall de capa 3 y 4, las principales funciones de un firewall de capa 7 son:

Filtraje a nivel de aplicación

- Filtrar por URL.
- Control de aplicaciones: WEB, FTP, P2P,…
- Proteger frente a ataques de denegación de servicio.
- Proteger de ataques de inyección de código.
- SandBox
- Inspección de tráfico SSL.
- Filtrado por usuario.

Estos tipos de cortafuegos también se llaman **firewalls de aplicación**.

Firewall proxy

- Un firewall proxy, uno de los primeros tipos de dispositivos de firewall, funciona como gateway de una red a otra para una aplicación específica.
- Los servidores proxy pueden brindar funcionalidad adicional, como seguridad y almacenamiento de contenido en caché, evitando las conexiones directas desde el exterior de la red.
- Sin embargo, esto también puede tener un impacto en la capacidad de procesamiento y las aplicaciones que pueden admitir.

Firewall de inspección activa

- Un firewall de inspección activa, ahora considerado un firewall “tradicional”, permite o bloquea el tráfico en función del estado, el puerto y el protocolo.
- Este firewall monitorea toda la actividad, desde la apertura de una conexión hasta su cierre.
- Las decisiones de filtrado se toman de acuerdo con las reglas definidas por el administrador y con el contexto, lo que refiere a usar información de conexiones anteriores y paquetes que pertenecen a la misma conexión.

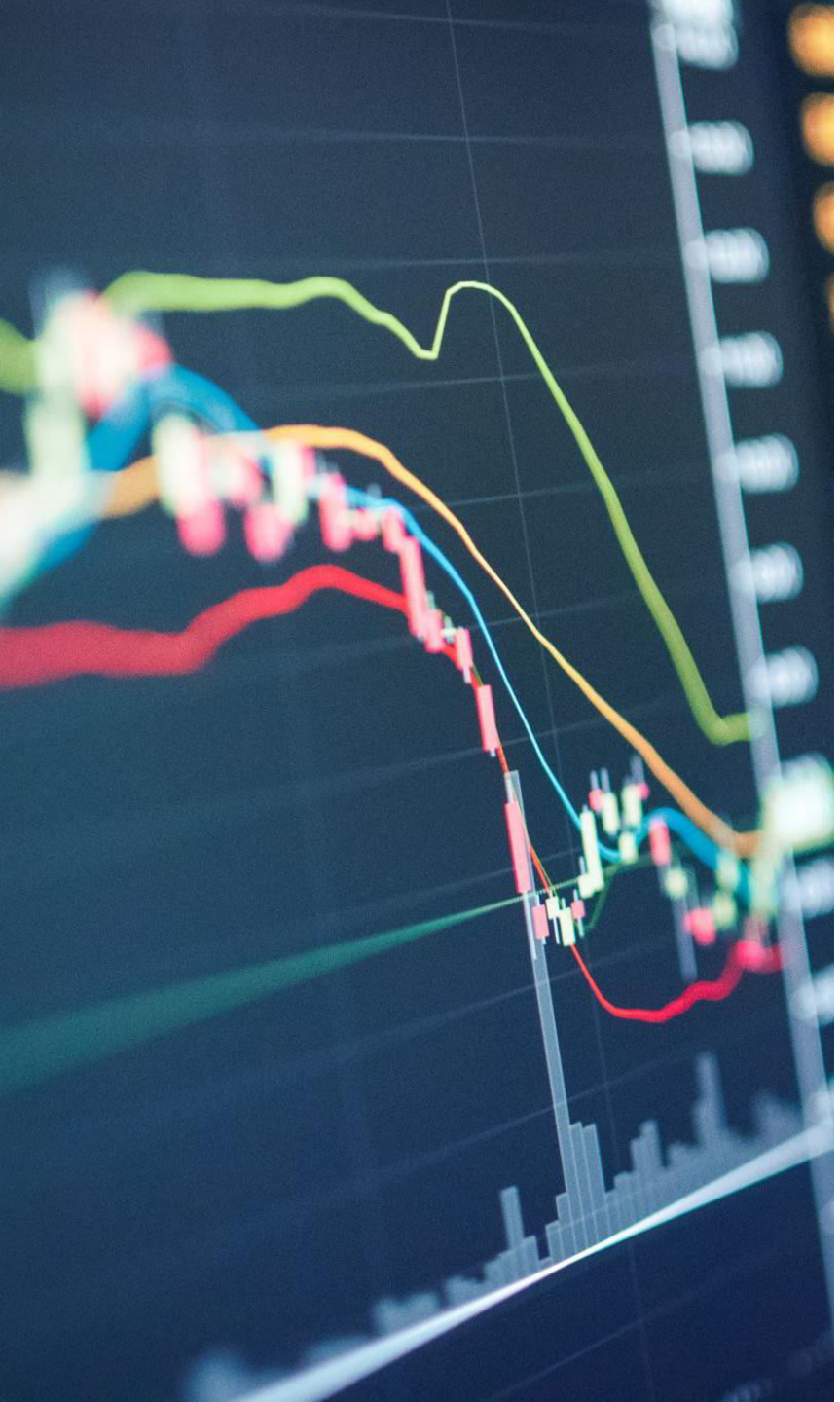
¿Qué són los firewalls UTM (**U**nified **T**hreat **M**anagment) o NGFW (**N**ext **G**eneration **F**irewall)?

Los firewalls UTM o NGFW, son aquellos que desarrollan funciones de inspección, control de paquetes y aplicaciones a nivel de capa 7.

Incluyen otras funciones que no son propias de un cortafuegos o pueden realizar otros equipos más específicos.

¿Que es un equipo UTM (Unified Threat Managment?

- Un equipo UTM o de gestión unificada de amenazas nace alrededor del año 2004, como equipos para la gestión unificada de la seguridad informática de la empresa.
- Además de las funciones de Firewall tradicional, añadieron funciones como VPN, IPS (Intrusion Protection System), Filtrage Web, Control de aplicaciones, Antivirus…
- Así los firewalls UTM, son en realidad sistemas de gestión que controlan todo lo que tenga que ver en seguridad de red.
- De esta forma se centralizan las funciones de protección en un equipo, cuando antes debías tener un software o hardware para cada una de estas funciones.
- Los firewalls que actualmente dispone el mercado casi todo son UTM o NGFW.



¿Qué diferencia hay entre un NGFW (Next Generation Firewall) y UTM(Unified Threat Management)?

Realmente creemos que no existe ninguna diferencia, se trata nada más de un término relacionado con el marketing, ya que después de comparar un UTM con un NGFW no se distingue ninguna diferencia.

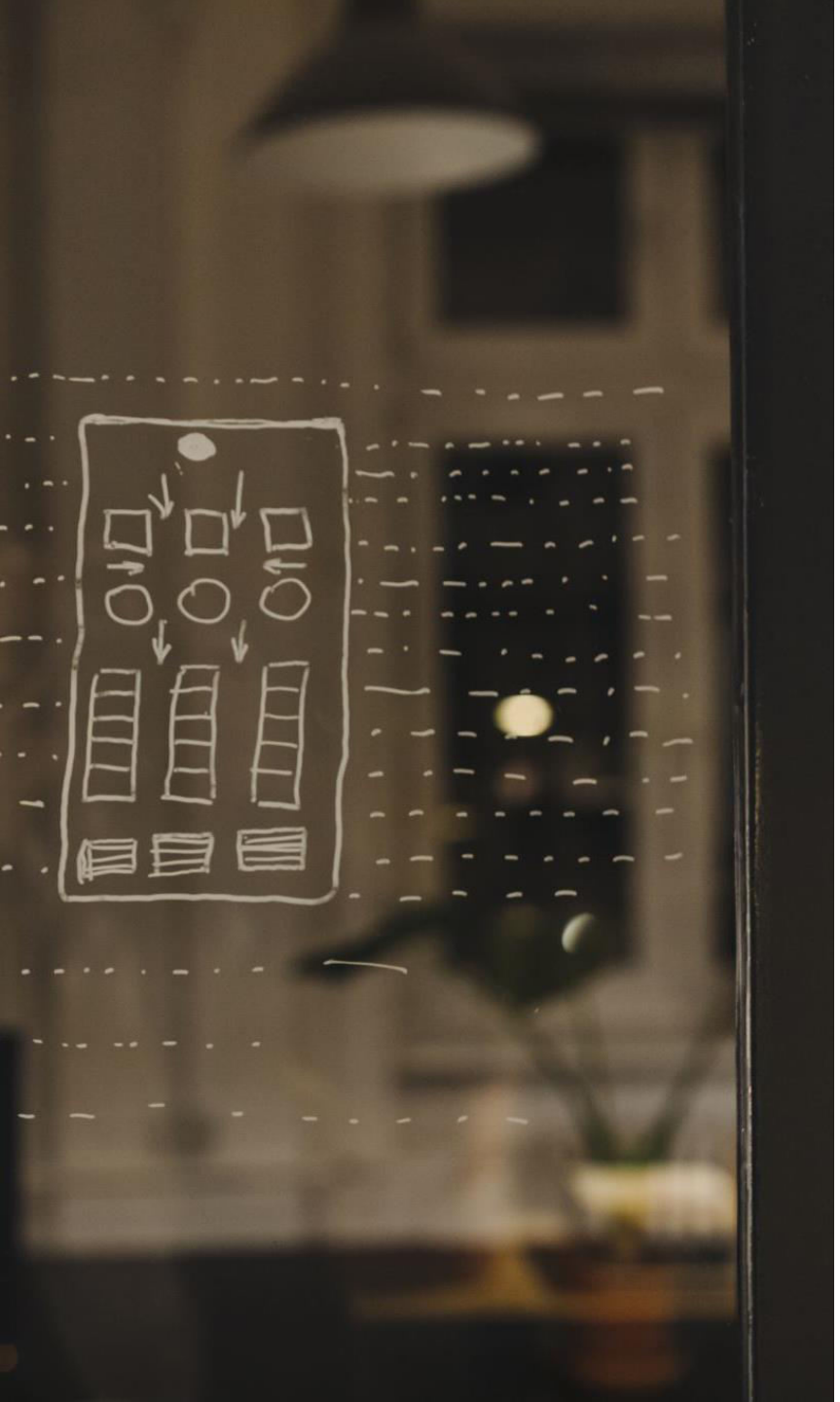
Si nos fijamos en los principales fabricantes de equipos de seguridad unificada, cada uno escoge y presenta sus soluciones, con los términos de UTM o NGFW.

A nivel de funcionalidades vemos que son las mismas.

Otros tipos de firewalls: Firewall de Windows Firewall Web.

El término firewall, también puede aplicarse a los distintos servicios o equipos que intervienen en una red informática.

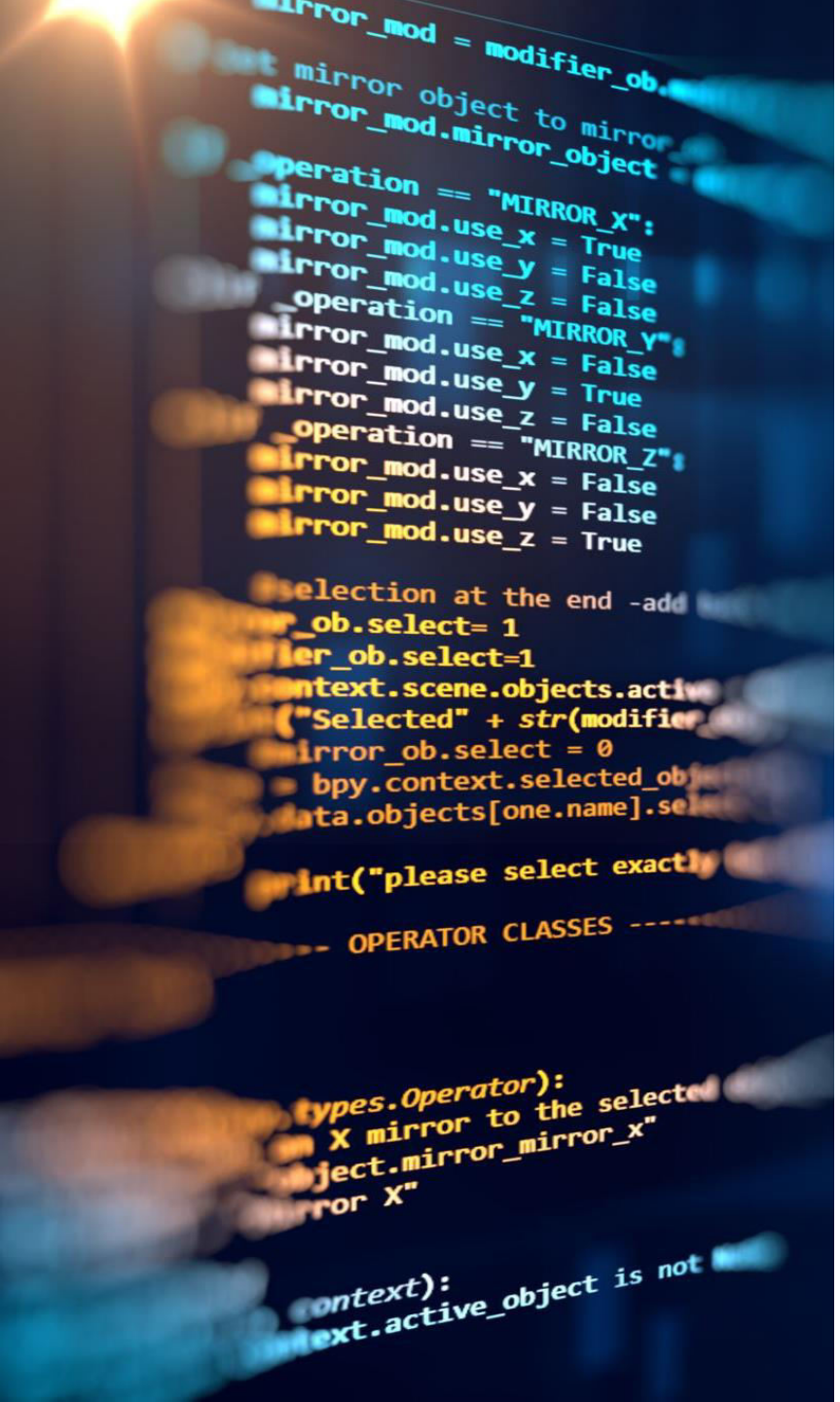
Así existen otros tipos de firewall que no son los de red.



Firewall de Windows

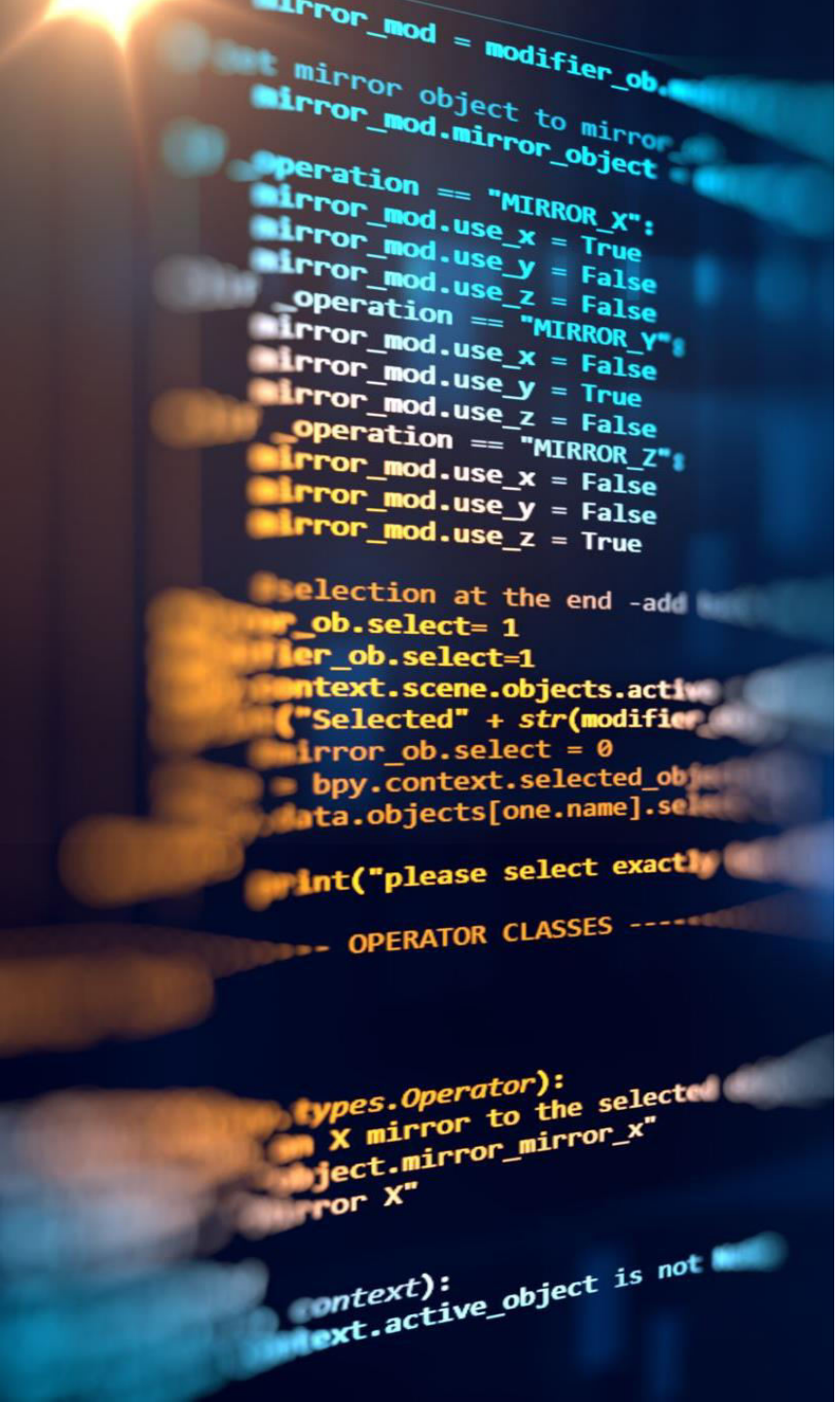
El firewall de Windows, es una parte del sistema operativo de Windows que controla las conexiones entrantes y salientes de nuestro ordenador.

Podemos configurar varias opciones y hasta podemos desactivar el cortafuegos de Windows 10 fácilmente.



Firewall Web

- Un firewall web, normalmente se encuentra instalado o funcionando dentro de nuestro servidor web o aplicación web.
- La función principal de un cortafuegos web es controlar las conexiones entrantes antes de consumir recursos web.
- Con ello podemos evitar ataques de denegación de servicio, para ataques procedentes de un IP o de IPs de un país entre otras funciones.



WAF

- Un WAF (Web Application Firewall) protege a las aplicaciones web de diversos ataques a la capa de aplicación, como el cross-site scripting (XSS), la inyección de SQL y el envenenamiento de cookies, entre otros.
- Los ataques a las aplicaciones son la principal causa de infracción (son la puerta de acceso a sus datos importantes).
- Colocando un WAF adecuado, se pueden bloquear los distintos ataques cuyo objetivo es poner en peligro los sistemas accediendo a esos datos.

WAF

¿Cómo funciona un WAF (Web Application Firewall)?

- El WAF protege sus aplicaciones web filtrando, vigilando y bloqueando todo el tráfico HTTP/S malicioso que se dirija hacia ellas e impide que salga de ellas cualquier dato no autorizado.
- Lo hace adhiriéndose a un conjunto de políticas que distinguen entre tráfico malicioso y seguro.
- Al igual que un servidor proxy actúa como intermediario para proteger la identidad de un cliente, un WAF funciona de manera similar, pero a la inversa (se llama proxy inverso), actuando como un intermediario que protege el servidor de aplicaciones web de un cliente potencialmente malicioso.
- Un WAF puede ser un software, un dispositivo o un servicio prestado.
- Las políticas se pueden personalizar para satisfacer las necesidades exclusivas de su aplicación o conjunto de aplicaciones web.
- Aunque muchos WAF requieren actualizar las políticas regularmente para abordar nuevas vulnerabilidades, los avances en el aprendizaje automático permiten a algunos WAF actualizarse automáticamente.
- Esta automatización es cada vez importante, dado que el panorama de amenazas sigue creciendo en complejidad y ambigüedad

Diferencia entre un WAF (Web Application Firewall), un IPS (sistema de prevención de intrusos) y un NGFW (Firewall de última generación)

IPS

Un **IPS** es un sistema de prevención de intrusiones, un WAF es un cortafuegos de aplicaciones web y un **NGFW** es un cortafuegos de última generación.

¿Cuál es la diferencia entre ellos?

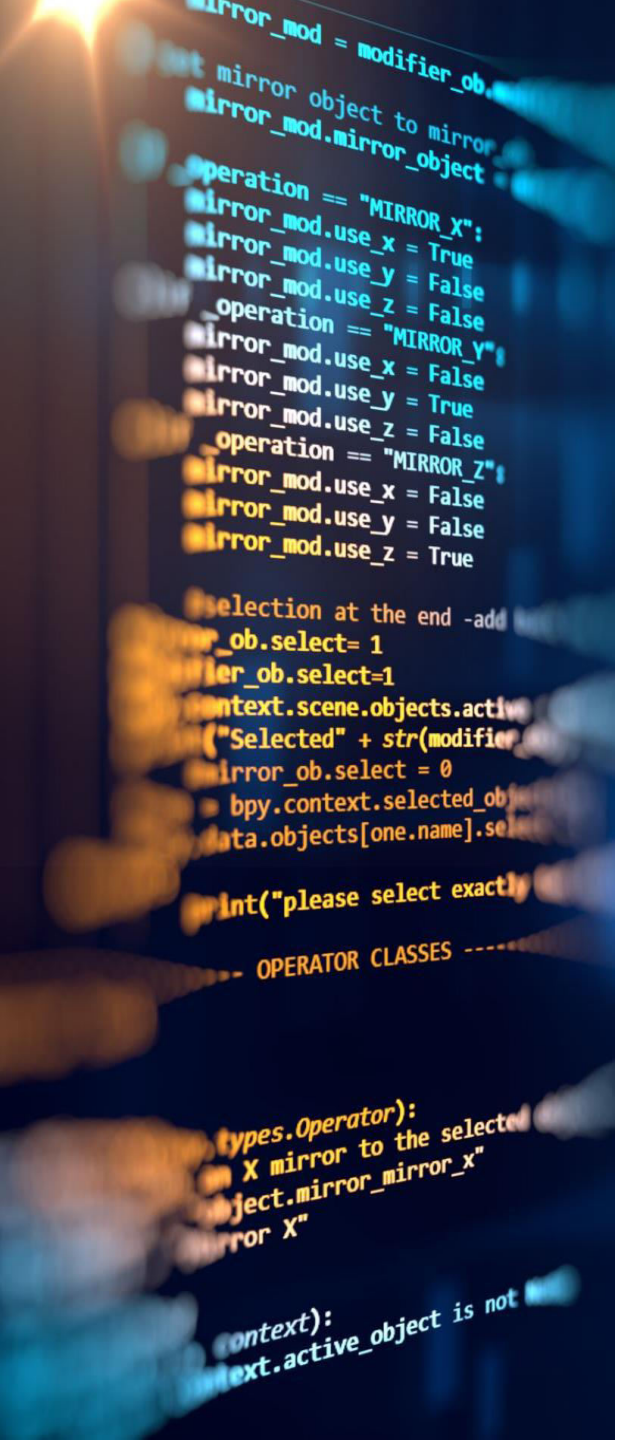
Un **IPS** es un producto de seguridad con un enfoque más amplio. Normalmente se basa en firmas y políticas, lo que significa que puede comprobar vulnerabilidades y vectores de ataque conocidos en función de una base de datos de firmas y en las políticas establecidas.

El IPS establece una norma basada en esta base de datos y estas políticas y luego envía alertas si el tráfico se desvía de la norma.

Las firmas y las políticas van creciendo a medida que se conocen nuevas vulnerabilidades.

En general, el IPS protege el tráfico a través de una gama de protocolos como DNS, SMTP, TELNET, RDP, SSH y FTP.

El IPS normalmente opera y protege las capas 3 y 4. Las capas de red y de sesión, aunque algunos pueden ofrecer una protección limitada en la capa de aplicación (capa 7).



Diferencia entre un WAF (Web Application Firewall), un IPS (sistema de prevención de intrusos) y un NGFW (Firewall de última generación)

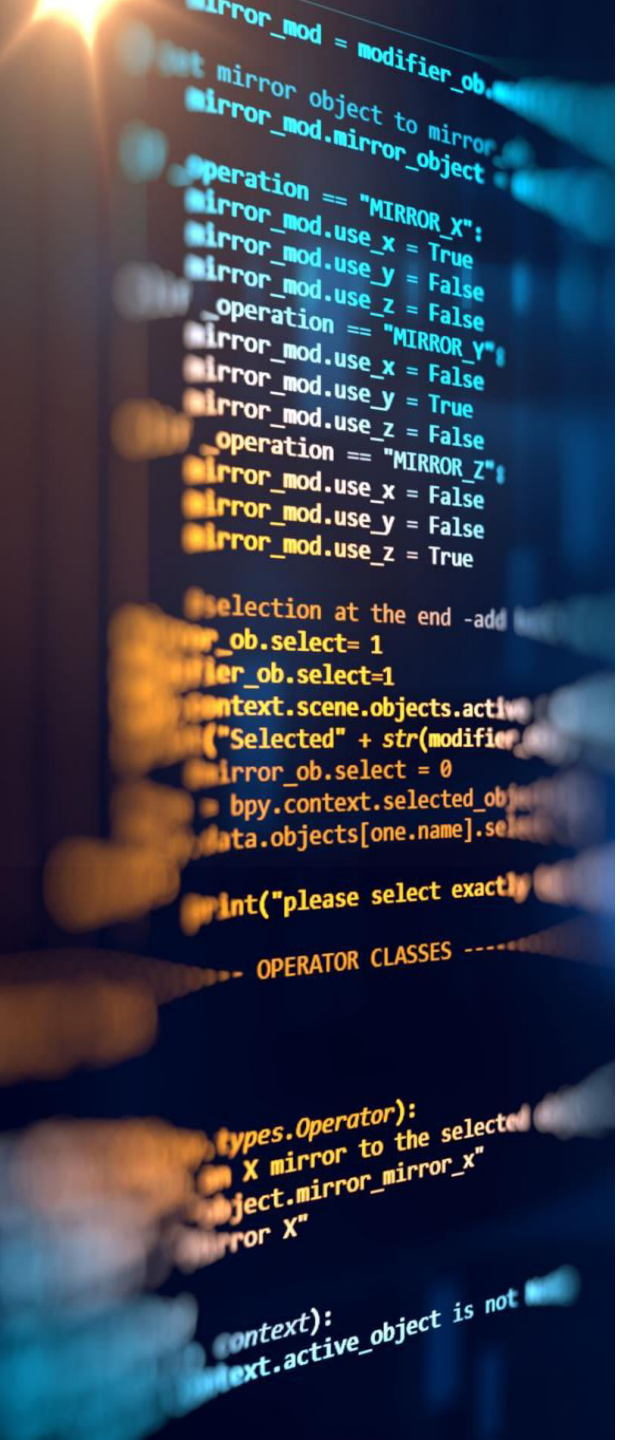
WAF

Un WAF (Web Application Firewall) protege la capa de aplicación y está diseñado específicamente para analizar cada petición HTTP/S en dicha capa.

Por lo general es consciente del usuario, la sesión y la aplicación y conoce las aplicaciones web que hay detrás y los servicios que ofrecen.

Por ello se puede considerar al WAF como un intermediario entre el usuario y la propia aplicación, que analiza todas las comunicaciones antes de que lleguen a la aplicación o al usuario.

Los WAF tradicionales garantizan que solo se puedan realizar las acciones permitidas (en función de la política de seguridad).

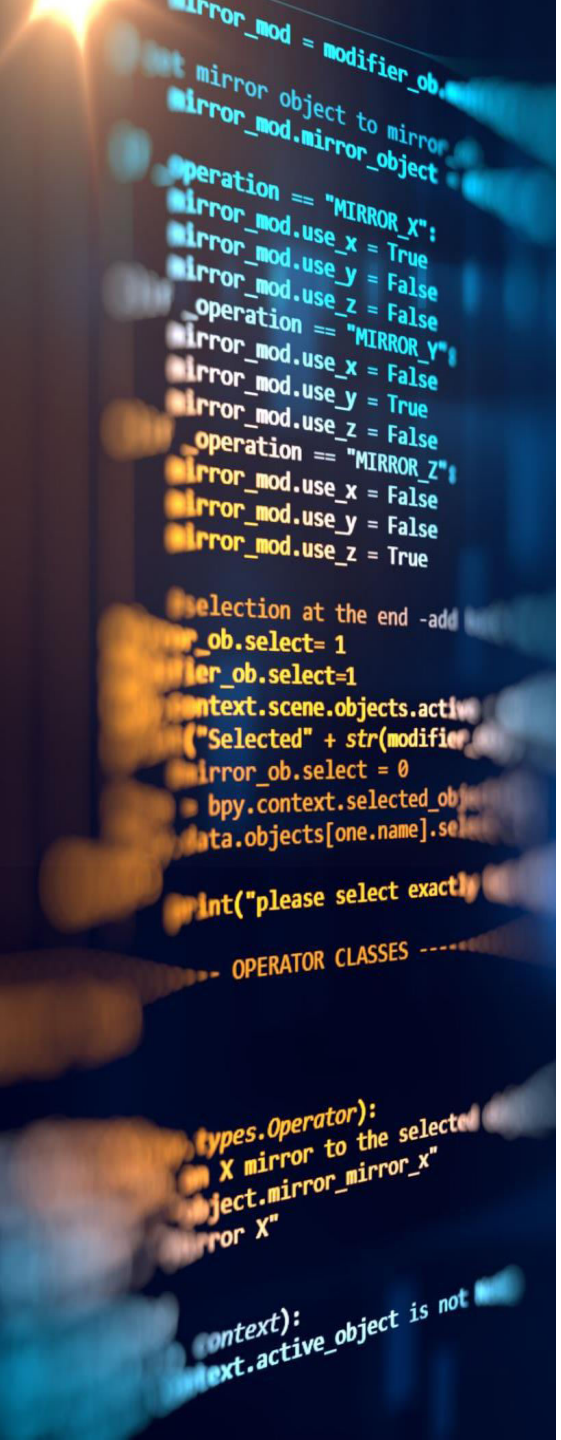


Diferencia entre un WAF (Web Application Firewall), un IPS (sistema de prevención de intrusos) y un NGFW (Firewall de última generación)

WAF

Para muchas organizaciones, las WAF son una primera línea de defensa fiable para las aplicaciones, especialmente para protegerse contra el OWASP Top 10 (la lista de las 10 vulnerabilidades de aplicaciones más comunes). Entre ellas, están las siguientes:

- Ataques de inyección
- Pérdida de autentificación
- Exposición de datos sensibles
- XXE (entidades externas XML)
- Interrupción del control de acceso
- Configuración de seguridad defectuosa
- XSS (cross-site scripting)
- Deserialización desprotegida
- Compobnetes con vulnerabilidades conocidas
- Registro y monitoreo insuficientes



Diferencia entre un WAF (Web Application Firewall), un IPS (sistema de prevención de intrusos) y un NGFW (Firewall de última generación)

NGFW

Un NGFW (Firewall de última generación) vigila el tráfico que sale a Internet (a través de sitios web, cuentas de correo electrónico y SaaS).

Las características de NGFW incluyen:

- Sistema de detección de intrusiones (IDS) y Sistema de prevención de intrusiones (IPS)
- Protección contra amenazas avanzadas (ATP)
- Seguridad del sistema de nombres de dominio (DNS)
- Control de aplicaciones
- Inspección profunda de paquetes (DPI)

El NGFW obliga a cumplir las políticas basadas en el usuario y agrega contexto a las políticas de seguridad, aparte de otras funciones como el filtrado de URL, antivirus/anti-malware, y potencialmente, sus propios sistemas de prevención de intrusos (IPS).

Mientras que el WAF suele ser un proxy inverso (utilizado por los servidores), el NGFW suele ser un proxy de avance (utilizado por clientes como navegador).

IPS e IDS

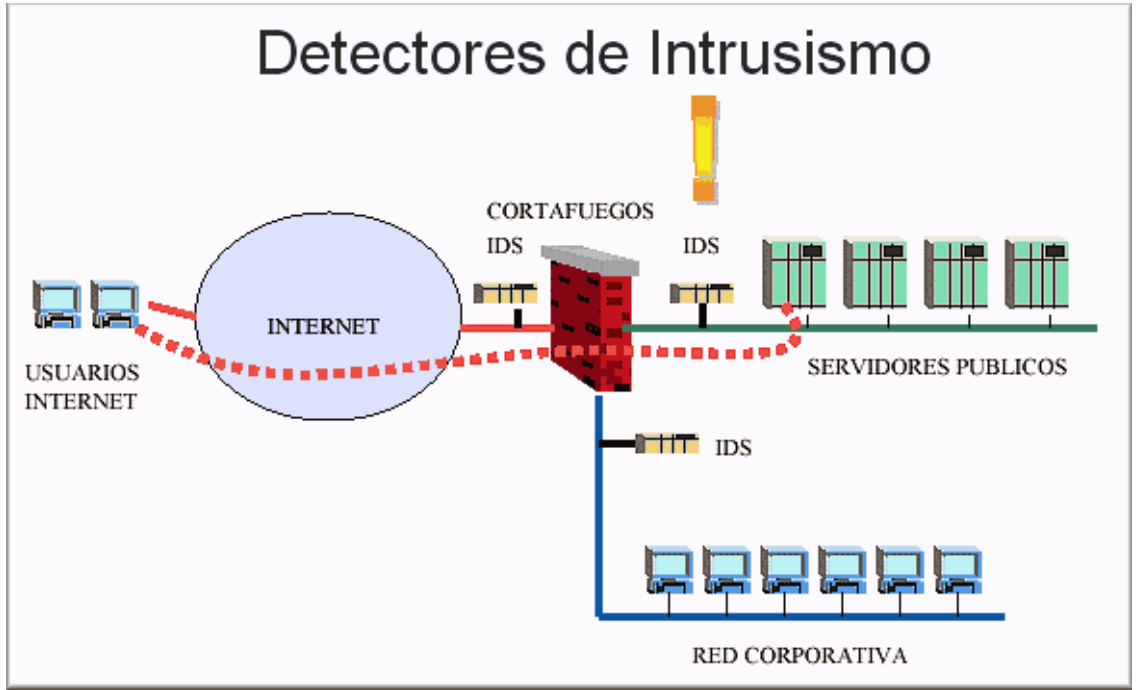
Seguridad = Visibilidad + Control

Fórmula para representar la idea de la seguridad.

IDS (*Intrusion Detection System*)

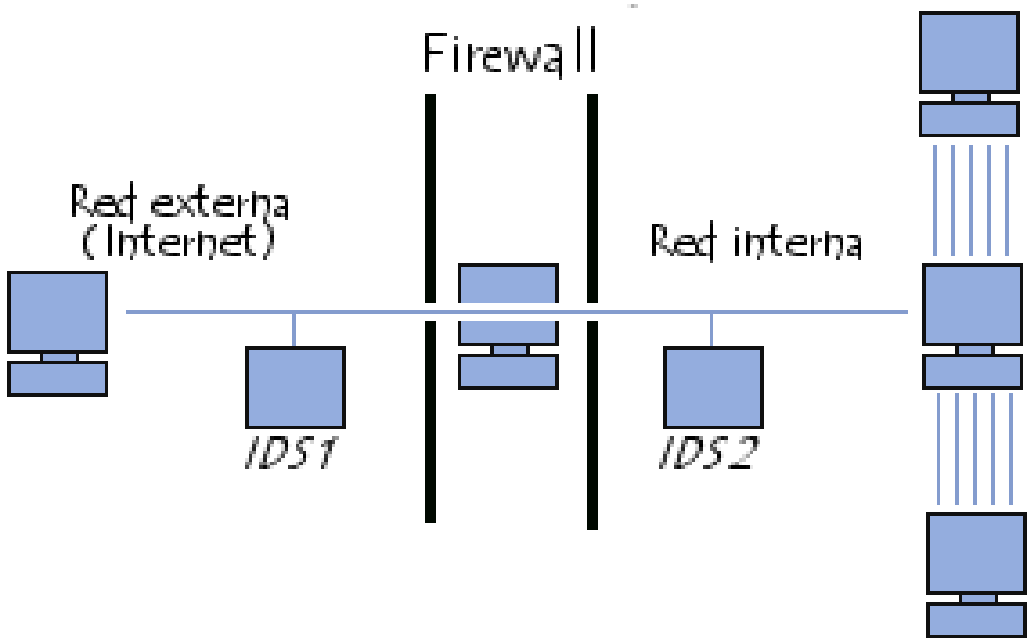
Sistema de detección de intrusos

Mecanismo que sigilosamente, escucha el tráfico en la red para detectar actividades anormales o sospechosas, y de este modo, reducir el riesgo de intrusión.



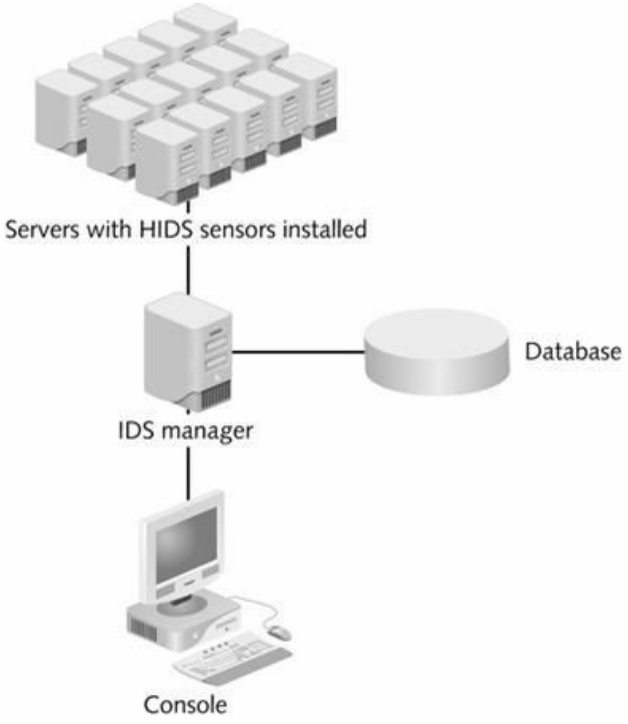
TIPOS DE IDS

HIDS (HostIDS)



NIDS (NetworkIDS)

HIDS Host-based Intrusion Detection System



Es un servidor o estación de trabajo.

Analiza los datos locales de esa máquina, como archivos de registro del sistema, cambios en el sistema de archivos y a veces los procesos del sistema.

Puede tomar medidas protectoras.

El HIDS intenta detectar tales modificaciones en el equipo afectado, y hacer un reporte de sus conclusiones.

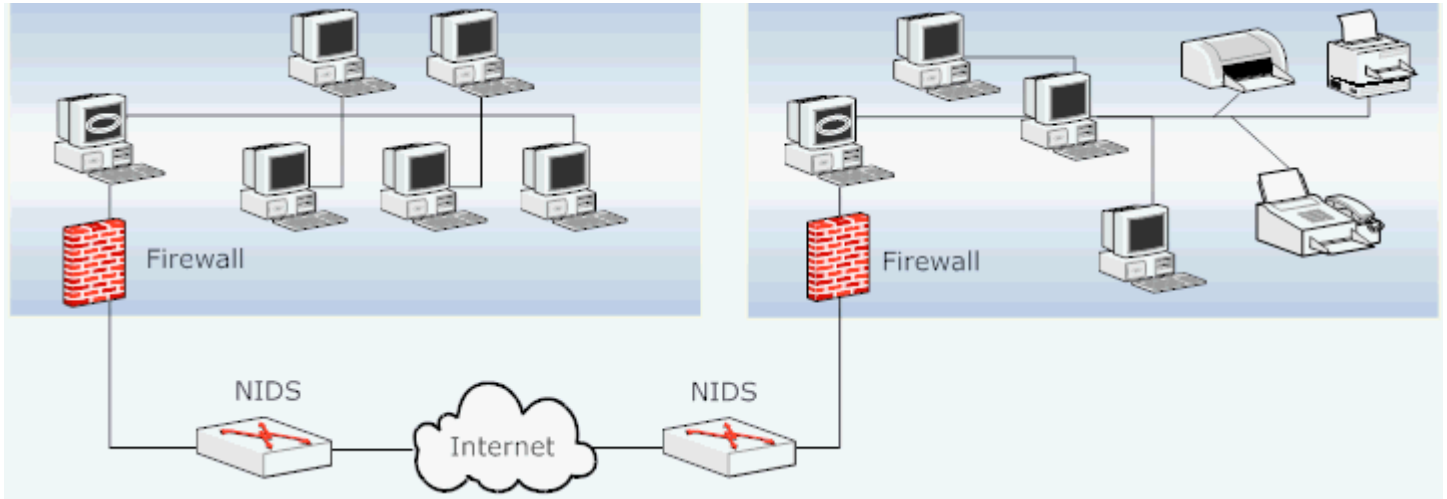
NIDS (NetworkIDS)

Es un IDS basado en red, detectando ataques a todo el segmento de la red.

Su interfaz debe funcionar en modo promiscuo capturando así todo el tráfico de la red.

Éste es una especie de modo "invisible" en el que no tienen dirección IP.

Tampoco tienen una serie de protocolos asignados.

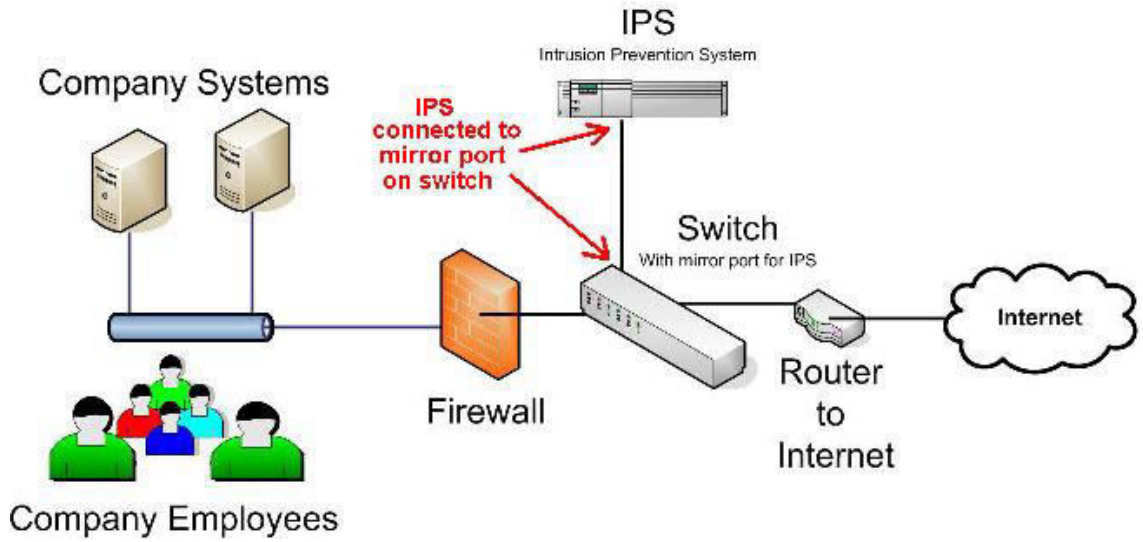


Intrusion Prevention System (IPS)

Es un sistema control de acceso en una red para proteger a los equipos internos de ataques.

Se utiliza para desconectar conexiones que no tienen autorización.

Los IPS presentan una mejora importante sobre las tecnologías de cortafuegos tradicionales, al tomar decisiones de control de acceso basados en los contenidos del tráfico, en lugar de direcciones IP o puertos.

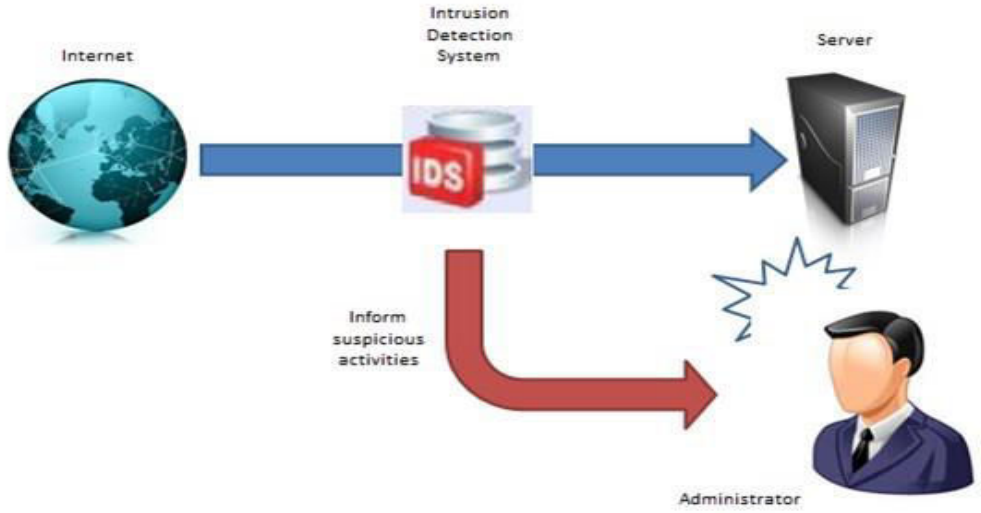


Instalación de un IDS fuera de la frontera del firewall y del Router

Permiten ver la amplitud de los intentos de ataques en contra de la empresa.

- Proporciona herramienta que captura datos para el análisis y posiblemente estudios forenses.

Fuera de la arquitectura de banda, se sitúa en un punto compartido en donde captura tantos paquetes como se pueda para manejar en un modo promiscuo y pueda dar informes de los resultados.

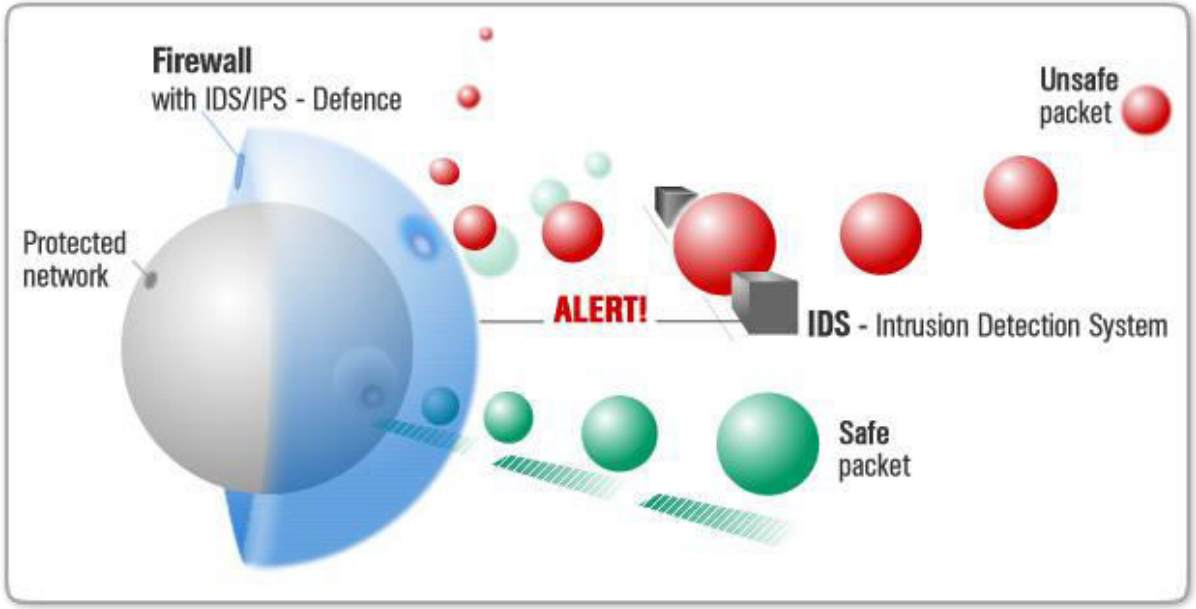


Instalación de IDS en despliegue en línea

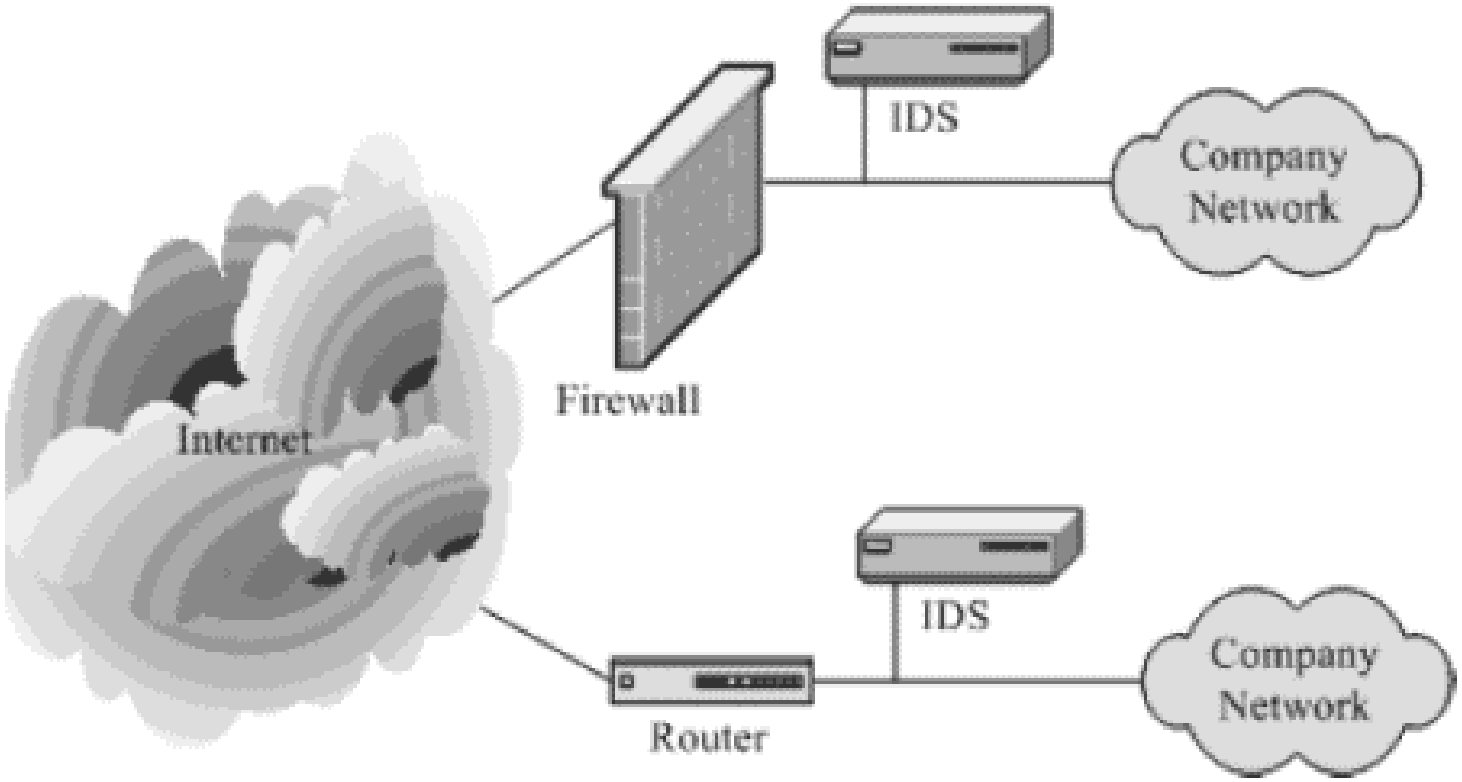
Todos los datos procedentes de entrada y salida deben pasar a través del dispositivo.

De igual manera cuenta con desventajas como:

- Si el dispositivo en línea falla, la conexión se detendrá y de igual manera la visibilidad del IDS, hasta que el mismo se fije o se elimine.

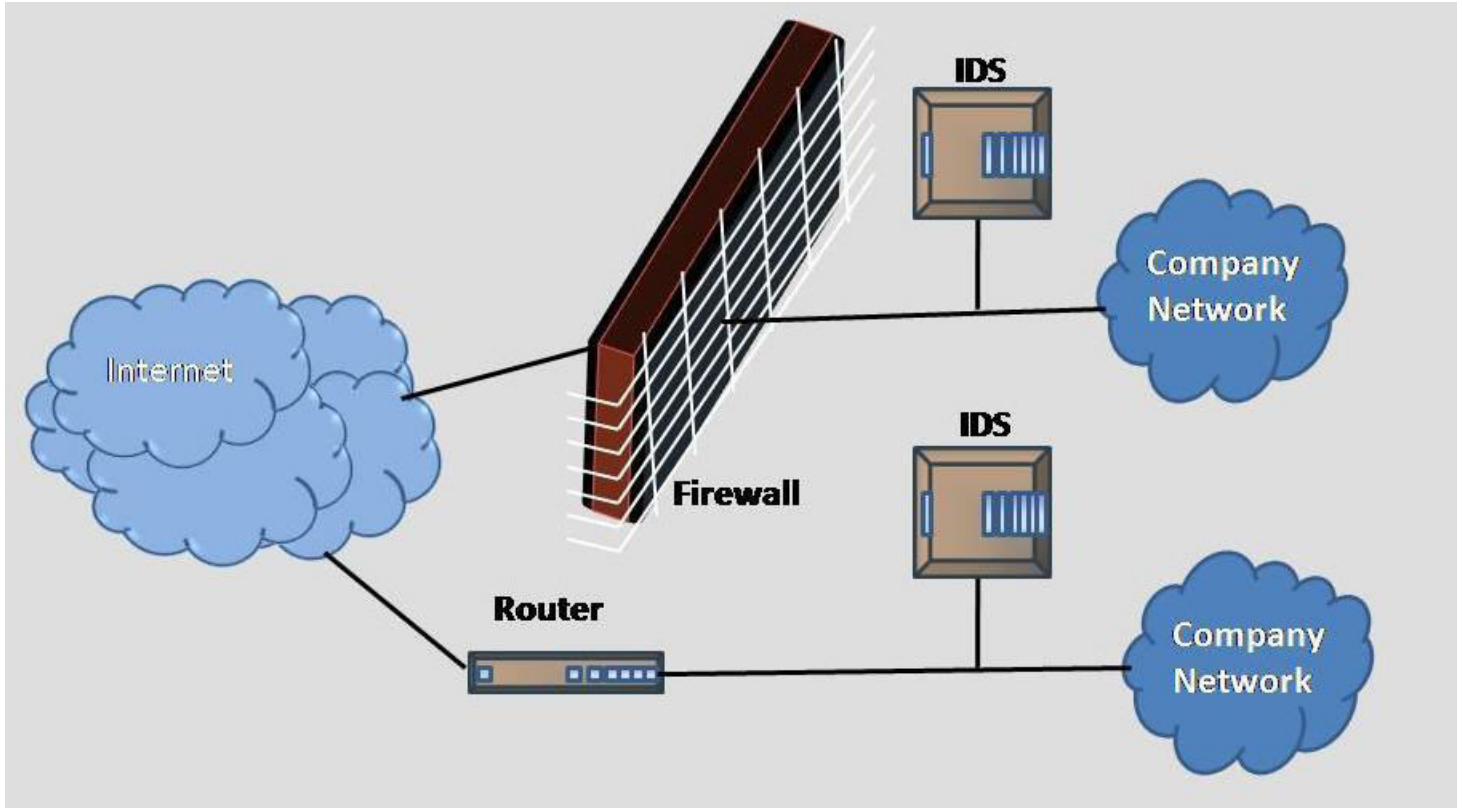


Instalación de dispositivos IDS en puntos primarios de red para proporcionar visibilidad.



Este tipo de despliegue proporciona los datos necesarios para localizar a potenciales amenazas internas, así como los que se plantean en contra de la empresa desde el exterior.

Preocupaciones de los despliegues de IDS

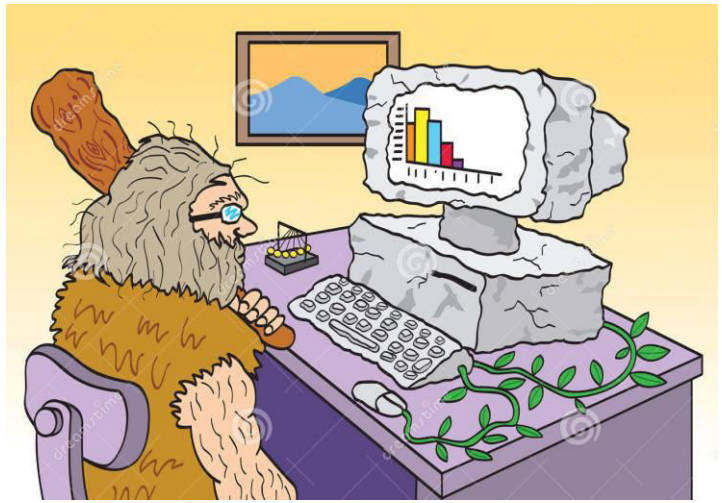


El factor de rendimiento.

El cifrado.

Con el crecimiento explosivo de VPN y otros datos cifrados han desarrollado la necesidad de tener una solución como IPS en donde el perímetro es cada vez más necesario.

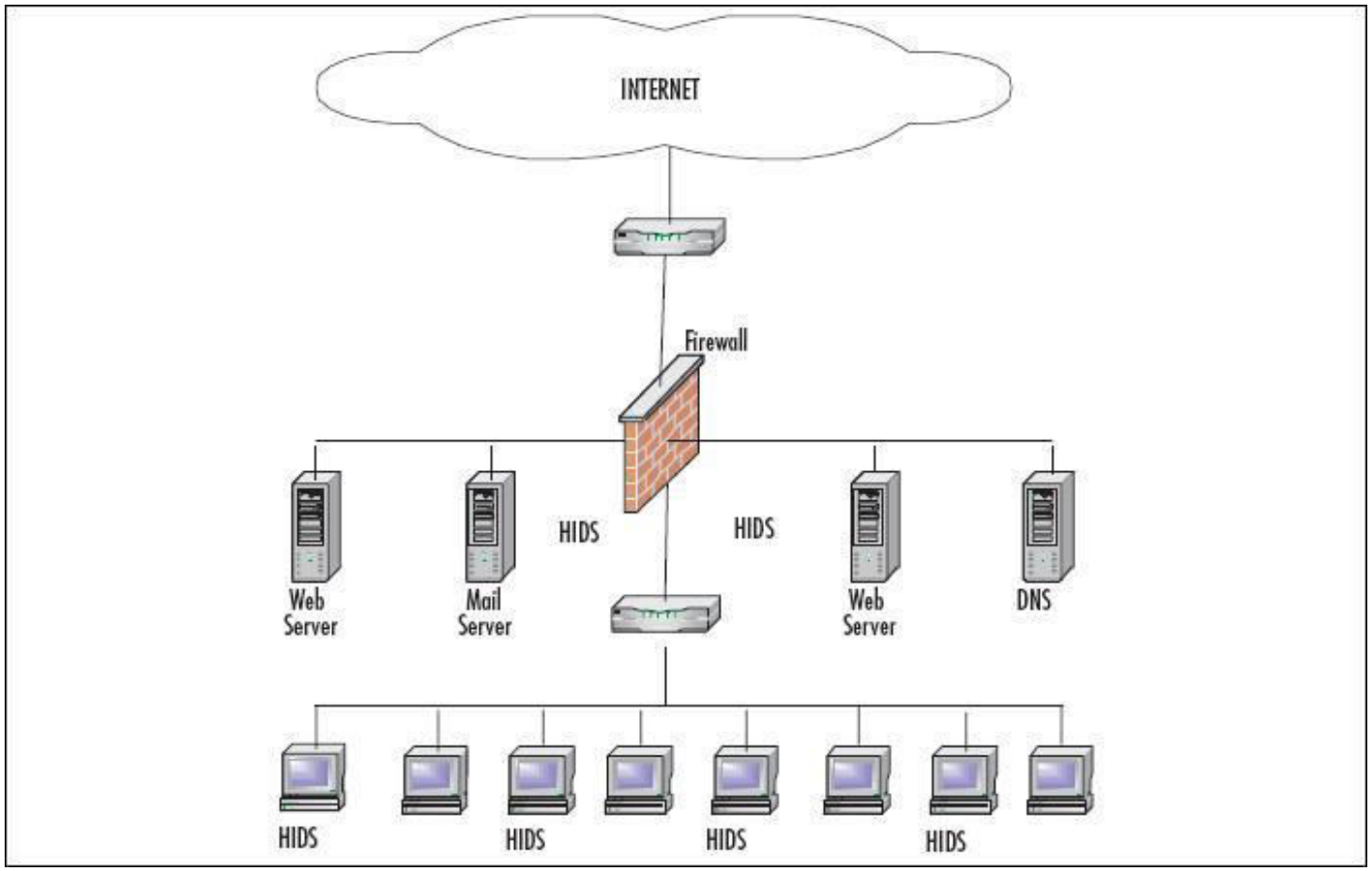
IDS puede convertirse en obsoleto



No puede cifrar el tráfico analizado.

Con el tiempo las redes crecen y necesitan cada vez de más equipos, por lo tanto necesitan más número de sensores (IDS) a lo cual el costo también aumenta.

Genera una cantidad muy grande de “posibles ataques” (falsos positivos) cuando estos pueden no serlo.



Para erradicar los problemas con IDS.

Añadir IDS basados en host (HIDS).

El uso de un HIDS ofrece la visibilidad necesaria para identificar y rastrear intrusiones, intentos de filtrado en un host o una aplicación específica.

Tecnologías en IPS

Las tecnologías IPS en software o hardware son relativamente nuevas.

Se puede decir que los firewalls y las listas de acceso son consideradas como IPS básicas.

Al combinar las capacidades de bloqueo de un firewall con un IDS se obtiene un IPS7.

La tecnología IPS es fundamental porque el tiempo es dinero y la disponibilidad de la red es fundamental para todas las organizaciones.

Despliegues de IPS no generan ingresos

Por esta razón es difícil justificar el gasto en empresas.

Por lo contrario; sin visibilidad de la red, y la capacidad de prevenir intrusos y ataques a la red existe un argumento de los costos asociados con esta actividad.

Argumentos para implementar IPS

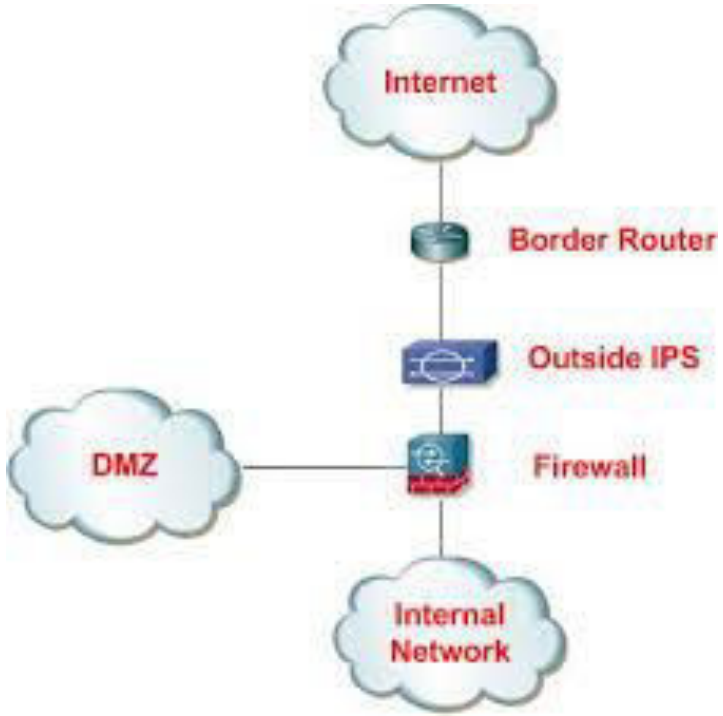
Podría ahorrar dinero a través de la identificación y la prevención de un ataque de gusano o virus.

Por lo general las empresas desarrollar matrices para cuantificar la cantidad de dinero y/o el tiempo perdido debido a virus o a los ataques de gusanos, está información se puede obtener con el IPS .

Ahorros potenciales asociados con la prevención en tiempo de inactividad.

Hacer frente a las amenazas internas.

Recomendaciones



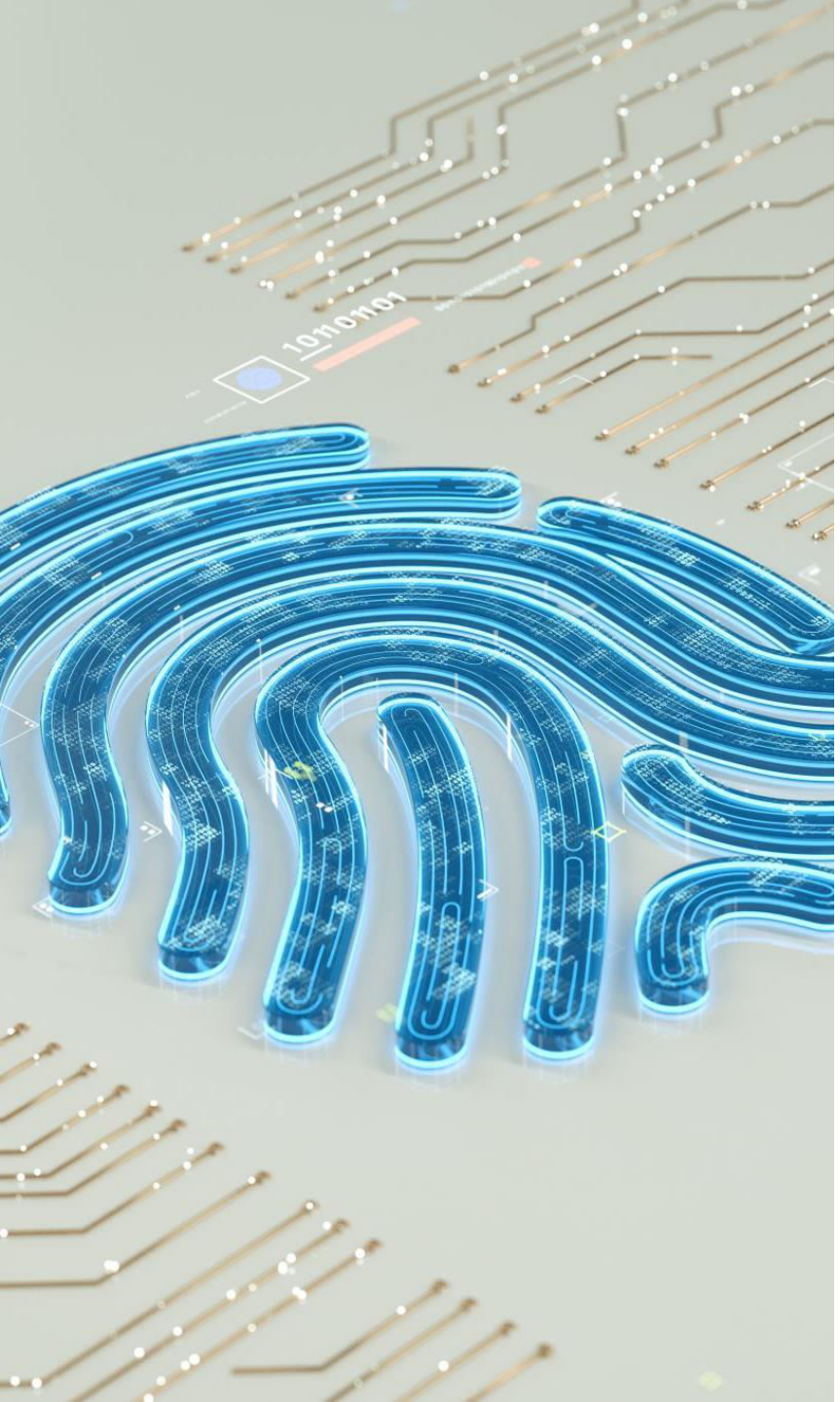
- Colocar estratégicamente tecnologías IPS en el perímetro de la red para ayudar en la prevención de cero ataques como gusanos o virus a través de reglas basadas en anomalías, así como inspección basada en la firma de paquetes.
- Usar correctamente una solución IPS en todos los puntos de ingreso/egreso ayudará a asegurar que las amenazas más nuevas no ingresen al perímetro.
- Asegurar que solo el tráfico legitimo pueda pasar.

Fabricantes hardware y/o soluciones de Seguridad

Cisco Umbrella

CISCO UMBRELLA ES UNA APLICACIÓN INTEGRADA EN LA BASE DE INTERNET

- **Cisco Umbrella** utiliza la infraestructura de Internet para bloquear destinos maliciosos antes de que se establezca una conexión.
- Al ofrecer seguridad desde la nube, no sólo ahorra dinero a las empresas, sino que también les proporciona una seguridad más efectiva.
- Las compañías que apuesten por implementar una solución como **Cisco Umbrella** se benefician de una plataforma de seguridad que es capaz de impedir que se infecten sus datos confidenciales incluso antes de que el ataque malicioso sea lanzado.

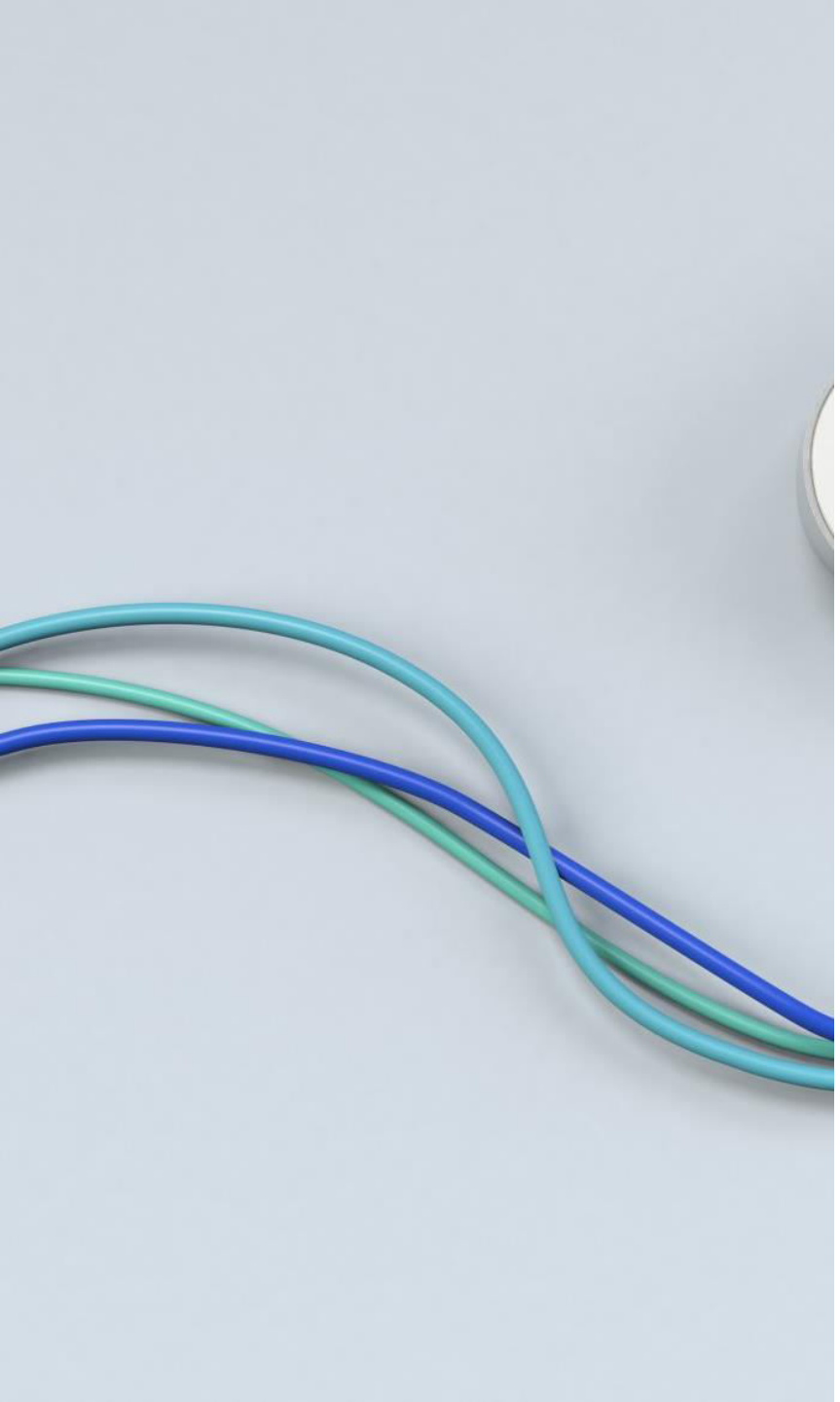


CISCO UMBRELLA CUENTA CON INTELIGENCIA DE AMENAZAS

- La solución de seguridad de **Cisco** dispone de un sistema de inteligencia de amenazas que le permite ver los ataques antes de que se lancen.
- Gracias a esta tecnología, Umbrella aprende de la actividad de Internet para identificar automáticamente la infraestructura del atacante y defenderse de ella.
- **Umbrella** es capaz de analizar los datos para identificar patrones, detectar anomalías y crear modelos para predecir si un dominio o IP es malicioso o no lo es.
- Además, correlaciona automáticamente los datos y bloquea ataques cuando es necesario.

CISCO UMBRELLA PERMITE VISUALIZAR TODO EL TRÁFICO TANTO SI ESTÁN O NO CONECTADOS

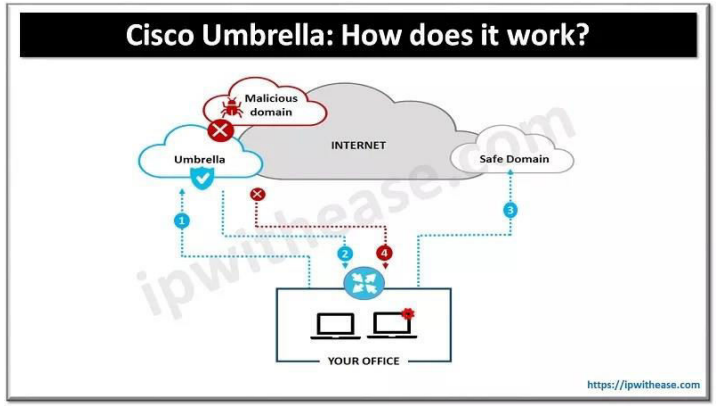
- La solución **Cisco Umbrella** visualiza toda la actividad de Internet de todos los dispositivos en todos los puertos, incluso en el caso que los usuarios se hayan desconectado de la red.
- De esta manera, las organizaciones que se hagan con **Cisco Umbrella** podrán controlar en todo momento el comportamiento de sus usuarios para comprobar si están en lugares seguros o, por el contrario, se encuentran en peligro.



CISCO UMBRELLA SE IMPLEMENTA EN TODA LA EMPRESA EN MINUTOS

- La plataforma de seguridad **Cisco Umbrella** se implementa de un modo sencillo.
- No hay ninguna clase de hardware para instalar ni software para actualizar de manera manual.
- Además, la interfaz del navegador permite una configuración rápida y una administración continua.
- Las empresas que decidan apostar por una solución de seguridad como **Cisco Umbrella** podrán dotar a su propia red de un nivel de protección máximo con el mínimo esfuerzo.
- En este sentido, las organizaciones no tendrán que dedicar muchas horas de personal IT a instalar y gestionar la red, ya que esto se hace de manera sencilla.

¿CÓMO TRABAJA CISCO UMBRELLA?



- Cisco Umbrella construido desde la base de Internet Cisco cuenta con 25 data centers en todo el mundo.
- Están conectados con 500 de los más importantes proveedores de Internet o ISPs y redes de entrega de contenido o CDNs para intercambiar rutas BGP.
- Centros de datos de calidad que no añaden más latencia sobre los proveedores regionales de DNS y que mantienen, además, el tiempo de actividad al 100% desde que esta red de Cisco empezó a funcionar en 2006.
- De esta manera, la empresa dispone de una red automatizada que funciona 24 horas los siete días de la semana.
- El centro de operación de la red que monitoriza y gestiona el enrutamiento de IP anycast y otras protecciones para asegurar la actividad al 100%, ha manejado aproximadamente el 2% de la actividad de Internet durante los últimos cinco años.

Cisco Umbrella cuenta con inteligencia para visualizar ataques antes de que se produzcan

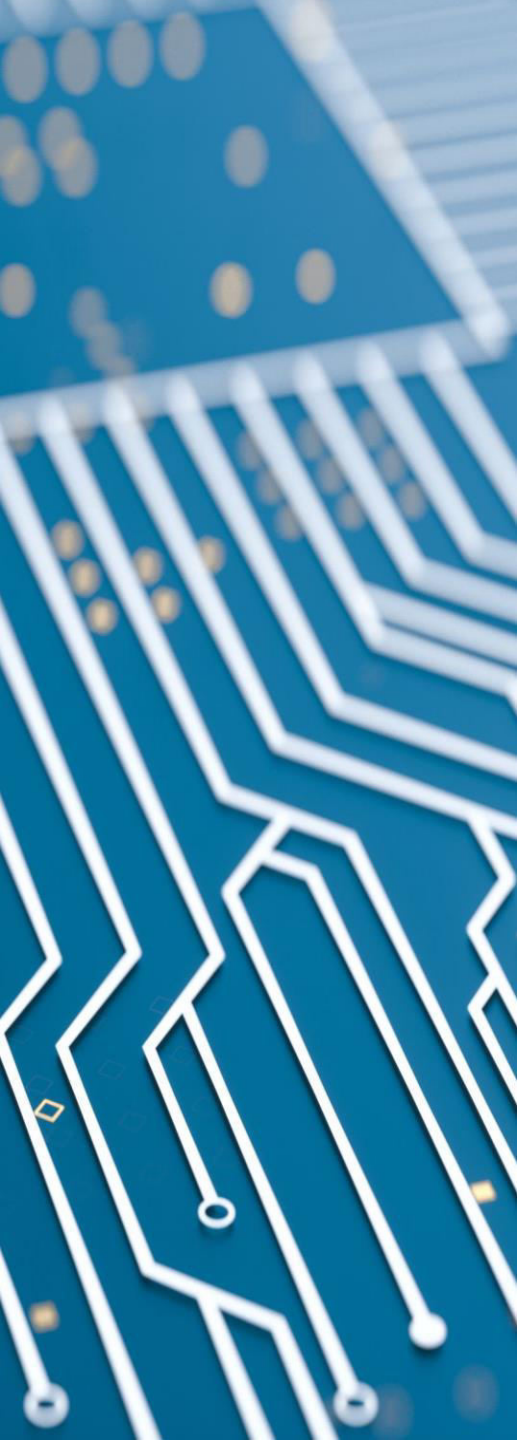
Cisco recoge toda la información de la red en tiempo real en una base de datos y la plataforma ejecuta continuamente modelos estadísticos que permiten analizar los datos para investigar las amenazas de Internet, en una combinación de inteligencia y machine learning, para identificar sitios maliciosos de la red.

Cisco Umbrella cuenta con inteligencia para visualizar ataques antes de que se produzcan cont.

En este sentido, Umbrella trabaja a partir de los siguientes modelos:

- **Modelo de Co-ocurrencia** El análisis estadístico de los datos se basa en el modelo de co-ocurrencia, el cual identifica los dominios consultados antes o después de un dominio dado. Este modelo ayuda a descubrir dominios unidos al mismo ataque, incluso si estos están alojados en redes separadas
- **Modelo de procesamiento natural del lenguaje** El análisis estadístico también se basa en el modelo de procesamiento natural del lenguaje. Un procedimiento para detectar nombres de dominio que falsifiquen términos y marcas. Indicios más que suficientes para descubrir dominios sospechosos.
- **Modelo spike-ranked** El análisis estadístico también se basa en el modelo "spike-ranked". El modelo "spike ranked" reconoce cuándo las puntas de tráfico en un dominio, encajan con los patrones vistos en otros ataques y así poder bloquear amenazas antes de que se produzcan.
- **Modelo del monitoreo predictivo del espacio IP** El análisis estadístico también se basa en el modelo del monitoreo predictivo del espacio IP. El modelo del monitoreo predictivo del espacio IP empieza con los dominios identificados por el modelo "spike ranked". Se anotan los pasos a los atacantes para aprovechar la configuración de la infraestructura, como el nombre del proveedor del hosting, el servidor, la IP, etc., para predecir este identificador y comprobar si son maliciosos y así bloquear sitios de forma proactiva antes de que se inicie el ataque.

Fortinet



Fortinet

- Fortinet es una empresa de tecnología de la información que se dedica a la ciberseguridad.
- La empresa ofrece una amplia gama de soluciones de seguridad informática, incluyendo hardware, software

y servicios en la nube para proteger redes, sistemas, aplicaciones y datos contra una amplia variedad

de amenazas cibernéticas.

- Entre las soluciones de seguridad que ofrece Fortinet se encuentran firewalls de última generación,

soluciones de seguridad de acceso remoto, protección contra amenazas avanzadas, soluciones de seguridad

para aplicaciones en la nube, gestión unificada de amenazas (UTM) y soluciones de seguridad para redes

inalámbricas.

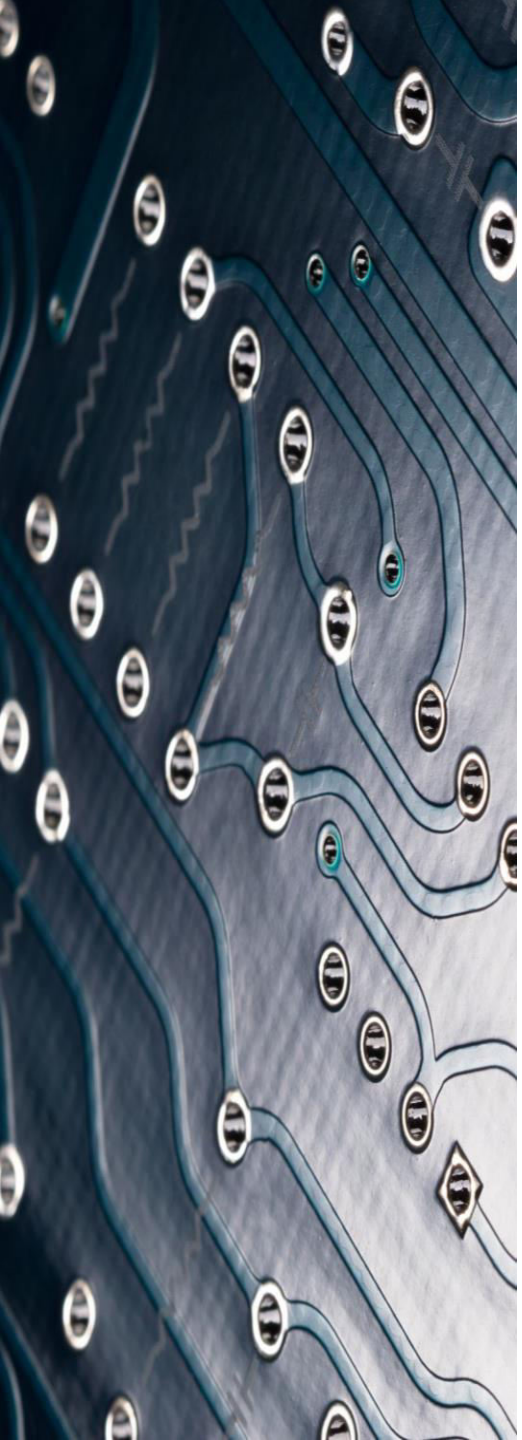
- Fortinet tiene presencia en más de 100 países y cuenta con una amplia base de clientes en

diversos sectores, incluyendo empresas, proveedores de servicios y gobiernos.

- Los *Firewall Fortinet* (también conocidos como *firewalls* de próxima generación *NGFW* o simplemente *FortiGate)*

son dispositivos de seguridad que permiten la creación de redes seguras y proporcionan una protección amplia,

integrada y automatizada



Fortinet

Fortinet ofrece una amplia gama de soluciones de seguridad informática para ayudar a proteger redes,
sistemas, aplicaciones y datos contra una variedad de amenazas cibernéticas.
Algunas de las soluciones más populares de Fortinet incluyen:

1. **FortiGate**: Una plataforma de seguridad de redes de próxima generación que combina firewall, VPN,
seguridad de red avanzada, gestión de tráfico y más.
2. **FortiManager**: Una solución centralizada de gestión de seguridad para simplificar y automatizar la
administración de múltiples dispositivos Fortinet.
3. **FortiAnalyzer**: Una solución de gestión y análisis de registros de seguridad para recolectar, correlacionar
y analizar datos de eventos de seguridad.
4. **FortiWeb**: Una solución de seguridad de aplicaciones web que protege contra ataques de aplicación web
Y proporciona visibilidad y control de las aplicaciones web.
5. **FortiMail**: Una solución de seguridad de correo electrónico que protege contra amenazas de correo
electrónico, como phishing y malware, y proporciona herramientas de colaboración seguras.
6. **FortiEDR**: Una solución de respuesta a incidentes de endpoint que ofrece detección y respuesta de
amenazas en tiempo real para endpoints, servidores y dispositivos IoT.
7. **FortiSIEM**: Una solución de gestión de seguridad de la información y eventos que proporciona visibilidad
y correlación de eventos de seguridad de múltiples fuentes.

Estas son solo algunas de las soluciones que Fortinet ofrece, y la y desarrollando
nuevas soluciones de seguridad para adaptarse a las necesidades ca

Fortinet

Características de un FortiGate

Cabe destacar que los FortiGate son bien conocidos tanto por su rendimiento como por su eficacia de seguridad, para tener más claro esto, veamos las siguientes características avanzadas con las que cuentan:

- **Control de aplicaciones:** Permite crear políticas rápidamente para permitir, denegar o restringir el acceso a aplicaciones o categorías completas de aplicaciones.
- **Prevención de intrusiones:** Protege contra intrusiones en la red mediante la detección y el bloqueo de amenazas antes de que lleguen a los dispositivos de red.
- **Antivirus:** Efectivo contra virus, software espía y otras amenazas a nivel de contenido.
- **Filtrado de URL:** Bloquea el acceso a sitios web maliciosos, pirateados o inapropiados.
- **Sandboxing:** Es una solución avanzada de detección de amenazas para protegernos identificando *malware* previamente desconocido.
- **Inspección SSL:** Obtén visibilidad del tráfico cifrado y previene el *malware.*

Fortinet

FortiGate y SD-WAN

Los equipos *Fortigate* vienen con capacidades *SD-WAN* integradas. Esto significa que los clientes obtienen funcionalidades muy avanzadas (como es el caso de *SD-WAN)* sin complejidad y sin costo adicional.

FortiGate SD-WAN es rico en características e incluye todas las funciones típicas de *SD-WAN*, por mencionar algunos ejemplos:

- *Application Steering*
- *WAN Path Control*
- Aprovisionamiento *Zero Touch.*

Para las organizaciones que están migrando a aplicaciones en la nube, *FortiGate SD-WAN* proporciona acceso directo a Internet para reducir la latencia y aumentar el rendimiento de las aplicaciones. Para que esto sea posible, *Fortinet* proporciona visibilidad en más de 3000 aplicaciones.

Luego, se puede priorizar el tráfico crítico para el negocio proporcionando un alto rendimiento de las aplicaciones.

Por último, es importante mencionar que *FortiGate* ofrece el mejor rendimiento de ***VPN IPSEC*** de la industria, asegurando el rendimiento de las aplicaciones lo cual es un requisito fundamental para *SD-WAN*.

F5

F5

F5 Networks es una empresa que ofrece soluciones de entrega de aplicaciones y seguridad de

aplicaciones en la nube y en redes empresariales.

La empresa se enfoca en ayudar a las organizaciones a garantizar la disponibilidad, rendimiento y

seguridad de sus aplicaciones, lo que permite una mejor experiencia de usuario.

F5

Las soluciones de F5 Networks incluyen:

1.Balanceadores de carga: F5 ofrece una variedad de balanceadores de carga de alta disponibilidad que distribuyen el tráfico de red y optimizan el rendimiento de las aplicaciones.
2.Servicios de entrega de aplicaciones: F5 proporciona soluciones para acelerar y optimizar la entrega de aplicaciones, lo que mejora la experiencia del usuario y reduce el costo de ancho de banda.
3.Seguridad de aplicaciones: F5 ofrece soluciones de seguridad de aplicaciones que protegen las aplicaciones y los datos de amenazas, incluyendo ataques de inyección de SQL, cross-site scripting (XSS) y denegación de servicio (DoS).
4.Protección contra ataques DDoS: F5 ofrece soluciones para proteger las aplicaciones y los sistemas contra ataques DDoS y otros ataques de red.
5.Servicios de seguridad en la nube: F5 ofrece soluciones de seguridad en la nube que protegen las aplicaciones y los datos en la nube pública y privada.
Las soluciones de F5 Networks son utilizadas por empresas de diversos sectores, incluyendo finanzas, salud, gobierno, medios de comunicación y tecnología.
La empresa tiene presencia en todo el mundo y cuenta con una amplia base de clientes.

F5

Es una empresa que tiene soluciones propias tanto de harware como de software y además integra con otros vendors.

Seguridad de aplicaciones

Access Policy Manager:

F5 BIG-IP Access Policy Manager (APM) protege, simplifica y centraliza el acceso a las aplicaciones, las API y los datos, sin importar dónde se encuentren los usuarios y sus aplicaciones.

Advanced WAF:

BIG-IP Advanced WAF puede identificar y bloquear los ataques que otras soluciones WAF no detectan.

SSL Orchestrator:

SSL Orchestrator proporciona un cifrado/descifrado robusto del tráfico SSL/TLS.

F5

Seguridad de aplicaciones

DDoS Hybrid Defender:

Proporciona una mayor profundidad de defensa. Es la única defensa de varias capas que protege contra ataques de red combinados y sofisticados ataques de aplicaciones, a la vez que permite el descifrado completo de SSL, capacidades anti-robots y métodos avanzados de detección, todo en un solo dispositivo. También ofrece el máximo rendimiento con capacidades de velocidad de línea y sin afectar al tráfico legítimo.

Advanced Firewall Manager:

Mitiga las amenazas de red antes de que interrumpan los recursos críticos del centro de datos

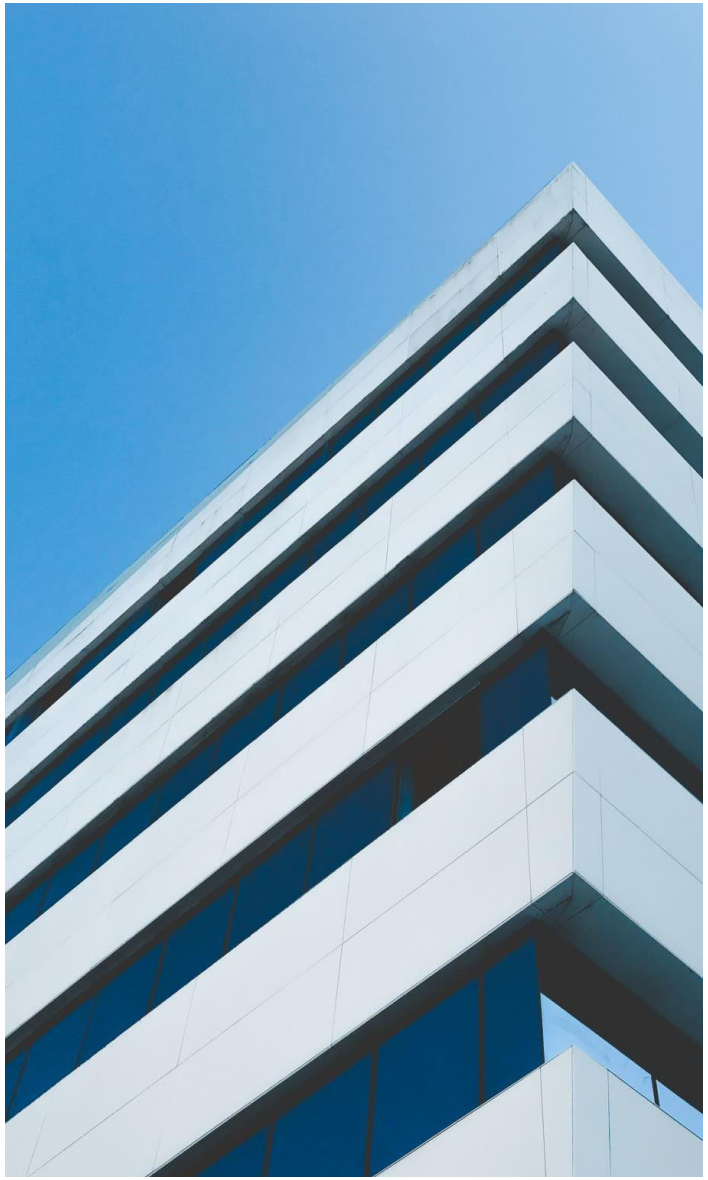
Distributed Cloud WAAP en comparación con la CDN tradicional

Características	CDN tradicional	Distributed Cloud WAAP
Automatización de la implantación y los cambios de política	✓	✓
Visualización de infracciones, patrones de tráfico y eventos de DDoS	✓	✓
Autodescubrimiento de API e inclusión en lista	✓	✓
Escaneo de firmas e IA/aprendizaje automático para la detección de anomalías y usuarios malintencionados	✗	✓

F5

Distributed Cloud WAAP(Web Application and API Protection:

Palo Alto



Palo Alto Networks

Palo Alto Networks es una empresa de seguridad de redes y ciberseguridad con sede en California, Estados Unidos.

Se especializa en el desarrollo y venta de soluciones de seguridad de próxima generación que protegen las redes y los sistemas contra amenazas cibernéticas.

Algunas de las soluciones y productos más conocidos de Palo Alto Networks son:

1.Palo Alto Networks Next-Generation Firewall (NGFW): Estos firewalls de última generación ofrecen una protección integral contra amenazas, como malware, exploits y ataques cibernéticos avanzados.

También incluyen funciones de inspección de aplicaciones, control de acceso y prevención de intrusiones (IPS).

2.Prisma Access: Es una solución de seguridad en la nube que proporciona acceso seguro a aplicaciones y datos, independientemente de la ubicación de los usuarios. Ofrece protección avanzada contra amenazas y políticas de seguridad coherentes en redes distribuidas y entornos de nube.

Palo Alto Networks

3.Cortex XDR: Esta solución es una plataforma de detección y respuesta extendida (XDR) que permite la detección temprana y la respuesta a amenazas avanzadas en tiempo real. Utiliza análisis avanzados y automatización para identificar y responder rápidamente a actividades sospechosas en la red.

4.Panorama: Es una plataforma de gestión centralizada que permite la administración y el monitoreo unificados de múltiples firewalls de Palo Alto Networks. Proporciona una visibilidad completa de la red y simplifica las tareas de configuración, políticas y generación de informes.

5.WildFire: Es una solución de análisis y detección de amenazas basada en la nube.

Analiza archivos y enlaces en busca de malware y otras amenazas desconocidas utilizando técnicas avanzadas de inteligencia artificial y aprendizaje automático.

McAfee

McAfee® Endpoint Security

McAfee® Endpoint Security

- Es una solución de seguridad integrada y ampliable que protege servidores, sistemas de equipos, portátiles y tabletas contra amenazas conocidas y desconocidas.
- Las posibles amenazas incluyen malware, comunicaciones sospechosas, sitios web no seguros y archivos descargados.
- Endpoint Security facilita que múltiples tecnologías de defensa se comuniquen en tiempo real para analizar y proteger contra amenazas.

McAfee® Endpoint Security

Endpoint Security consiste en estos módulos de seguridad:

Prevención de amenazas: evita que la amenazas accedan a los sistemas, analiza los archivos automáticamente cuando se accede a ellos y ejecuta análisis dirigidos en busca de malware en los sistemas cliente.

Firewall: supervisa la comunicación entre el equipo y los recursos de la red e Internet. Intercepta las comunicaciones sospechosas.

Control web: supervisa las búsquedas web y la actividad de navegación en los sistemas cliente y bloquea los sitios web y descargas según las calificaciones de seguridad y el contenido.

Protección adaptable frente a amenazas: analiza el contenido de su empresa y decide cómo responder en función de la reputación de los archivos, las reglas y los umbrales de reputación.

El módulo Ajustes generales proporciona la configuración para las funciones comunes, tales como la seguridad de interfaz y el registro. Este módulo se instala automáticamente si se instala cualquier otro módulo.

Todos los módulos se integran en una única interfaz de Endpoint Security en el sistema cliente. Cada módulo funciona conjuntamente e independiente para proporcionar varios niveles de seguridad.

McAfee® Endpoint Security – Como funciona

Endpoint Security intercepta las amenazas, supervisa el mantenimiento general del sistema y proporciona información sobre el estado y detecciones.

El software cliente se instala en cada sistema para realizar estas tareas.

Normalmente, instala uno o más módulos Endpoint Security en sistemas cliente, gestiona las detecciones y configura los ajustes que determinan cómo se comportan las funciones del producto.

McAfee ePO

Utiliza McAfee® ePolicy Orchestrator® (McAfee® ePO™) para desplegar y gestionar los módulos de Endpoint Security en sistemas cliente.

Cada módulo incluye una extensión y un paquete de software que se instalan en el servidor de McAfee ePO. A continuación, McAfee ePO despliega el software en los sistemas cliente.

Con **McAfee® Agent**, el software cliente se comunica con McAfee ePO para obtener la configuración e implementación de directivas, actualizaciones de productos y generación de informes

McAfee® Endpoint Security – Como funciona cont.

Módulos de cliente

El software cliente protege los sistemas mediante actualizaciones regulares, supervisión continua y generación de informes detallados.

Envía datos sobre detecciones en sus equipos al servidor McAfee ePO. Estos datos se emplean para generar informes sobre las detecciones y los problemas de seguridad en sus equipos.

Servidor de TIE y Data Exchange Layer

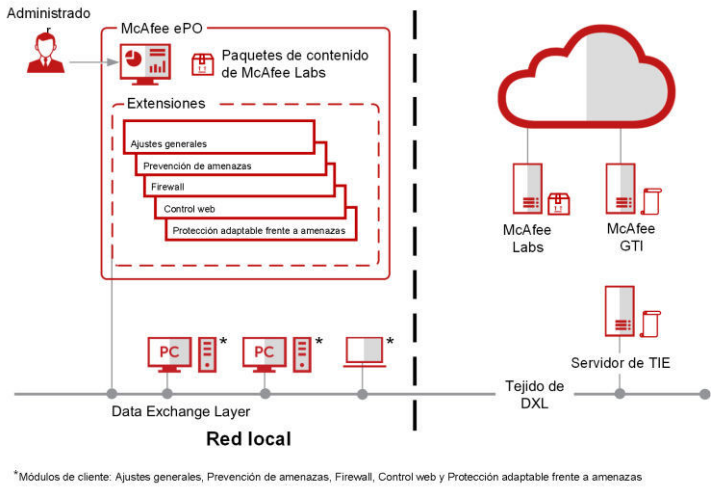
El marco de trabajo de Endpoint Security se integra con McAfee® Threat Intelligence Exchange (TIE) y McAfee® Data Exchange Layer (DXL) cuando utiliza la Protección adaptable frente a amenazas.

Estos productos opcionales le permiten controlar localmente la reputación de archivos y compartir la información inmediatamente en su entorno. Si el servidor de TIE no está disponible, Protección adaptable frente a amenazas consulta a McAfee® Global Threat Intelligence™ (McAfee GTI) la información de reputación.

McAfee GTI

Prevención de amenazas, Firewall, Control web y Protección adaptable frente a amenazas consultan a McAfee GTI la información de reputación para determinar cómo gestionar los archivos en el sistema cliente.

McAfee® Endpoint Security – Como funciona cont.



*Módulos de cliente: Ajustes generales, Prevención de amenazas, Firewall, Control web y Protección adaptable frente a amenazas

McAfee Labs

El software cliente se comunica con McAfee Labs para obtener actualizaciones de motor y archivos de contenido. McAfee Labs publica regularmente paquetes de contenido actualizado.

McAfee® Endpoint Security – Prevención de amenazas

Prevención de amenazas de McAfee® Endpoint Security evita que las amenazas accedan a sistemas, analiza automáticamente los archivos cuando se accede a ellos y ejecuta análisis dirigidos para malware en sistemas cliente.

Prevención de amenazas de Endpoint Security detecta las amenazas basadas en archivos de contenido de seguridad.

Se realizan de forma automática actualizaciones del contenido de seguridad a fin de hacer frente a vulnerabilidades específicas y bloquear la ejecución de las amenazas emergentes.

Prevención de amenazas protege su entorno de lo siguiente:

- Virus, gusanos y troyanos
- Infracciones de los puntos de acceso
- Exploits de desbordamiento del búfer
- Uso no válido de API
- Intrusiones en la red
- Código y programas potencialmente no deseados
- Detección centrada en las vulnerabilidades
- Detección de exploits de día cero

Utilice McAfee ePO para desplegar y gestionar Prevención de amenazas en sistemas cliente.

McAfee® Endpoint Security – Prevención de amenazas Funciones claves

Las características clave de Prevención de amenazas protegen su entorno de amenazas y malware y corrigen problemas limpiando o reparando los archivos infectados.

Protección

Proteja sus sistemas frente a intrusiones antes de que otros accedan a su entorno con estas funciones de Prevención de amenazas.

Protección de acceso:

Proteje los sistemas cliente de cambios no deseados restringiendo el acceso a determinados archivos, datos compartidos y claves y valores de Registro, además de evitar o restringir la ejecución de procesos y servicios que representen una amenaza.

Prevención de exploits:

Prevención de amenazas utiliza firmas en las actualizaciones de contenido para proteger frente a los siguientes exploits:

- Protección contra desbordamiento de búfer: impide la ejecución de código arbitrario debido a desbordamientos del búfer.
- Uso no válido de API: impide que aplicaciones desconocidas o comprometidas que se ejecutan en el sistema realicen llamadas maliciosas a la API.
- Prevención de intrusiones en la red (IPS de red): impide los ataques de denegación de servicio en la red y los relacionados con el ancho de banda que deniegan o reducen el tráfico de la red.
- Reglas expertas: proporcione parámetros adicionales y permita una flexibilidad superior a la de las reglas personalizadas de Protección de acceso. Sin embargo, para crear reglas expertas, debe familiarizarse con la sintaxis específica de McAfee

Arbor

Arbor

Arbor Networks es una empresa de seguridad cibernética que se especializa en soluciones para detectar y mitigar ataques DDoS (denegación de servicio distribuida).

La empresa ofrece una variedad de soluciones de seguridad, incluyendo productos de hardware y software para proteger redes, aplicaciones y datos contra amenazas cibernéticas. Entre las soluciones más populares de Arbor se encuentran:

1. **Arbor DDoS**: una solución de mitigación de ataques DDoS que utiliza inteligencia de amenazas en tiempo real para detectar y bloquear ataques.
2. **Arbor Sightline**: una solución de gestión de tráfico de red que proporciona visibilidad en tiempo real del tráfico de red y ayuda a detectar y solucionar problemas de rendimiento.
3. **Arbor Cloud**: una solución de seguridad en la nube que ofrece protección contra ataques DDoS, así como seguridad de correo electrónico y filtrado de URL.
4. **Arbor SP**: una solución de gestión de servicio que ayuda a los proveedores de servicios a gestionar el tráfico de red, proporcionar seguridad y ofrecer servicios diferenciados.

Arbor también ofrece soluciones para la gestión de seguridad de aplicaciones, la seguridad de servicios financieros y la seguridad para operadores de infraestructura crítica. La empresa tiene presencia en todo el mundo y es conocida por su experiencia en la mitigación de ataques DDoS a gran escala.

Juniper

Sophos

101

Seguridad en Informática - Módulo 6

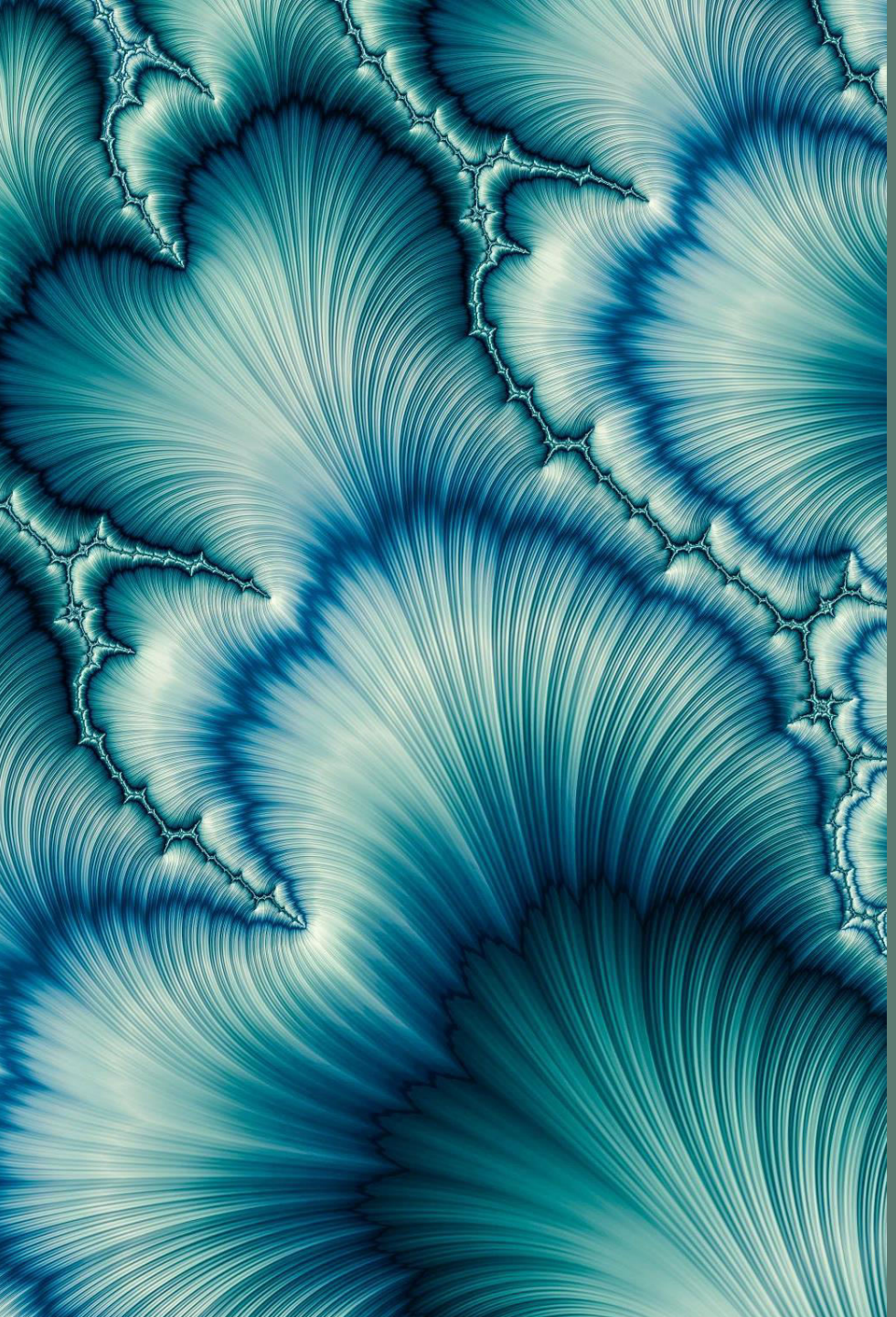
Docente: Carlos Cagnani

*Este documento fue realizado en concepto de capacitación en Formación Profesional y dictada para el **Sindicato CePETel** a contar del mes de mayo del año 2023.*

CLASE 6 Ciberseguridad

Índice de temas

Ciberseguridad



Capítulo 6

Ataques

Aplicaciones Web Ataques

Aplicaciones Web
Tipos de ataques

Los ataques comunes contra las aplicaciones web incluyen:

- Fuerza bruta
- Relleno de credenciales
- Inyección de SQL e inyecciones de formjacking
- Cross-site scripting
- Envenenamiento de cookies
- Ataques del tipo «Man in the middle» (MITM) y del tipo «Man in the browser»
- Divulgación de datos confidenciales
- Ataques de phishing
- Secuestro de sesión

Aplicaciones Web
Tipos de ataques

Ataques de Fuerza Bruta

- Un ataque de fuerza bruta es un método de prueba y error utilizado para decodificar datos confidenciales.
- Las aplicaciones más comunes para los ataques de fuerza bruta son descifrar contraseñas y descifrar claves de cifrado.
- Otros destinos comunes para los ataques de fuerza bruta son las claves API y los inicios de sesión de SSH.
- Los ataques de contraseña de fuerza bruta a menudo se llevan a cabo mediante scripts o bots que tienen como destino la página de inicio de sesión de un sitio web.
- Lo que distingue los ataques de fuerza bruta de otros métodos de decodificación es que los ataques de fuerza bruta no emplean una estrategia intelectual; simplemente intentan usar diferentes combinaciones de caracteres hasta encontrar la combinación correcta.
- Esto se asemeja a un ladrón que intenta abrir una caja fuerte combinada al probar todas las combinaciones posibles de números hasta que se abre la caja fuerte.

Aplicaciones Web
Tipos de ataques

Ataques de Fuerza Bruta

- Las mayores **ventajas** de los ataques de fuerza bruta es que son relativamente simples de realizar, y dado el tiempo suficiente y la falta de una estrategia de mitigación para el destino, siempre funcionan.
- Cada sistema basado en contraseñas y claves de cifrado puede ser descifrado mediante un ataque de fuerza bruta.
- De hecho, la cantidad de tiempo que lleva acceder por fuerza bruta a un sistema es una medida útil para medir el nivel de seguridad de ese sistema.

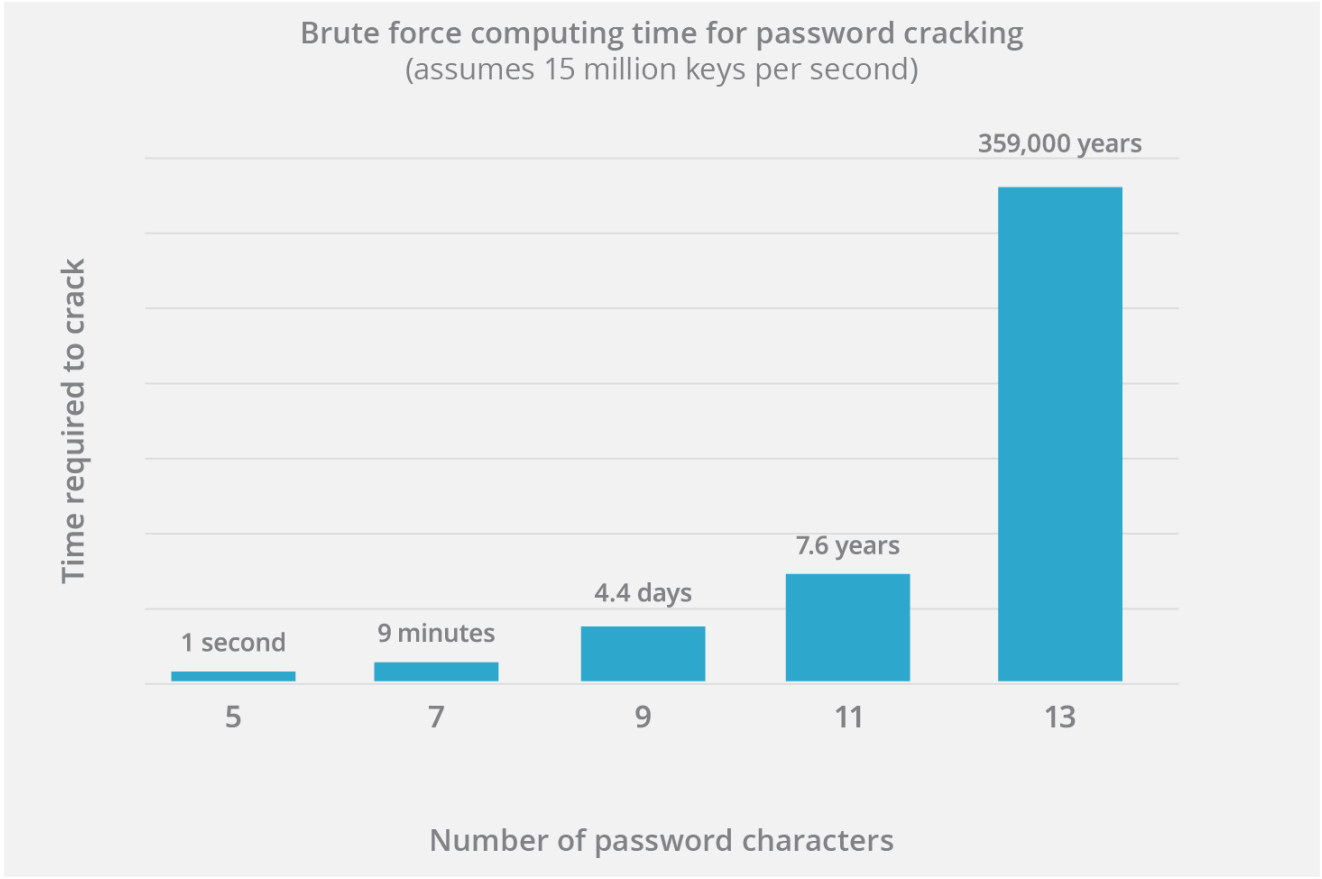
Aplicaciones Web
Tipos de ataques

Ataques de Fuerza Bruta

- Por otro lado, los ataques de fuerza bruta son muy lentos, ya que es probable que deban pasar por cada una de las combinaciones posibles de caracteres antes de lograr su objetivo.
- Esta lentitud se agrava a medida que aumenta el número de caracteres en la cadena de destino (una cadena es solo una combinación de caracteres).
- Por ejemplo, acceder a una contraseña de cuatro caracteres por fuerza bruta toma mucho más tiempo que acceder a una contraseña de tres caracteres, y una contraseña de cinco caracteres toma mucho más tiempo que una contraseña de cuatro caracteres.
- Una vez que el recuento de caracteres supera un cierto punto, acceder por fuerza bruta a una contraseña correctamente aleatorizada se vuelve poco realista.

Aplicaciones Web

Tipos de ataques



Aplicaciones Web
Tipos de ataques

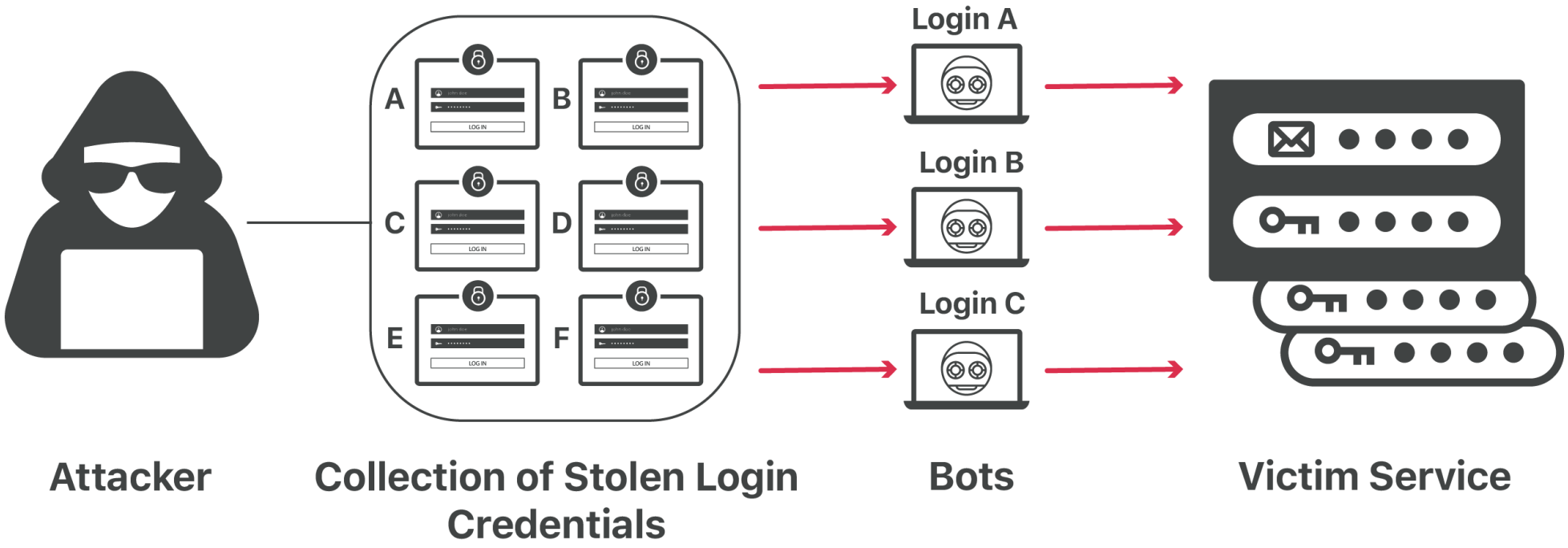
Ataques de Relleno de Credenciales

- Por ejemplo, un atacante puede tomar una lista de nombres de usuario y contraseñas obtenida de una violación de un centro comercial importante, y usar las mismas credenciales de inicio de sesión para intentar iniciar sesión en el sitio de un banco nacional.
- El atacante espera que una fracción de esos clientes del centro comercial también tenga una cuenta en ese banco, y que reutilice los mismos nombres de usuario y contraseñas para ambos servicios.
- Estadísticamente hablando, los ataques de relleno de credenciales tienen una tasa muy baja de éxito.
- Muchas estimaciones sostienen que esta tasa es de, aproximadamente, el 0,1 %, lo que significa que por cada mil cuentas que un atacante intenta descifrar, tendrá éxito apenas una vez.
- El gran volumen de las colecciones de credenciales que intercambian los atacantes hace que valga la pena el relleno de credenciales, a pesar de la baja tasa de éxito.

Aplicaciones Web
Tipos de ataques

Ataques de Relleno de Credenciales

- Por ejemplo, un atacante puede tomar una lista de nombres de usuario y contraseñas obtenida de una violación de un centro comercial importante, y usar las mismas credenciales de inicio de sesión para intentar iniciar sesión en el sitio de un banco nacional.
- El atacante espera que una fracción de esos clientes del centro comercial también tenga una cuenta en ese banco, y que reutilice los mismos nombres de usuario y contraseñas para ambos servicios.
- Estadísticamente hablando, los ataques de relleno de credenciales tienen una tasa muy baja de éxito.
- Muchas estimaciones sostienen que esta tasa es de, aproximadamente, el 0,1 %, lo que significa que por cada mil cuentas que un atacante intenta descifrar, tendrá éxito apenas una vez.
- El gran volumen de las colecciones de credenciales que intercambian los atacantes hace que valga la pena el relleno de credenciales, a pesar de la baja tasa de éxito.



Aplicaciones Web
Tipos de ataques

Ataques de Relleno de Credenciales

Aplicaciones Web
Tipos de ataques

Ataques de Relleno de Credenciales

- OWASP clasifica el relleno de credenciales como un subconjunto de ataques de fuerza bruta.
- Pero, estrictamente hablando, el relleno de credenciales es muy diferente de los ataques de fuerza bruta tradicionales.
- Los ataques de fuerza bruta intentan adivinar las contraseñas sin contexto o pistas, usan caracteres al azar y a veces combinados con sugerencias de contraseñas comunes.
- El relleno de credenciales utiliza datos expuestos, lo que reduce drásticamente el número de posibles respuestas correctas.
- Una buena defensa contra los ataques de fuerza bruta es una contraseña segura que conste de varios caracteres e incluya letras mayúsculas, números y caracteres especiales. Sin embargo, la seguridad de la contraseña no protege contra el relleno de credenciales.
- No importa cuán fuerte sea una contraseña: si se comparte entre diferentes cuentas, el relleno de credenciales puede comprometerla.

Aplicaciones Web
Tipos de ataques

Ataques de Inyección de SQL

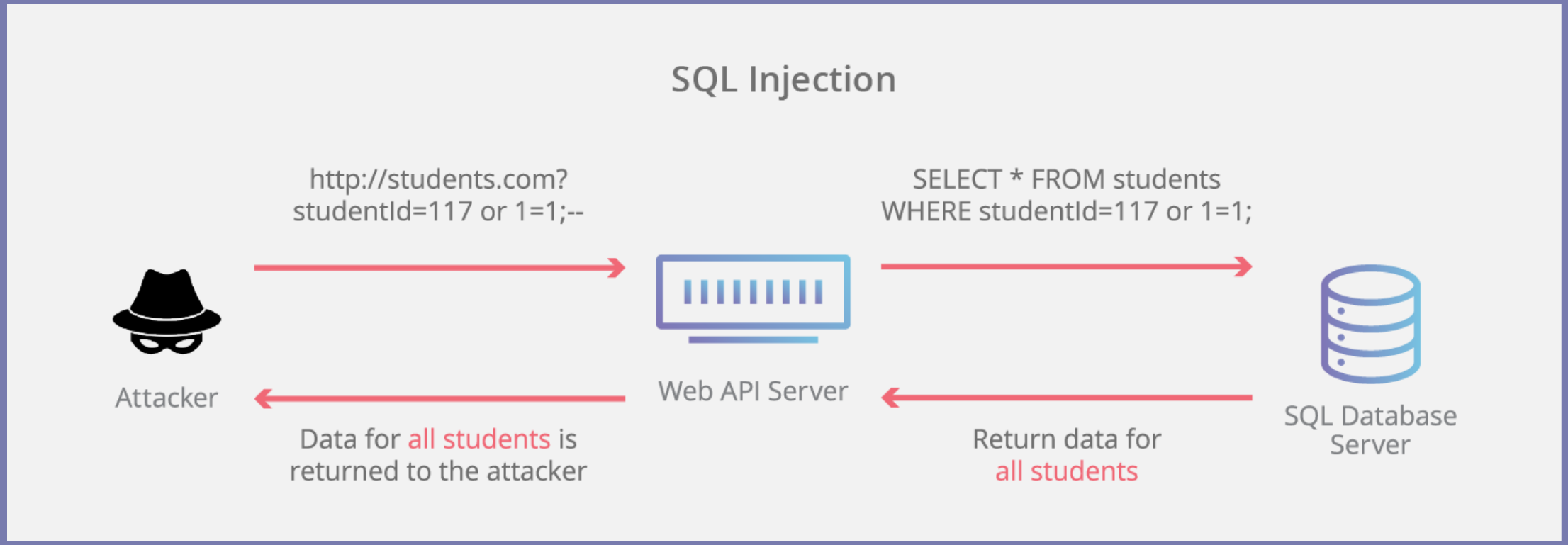
- SQi es un método en el cual un atacante se aprovecha de las vulnerabilidades por el modo en el que una base de datos ejecuta consultas de búsqueda.
- Los atacantes utilizan SQi con el objetivo de conseguir acceso a información no autorizada, modificar o crear nuevos permisos de usuario, o manipular o destruir datos confidenciales.
- Con la ejecución adecuada de comandos SQL, el usuario no autorizado es capaz de suplantar la identidad de un usuario con más privilegios, convertirse a sí mismo o a otros en administradores de la base de datos, manipular los datos existentes, modificar las transacciones y los balances, y recuperar y/o destruir todos los datos del servidor.
- En la informática moderna, la inyección SQL suele producirse a través de Internet mediante el envío de consultas SQL maliciosas a un punto final de la API proporcionado por un sitio web o un servicio (más información al respecto más adelante).
- En su forma más grave, la inyección SQL puede permitir a un atacante obtener acceso de raíz a una máquina, dándole el control total.
- *SQL es un lenguaje de programación utilizado para mantener la mayoría de las bases de datos.

Aplicaciones Web
Tipos de ataques

Ataques de Inyección de SQL

¿Cómo funciona un ataque de inyección SQL?

- Imagina una sala de justicia en la que un hombre llamado Bob está siendo juzgado y está a punto de comparecer ante el juez. Al rellenar el papeleo antes del juicio, Bob escribe su nombre como "***Bob es libre de irse***". Cuando el juez llega a su caso y lee en voz alta "Ahora llamando a Bob es libre de irse", el alguacil deja ir a Bob porque el juez lo ha dicho.
- Aunque hay variedades ligeramente diferentes de SQLi, el núcleo de la vulnerabilidad es esencialmente el mismo:
- Un campo de consulta SQL que se supone que está reservado para un tipo particular de datos, como un número, se pasa en su lugar información inesperada, como un comando.
- El comando, cuando se ejecuta, se escapa más allá de los límites previstos, permitiendo un comportamiento potencialmente nefasto.
- Un campo de consulta se suele rellenar a partir de los datos introducidos en un formulario de una página web.



Aplicaciones Web
Tipos de ataques

Aplicaciones Web
Tipos de ataques

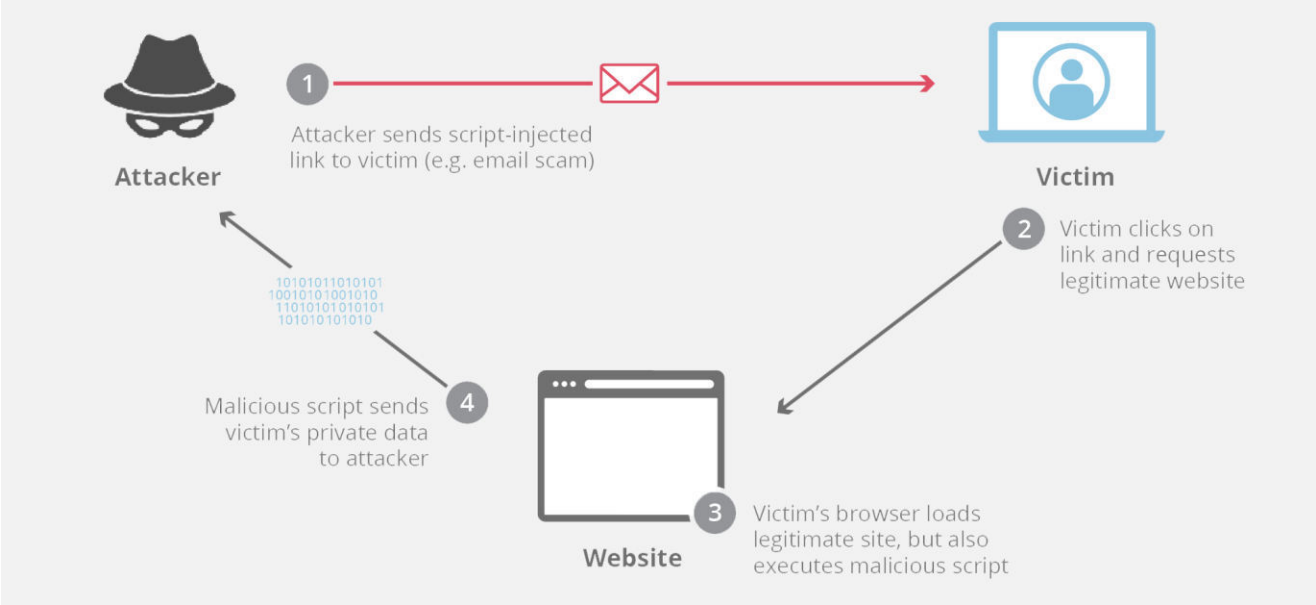
Cross site scripting(XSS)

- XSS es una vulnerabilidad que permite que un atacante inyecte scripts del lado del cliente en una página web con el objetivo de acceder a información importante, hacerse pasar por el usuario o engañar al usuario para que revele información importante.
- El cross-site scripting (XSS) es un exploit en el que el atacante adjunta código en un sitio web legítimo que se ejecutará cuando la víctima cargue el sitio web.
- Ese código malicioso puede insertarse de varias maneras.
- La más popular es añadirlo al final de una url o colocarlo directamente en una página que muestre contenido generado por el usuario.
- En términos más técnicos, el cross-site scripting es un ataque de inyección de código del lado del cliente.

Aplicaciones Web

Tipos de ataques

Cross site scripting(XSS)



Aplicaciones Web
Tipos de ataques

Cross site scripting(XSS)

¿Cómo puede un atacante utilizar el cross-site scripting para causar daño?

- Los ataques de cross-site scripting de JavaScript son populares porque JavaScript tiene acceso a algunos datos sensibles que pueden ser utilizados para el robo de identidad y otros fines maliciosos.
- Por ejemplo, JavaScript tiene acceso a las cookies*, y un atacante podría utilizar un ataque XSS para robar las cookies de un usuario y hacerse pasar por él en línea.
- JavaScript también puede crear peticiones HTTP, que pueden utilizarse para enviar datos (como las cookies robadas) al atacante.
- Además, el JavaScript del lado del cliente también puede ayudar a un atacante a obtener acceso a las API que contienen coordenadas de geolocalización, datos de la cámara web y otra información sensible.

Aplicaciones Web
Tipos de ataques

Cross site scripting(XSS)

¿Cómo puede un atacante utilizar el cross-site scripting para causar daño?

El flujo típico de un ataque de cross-site scripting es el siguiente:

La víctima carga una página web y el código malicioso copia las cookies* del usuario

A continuación, el código envía una solicitud HTTP al servidor web del atacante con las cookies robadas en el cuerpo de la solicitud.

El atacante puede entonces utilizar esas cookies para hacerse pasar por el usuario en ese sitio web con el fin de realizar un ataque de ingeniería social o incluso para acceder a números de cuentas bancarias u otros datos sensibles.

*Las cookies son credenciales de acceso temporales que se guardan en el ordenador del usuario.

Por ejemplo, cuando un usuario entra en un sitio como Facebook, el sitio le da una cookie para que, si cierra la ventana del navegador y vuelve a Facebook más tarde ese mismo día, sea autenticado automáticamente por la cookie y no tenga que volver a iniciar sesión.

Aplicaciones Web
Tipos de ataques

Envenenamiento de cookies

- En informática, una cookie es un dato específico de un sitio web y de una sesión de usuario que incluye información de interés o de identidad del usuario, y que se crea y almacena en el navegador del usuario.
- Los sitios y los servidores web pueden utilizar las cookies para llevar un seguimiento de las tendencias de uso, por ejemplo, qué páginas del sitio reciben más tráfico, así como para personalizar y racionalizar la experiencia del usuario, que puede significar dar prioridad al contenido relacionado con el contenido de las visitas anteriores del usuario, rastrear los artículos de un carrito de compras en línea o rellenar automáticamente la información personal.
- Los atacantes pueden interceptar las cookies antes de que vuelvan al servidor con el fin de extraer información o de modificarlas.
- Las cookies falsas también se pueden crear desde cero como medio para suplantar la identidad de un usuario y acceder a datos adicionales del mismo.
- El envenenamiento de cookies es, por tanto, un término inexacto, ya que con frecuencia se utiliza para referirse no únicamente a las cookies modificadas («envenenadas»), sino también a una variedad de métodos para robar datos de cookies válidas o para hacer otro uso malicioso de las mismas.

Aplicaciones Web
Tipos de ataques

Envenenamiento de cookies

¿Por qué es importante el envenenamiento de cookies?

- Las cookies se utilizan con frecuencia para la autenticación y el seguimiento de manera que se sepa si un usuario ha iniciado la sesión en una cuenta, lo que significa que contienen información que puede utilizarse para el acceso no autorizado.
- También pueden contener otros datos confidenciales, incluyendo información financiera, que previamente ha introducido el usuario.
- El envenenamiento de cookies resulta relativamente sencillo para los atacantes, que pueden utilizar una cookie envenenada para robar las identidades de los usuarios con fines de fraude o para obtener acceso no autorizado al servidor web y llevar a cabo saqueos posteriores.

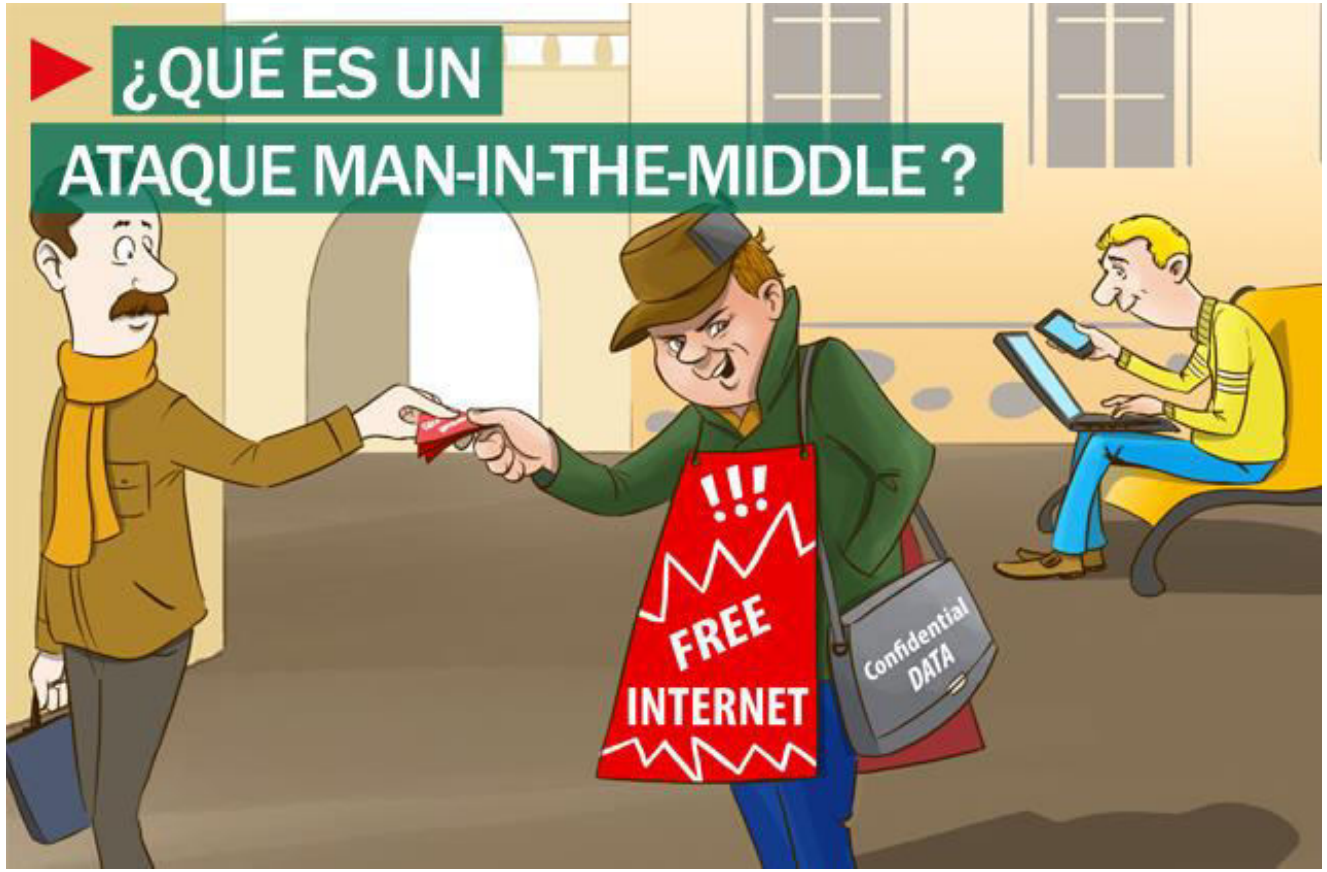
Aplicaciones Web
Tipos de ataques

Ataques del tipo «Man in the middle» (MITM)

- El concepto de un ataque MiTM es muy sencillo. Además, no se limita únicamente al ámbito de la seguridad informática o el mundo online.
- Este método sólo necesita que el atacante se sitúe **entre** las dos partes que intentan comunicarse; interceptando los mensajes enviados e imitando al menos a una de ellas.
- Por ejemplo, en el mundo offline, se crearían facturas falsas, enviándolas al correo de la víctima e interceptando los cheques de pago de dichos recibos.
- En el mundo online, un ataque MiTM es mucho más complejo, pero la idea es la misma. El atacante se sitúa entre el objetivo y la fuente; pasando totalmente desapercibido para poder alcanzar con éxito la meta.

Aplicaciones Web

Tipos de ataques



Aplicaciones Web Tipos de ataques

Ataques del tipo «Man in the middle» (MITM)

Variantes de ataque MiTM

- En el ataque MiTM más habitual, se utiliza un router WiFi para interceptar las comunicaciones del usuario.
- Esto se puede realizar configurando el router malicioso para que parezca legítimo o atacando un error del mismo e interceptando la sesión del usuario.
- En el primero de los casos, el atancante configura su ordenador u otro dispositivo para que actúe como red WiFi, nombrándolo como si fuera una red pública (de un aeropuerto o una cafetería).
- Después, el usuario se conecta al "router" y busca páginas de banca o compras online, capturando el criminal las credenciales de la víctima para usarlas posteriormente.
- En el segundo caso, un delincuente encuentra una vulnerabilidad en la configuración del sistema de cifrado de un WiFi legítimo y la utiliza para interceptar las comunicaciones entre el usuario y el router.
- Éste es el método más complejo de los dos, pero también el más efectivo; ya que el atacante tiene acceso continuo al router durante horas o días. Además, puede husmear en las sesiones de forma silenciosa sin que la víctima sea consciente de nada.
- Una variante más reciente de este tipo de ataque es el ataque man-in-the-browser.
- En este contexto, el ciberdelincuente usa una serie de métodos para insertar un código malicioso en el equipo de la víctima, el cual funciona dentro del navegador.
- Este malware registra, silenciosamente, los datos enviados entre el navegador y las páginas. Estos ataques han ganado en popularidad porque permiten al delincuente atacar a un grupo mayor de víctimas sin la necesidad de estar cerca de éstas.

Aplicaciones Web
Tipos de ataques

Ataques del tipo «Man in the middle» (MITM)

Como defenderse

- Existen diferentes formas efectivas para defendernos de los ataques MiTM, pero la mayoría de ellas usan un router/ servidor y no permiten que el usuario controle la seguridad de la transacción que realiza.
- Este método de defensa usa un sistema de cifrado fuerte entre el cliente y el servidor. En este caso, el servidor se verifica a sí mismo presentando un certificado digital y se establece un canal cifrado entre el cliente y el servidor a través del que se envía la información confidencial.
- Además, los usuarios pueden protegerse de estos ataques evitando conectarse a routers WiFi abiertos o usando plugins de navegador como HTTPS Everywhere o ForceTLS; los cuales establecen una conexión segura siempre que sea posible. Sin embargo, cada una de estos métodos tiene sus límites y existen ejemplos de ataques como SSLStrip o SSLSniff que pueden invalidar la seguridad de las conexiones SSL.

Aplicaciones Web
Tipos de ataques

Divulgación de datos confidenciales

- La divulgación de información permite a un atacante ganar valiosa información sobre un sistema.
- Por consiguiente, siempre considere qué información divulga y si un usuario malintencionado puede utilizarla.
- A continuación se muestra una lista de los posibles ataques de divulgación de información y proporciona métodos paliativos para cada uno de ellos.

Aplicaciones Web
Tipos de ataques

Divulgación de datos confidenciales

Posibles ataques de divulgación de información

Seguridad de mensajes y HTTP

- Si utiliza la seguridad del nivel de mensaje sobre una capa de transporte HTTP, sea consciente de que la seguridad del nivel de mensaje no protege los encabezados HTTP.
- La única manera de proteger los encabezados HTTP consiste en utilizar transporte HTTPS en lugar de HTTP.
- El transporte HTTPS hace que se cifre el mensaje completo, incluidos los encabezados HTTP, mediante el protocolo Secure Sockets Layer (SSL).

Aplicaciones Web
Tipos de ataques

Divulgación de datos confidenciales

Posibles ataques de divulgación de información

Información de directiva

- Es importante proteger la directiva, sobre todo en escenarios de federación donde confidenciales requisitos de tokens emitidos o información sobre el emisor del token se exponen en la directiva.
- En estos casos, la recomendación es proteger el punto de conexión de la directiva del servicio federado para evitar que los atacantes obtengan información sobre el servicio, como el tipo de demandas que colocar en el token emitido o redirigir a los clientes a emisores de tokens malintencionados.
- Por ejemplo, un atacante podría detectar pares de nombre de usuario/contraseña reconfigurando la cadena de confianza federada para finalizar en un emisor que ejecutó un ataque de tipo “man-in-the-middle”.
- También se recomienda que los clientes federados que obtienen sus enlaces a través de la recuperación de directivas comprueben que confían en los emisores en la cadena de confianza federada obtenida.

Aplicaciones Web
Tipos de ataques

Divulgación de datos confidenciales

Posibles ataques de divulgación de información

Los volcados de memoria pueden revelar información de la demanda

Cuando se produce un error en una aplicación, los archivos de registro, como los generados por **Dr. Watson de Windows**, puede contener información de la demanda.

Esta información no se debería exportar a otras entidades, como equipos de compatibilidad; de lo contrario, se exporta también la información de la demanda que contiene los datos privados.

Esto se puede paliar si no se envían los archivos de registro a entidades desconocidas.

Aplicaciones Web
Tipos de ataques

Divulgación de datos confidenciales

Posibles ataques de divulgación de información

Direcciones de extremo

Una dirección de punto de conexión contiene la información necesaria para comunicarse con un punto de conexión.

La seguridad de SOAP(**Simple Object Access Protocol)** debe incluir la dirección completa en los mensajes de negociación de seguridad que se intercambian para negociar una clave simétrica entre un cliente y un servidor.

Dado que la negociación de seguridad es un proceso previo al arranque, los encabezados de dirección no se pueden cifrar durante este proceso.

Por consiguiente, la dirección no debería contener datos confidenciales; de lo contrario, conduce a ataques de divulgación de la información.

Aplicaciones Web
Tipos de ataques

Divulgación de datos confidenciales

Posibles ataques de divulgación de información

Certificados transferidos sin cifrar

Al utilizar un certificado X.509 para autenticar un cliente, el certificado se transfiere de manera abierta, dentro del encabezado SOAP(**Simple Object Access Protocol)**.

Considere esto como una divulgación potencial de la información de identificación personal (PII).

Éste no es un problema para el modo “TransportWithMessageCredential”, , donde se cifra el mensaje completo con seguridad de nivel de transporte.

Aplicaciones Web
Tipos de ataques

Divulgación de datos confidenciales

Posibles ataques de divulgación de información

Referencias del servicio

- Una referencia de servicio es una referencia a otro servicio.
- Por ejemplo, un servicio puede pasar una referencia de servicio a un cliente en el curso de una operación.
- La referencia de servicio también se usa con un comprobador de identidad de confianza , un componente interno que garantiza la identidad de la entidad de seguridad de destino antes de revelar información como datos de aplicación o credenciales al destino.
- Si la identidad de confianza remota no se puede comprobar o es incorrecta, el remitente debería garantizar que no se divulgó ningún dato que se podría poner en peligro a la aplicación o el usuario.

Aplicaciones Web
Tipos de ataques

Divulgación de datos confidenciales

Posibles ataques de divulgación de información

Referencias del servicio

Entre las mitigaciones se encuentran las siguientes:

- *Se supone que las referencias de servicio son de confianza.*
- *Tenga cuidado al transferir instancias de referencias de servicio para asegurarse de que no se han manipulado.*
- *Algunas aplicaciones pueden mostrar una experiencia de usuario que permite el establecimiento interactivo de confianza según los datos de la referencia de servicio y los datos de confianza demostrados por el host remoto.*
- *WCF proporciona puntos de extensibilidad para este tipo de instalación, pero el usuario debe implementarlos.*

Aplicaciones Web
Tipos de ataques

Divulgación de datos confidenciales

Posibles ataques de divulgación de información

NTLM

- De manera predeterminada, en el entorno de dominio de Windows, la autenticación de Windows utiliza el protocolo Kerberos para autenticar y autorizar a los usuarios.
- Si el protocolo Kerberos no se puede utilizar por alguna razón, NT LAN Manager (NTLM) se utiliza a modo de reserva.
- Este comportamiento se puede deshabilitar estableciendo la propiedad AllowNtlm en “false”

Aplicaciones Web
Tipos de ataques

Divulgación de datos confidenciales

Posibles ataques de divulgación de información

NTLM

Entre los problemas que se deben tener en cuenta al permitir NTLM se incluyen:

- NTLM expone el nombre de usuario del cliente.
- Si es necesario mantener el nombre de usuario forma confidencial, establezca la propiedad “AllowNTLM” del enlace en “false”.
- NTLM no proporciona autenticación de servidor.
- Por consiguiente, el cliente no puede asegurar que se esté comunicando con el servicio adecuado al utilizar NTLM como protocolo de autenticación.

Aplicaciones Web
Tipos de ataques

Divulgación de datos confidenciales

Posibles ataques de divulgación de información

Especificar credenciales de cliente o una identidad no válida, fuerza el uso de NTLM

Al crear un cliente, especificar las credenciales del cliente sin un nombre de dominio o especificar una identidad de servidor no válida, hace que NTLM sea utilizado en lugar del protocolo Kerberos (si la propiedad AllowNtlm está establecida en true).

Dado que NTLM no hace la autenticación de servidor, se puede divulgar información de manera potencial.

Aplicaciones Web
Tipos de ataques

Divulgación de datos confidenciales

Posibles ataques de divulgación de información

Especificar credenciales de cliente o una identidad no válida fuerza el uso de NTLM

- Por ejemplo, es posible especificar Windows cliente sin un nombre de dominio, como se muestra en el siguiente código de Visual C#.
- MyChannelFactory.Credentials.Windows.ClientCredential = new System.Net.NetworkCredential("username", "password");
- El código no especifica un nombre de dominio y, por consiguiente, se utilizará NTLM.
- Si se especifica el dominio, pero se especifica un nombre principal de servicio no válido mediante la característica de identidad de punto de conexión, se usará NTLM.

Aplicaciones Web
Tipos de ataques

Ataques de phishing

Sin duda estamos ante un clásico de los ataques cibernéticos.

- El **Phishing** es el proceso en el que un atacante intenta robar datos sensibles, contraseñas, credenciales…
- Busca que los usuarios introduzcan información como nombres de usuario, contraseñas y detalles de tarjetas de crédito haciéndose pasar por una entidad fiable en una comunicación electrónica.
- Sin embargo todo eso que pone la víctima termina en un servidor controlado por los atacantes.
- Cuando hablamos de robo de información, de datos sensibles, debemos recordar siempre el Phishing. Es uno de los métodos más utilizados por los piratas informáticos para recopilar todo tipo de información personal.

Aplicaciones Web
Tipos de ataques
Ataques de phishing

Aplicaciones Web
Tipos de ataques

Web Defacement

Otro ataque que puede comprometer seriamente una página es lo que se conoce como **Web Defacement**.

En español lo podemos traducir como desfiguración de un sitio web.

Es cambiar la apariencia a una página para que parezca lo que no es. Pueden acceder a un servidor y modificar o reemplazar todo el contenido que hay.

Esto podría afectar seriamente a la reputación de un sitio web.

Un atacante podría modificar totalmente la apariencia, los artículos publicados, el contenido…

Lógicamente se trata de un problema muy importante al que hay que hacer frente.

Aplicaciones Web
Tipos de ataques

Desbordamiento de buffer

- Un tipo de ataque más es lo que se conoce como desbordamiento de buffer.
- Se trata de un problema en el que un **proceso almacena datos** en un búfer fuera de la memoria que el programador reservó para ello.
- Es otra variedad de amenaza muy común. Los datos adicionales sobrescriben la memoria que puede contener otros datos, incluidas variables de programa y datos de control de flujo del programa.
- Esto podría provocar errores de acceso a la memoria, resultados incorrectos, finalización del programa o una violación de la seguridad del sistema.
- Hay que tener en cuenta que este tipo de vulnerabilidades puede estar presente en todo tipo de sistemas, aplicaciones y servidores.

Aplicaciones Web
Tipos de ataques

Navegación forzada

En este caso estamos ante un ataque cuyo objetivo es enumerar y acceder a los recursos a los que la aplicación no hace referencia, pero que aún son accesibles.

Podríamos nombrar como ejemplos los directorios como config, backup, logs a los que se puede acceder y que pueden revelar mucha información sobre la aplicación en sí, contraseña, actividades, etc.

Este método también lo debemos incluir como uno de los más utilizados por los piratas informáticos para comprometer la seguridad de servidores. Lo pueden usar para controlar y modificar directorios.

Aplicaciones Web
Tipos de ataques

División de respuesta HTTP

También se conoce como **separación de respuesta HTTP**.

En esta ocasión un atacante pasa datos maliciosos a una aplicación vulnerable, y la aplicación incluye los datos en un encabezado de respuesta HTTP.

Este ataque en sí no causa ningún daño, pero daría lugar a otros ataques sensibles como XSS.

Por tanto, podemos decir que este método es más bien una estrategia para dar lugar a otros ataques.

Es una puerta de entrada a través de una aplicación que tenga algún fallo de seguridad explotable.

Aplicaciones Móviles
Ataques

Aplicaciones Móviles
Tipos de ataques

Las vulnerabilidades en la tecnología móvil

- 1. “Controles débiles del lado del servidor”
- 2. “Alojamiento inseguro de Información”
- 3. “Protección insuficiente en la capa de transporte”
- 4.“Fuga de datos involuntaria”
- 5. “Autenticación y autorización débiles”
- 6.“Criptografía rota/quebrada”
- 7. “Inyección del lado del cliente”
- 8. “Decisiones de seguridad a través de entradas no confiables”
- 9. “Mal manejo de sesiones”
- 10. “Ausencia de protecciones de binarios”

Aplicaciones Móviles
Tipos de ataques

1. “Controles débiles del lado del servidor”

Este tipo de vulnerabilidades afecta directamente al servidor y la seguridad debe depender exclusivamente del mismo.

Las vulnerabilidades que afectan a esta categoría están asociadas a falta de controles y defensas por parte del servidor que espera que los clientes consuman sus servicios a través de parámetros de entrada (inputs de los servicios) que sin las protecciones necesarias puede generar eventos indeseados.

No es necesario que los ataques se efectúen desde un equipo móvil, en algunos casos se puede realizar un ataque desde un navegador Web o scripts sencillos desde una PC común.

Aplicaciones Móviles
Tipos de ataques

2. “Alojamiento inseguro de Información”

Esta vulnerabilidad ocurre cuando información sensible es alojada en el dispositivo móvil con ninguna ó pocas protecciones.

Es común ver que las aplicaciones utilizan archivos, bases de datos livianas, etc. para guardar datos.

Esta información podría ser accedida por malware o usuarios que no deberían tener acceso físico (tener en cuenta que los equipos pueden ser robados).

Es por eso que es necesario proteger dicha información no guardando datos a menos que sea absolutamente necesario y con datos que no sean sensibles.

Como medida extra se puede recurrir al almacenamiento cifrado.

Tampoco hay que confiar en la separación de privilegios del S.O., ya que los equipos pueden ser rooteados o jailbreakeados.

Aplicaciones Móviles
Tipos de ataques

3. “Protección insuficiente en la capa de transporte”

Aquí se presenta el histórico problema en el que las comunicaciones viajan en texto plano y quedan expuestas a cualquiera que pueda observar que ocurre en la red.

Ya sea a través de analizadores de protocolos o cualquier aplicación que pueda ponerse en el medio de la comunicación entre el dispositivo cliente y los servidores a los que se conecta.

La mitigación de esta vulnerabilidad es la que desde la seguridad ofensiva venimos alertando hace años: “Forzar el uso de TLS para las comunicaciones que transaccionan información sensible a través de certificados de confianza”, credenciales, información confidencial, etc.

Aplicaciones Móviles
Tipos de ataques

4.“Fuga de datos involuntaria”

La “Fuga de datos involuntaria” ocurre cuando la aplicación guarda datos sensibles en ubicaciones del dispositivo que pueden ser accedidos por cualquier persona o aplicación.

Esto ocurre generalmente sin el consentimiento o sin el conocimiento de los desarrolladores.

Es muy común dejar funciones activas como “debug=on” en las aplicaciones desarrolladas y que luego estas en producción comiencen a dejar información sensible en logs accesibles del sistema operativo del smartphone, tablet, etc.

La mitigación en este caso pasa por comprender las funciones y particularidades del sistema operativo y los frameworks de desarrollo con los que se trabaja, para evitar funciones por defecto (que desconozcan los desarrolladores) y guarde información en lugares desconocidos.

Aplicaciones Móviles
Tipos de ataques

5. “Autenticación y autorización débiles”

Esta debilidad radica en los mecanismos de autenticación y autorización poco efectivos que permiten a un usuario anónimo ejecutar acciones en nombre de un usuario válido o incluso a un usuario válido ejecutar acciones privilegiadas a nombre de otro.

Las vulnerabilidades asociadas a la autenticación y autorización débiles consisten en saltar las protecciones de login o funciones de aprobación para realizar determinadas acciones.

La manera de mitigar esta vulnerabilidad es asumiendo que los procesos de autorización y autenticación desde el lado del dispositivo cliente son fácilmente “bypasseables” y que se deben reforzar estas medidas desde el lado del servidor.

Aplicaciones Móviles
Tipos de ataques

6.“Criptografía rota/quebrada”

Cuando un atacante o proceso malicioso puede de revertir el proceso de cifrado con el fin de llegar a los datos originales estamos frente a la vulnerabilidad de “Criptografía quebrada”.

Este problema suele aparecer por el uso de algoritmos de cifrado débiles como RC2 o algoritmos de hashing con problemas de seguridad como MD4, MD5, etc.

El uso llaves débiles (generadas sin políticas de contraseñas robustas) también concluye en la posibilidad de romper la criptografía.

Algo poco visto pero que debe de tenerse en cuenta es evitar el uso de algoritmos de cifrados propios, asumiendo que el desconocimiento del proceso de transformación bit a bit fortalece un cifrado. Es bien conocido que la seguridad por oscuridad no es seguridad realmente.

Por último, recordar que Base64 NO es un cifrado, es un algoritmo de encoding reversible.

Aplicaciones Móviles
Tipos de ataques

7. “Inyección del lado del cliente”

Si bien este tipo de vulnerabilidades está dirigido al cliente (dispositivo móvil), los vectores de ataques son varios.

El atacante va a intentar realizar acciones maliciosas contra el cliente y no contra el servidor.

Las formas de atacar el cliente pueden ir desde levantar un servidor Web y esperar a que los clientes se conecten con un navegador Web para intentar hacer descargar y ejecutar una aplicación binaria o generar la ejecución de scripts en JavaScript para que el usuario realice acciones indeseadas.

La respuesta sencilla para mitigar esto es “validar todos los inputs” de la aplicación del dispositivo.

Es una buena práctica desactivar los plugins de JavaScript y proteger las cookies.

Hay aplicaciones que toman variables de servicios (web, etc.) y en base a eso realizan consultas a su propia base de datos. Esto puede aprovecharse para realizar ataques de inyección SQL, así que es importante también validar en la aplicación cliente los datos ingresados (validar inputs).

Aplicaciones Móviles
Tipos de ataques

8. “Decisiones de seguridad a través de entradas no confiables”

Esta vulnerabilidad se presenta cuando la aplicación utiliza datos (que suelen estar ocultos) en la misma para permitir funcionalidades especiales (como niveles de accesos, aprobaciones, etc.)

Un atacante malicioso podría cambiar un valor dentro de la aplicación, comunicación (Web Services) o incluso interferir un proceso (IPC hooking) y alterar el funcionamiento de la aplicación para que la misma realice acciones especiales o le de acceso a estas acciones.

La mitigación de esta vulnerabilidad es controlar los procesos y también tener una lista blanca de aplicaciones conocidas.

Aplicaciones Móviles
Tipos de ataques

9. “Mal manejo de sesiones”

El “Mal manejo de sesiones” ocurre cuando una token de sesión (sobre protocolos como HTTP ó SOAP) se mantiene en el servidor por un periodo de valides muy largo, cuando la generación de la token carece de complejidad (como por ejemplo que la token esté compuesta por el nombre de usuario y la fecha de login) o la longitud es muy corta.

Utilizar las mismas tokens (cookies) previas a la autenticación también está considerado como “Mal manejo de sesiones”.

Para mitigar esta vulnerabilidad es necesario mantener la premisa de seguridad en las sesiones desde el desarrollo, mantenimiento y eliminación de tokens de sesión.

Aplicaciones Móviles
Tipos de ataques

10. “Ausencia de protecciones de binarios”

En un resumen rápido, esta vulnerabilidad radica en la posibilidad de analizar y modificar la aplicación en el dispositivo móvil.

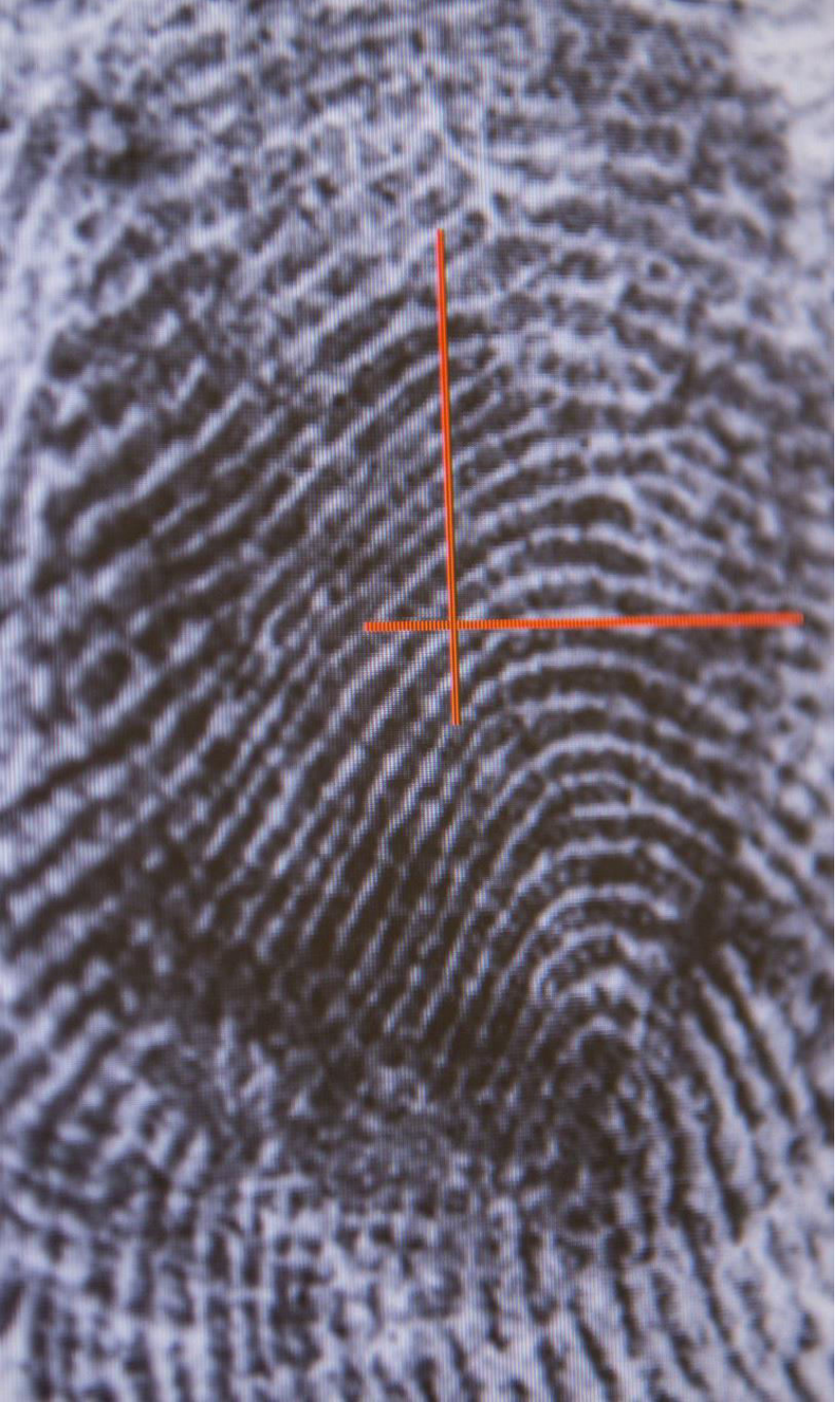
Esto normalmente está ligado a la realización de ingeniería inversa.

Es muy difícil implementar un “único” mecanismo de control final que mitigue por completo esta vulnerabilidad.

Sin embargo es posible minimizar el riesgo a través de varias capas de seguridad por ejemplo:

- Controles de “certificate pinning”.
- Controles de “checksum”.
- Detecciones de debuggers.
- Uso de técnicas de ofuscación de código.
- Detección de jailbreaking o rooting del dispositivo.

REDES
Ataques



Ataques de Red

Tipos

- Ataque DoS o ataque de denegación de servicio
- Ataque de denegación de servicio distribuido – Distributed Denial of Service (DDos)
- ARP Spoofing
- Ataque Man-In-The-Middle
- Ataque Ingeniería Social
- OS Finger Printing
- Escaneo de puertos
- ICMP Tunneling
- Ataque LOKI
- Ataque de secuencia TCP
- Ataques de redireccionamiento ICMP
- Ataque de transferencia de zona DNS

Ataques de Red
Tipos de ataques

Ataque DoS o ataque de denegación de servicio

Un **ataque de denegación de servicio**, tiene como **objetivo inhabilitar el uso de un sistema**, una aplicación, un ordenador o un servidor, con el fin de bloquear el servicio para el que está destinado.

Este ataque puede afectar, tanto a la fuente que ofrece la información, como puede ser una aplicación o el canal de transmisión, como a la red informática, o en otras palabras, el cibercriminal intentará evitar que los usuarios accedan a información o a servicios.

El tipo más común es cuando un atacante «inunda» una red con una gran cantidad de datos, que hace que se sature la red completa.

Por ejemplo, en un ataque DoS hacia una web, cuando escribimos una URL y accedemos, estaremos enviando una solicitud para que nos muestra la información, en este caso, un atacante podría realizar millones de peticiones con el objetivo de colapsar todo el sistema.

Por eso, este ataque toma el nombre de «denegación de servicio», ya que no se puede acceder al sitio en cuestión.

Algunos de los problemas que nos encontraremos si nos hacen un ataque DoS, es que notaremos una enorme bajada en el rendimiento de la red y mucha lentitud (abrir archivos o acceder a sitios web).

Un sitio web en particular es totalmente inaccesible y no está disponible. Seremos incapaces de entrar en cualquier sitio web al que intentemos acceder. Aumento drástico de la cantidad de spam que recibimos

Ataques de Red
Tipos de ataques

Ataque DoS o ataque de denegación de servicio

Tipos de ataques DoS

ICMP Flood Attack

Este tipo de ataque de denegación de servicio permite agotar el ancho de banda de la víctima. Consiste en enviar una gran cantidad de información usando paquetes ICMP Echo Request, es decir, el típico ping, pero modificado para que sea más grande de lo habitual.

Además, la víctima podría responderle con paquetes ICMP Echo Reply (respuesta al ping), por lo que tendremos una sobrecarga adicional, tanto en la red como en la víctima.

Lo más normal es utilizar uno o varios equipos muy potentes para atacar a una misma víctima, de esta forma, la víctima no podrá gestionar correctamente el tráfico generado.

Ataques de Red
Tipos de ataques

Ataque DoS o ataque de denegación de servicio

Tipos de ataques DoS

Ping of the Dead

Este ataque es similar al anterior, consiste en enviar un paquete de más de 65536 bytes, haciendo que el sistema operativo no sepa cómo manejar este paquete tan grande, haciendo que el sistema operativo se bloquee al intentar ensamblarlo nuevamente.

Hoy en día este ataque no funciona, porque el sistema operativo va a descartar los paquetes directamente.

Es muy importante conocer este ataque para evitarlo en el futuro, pero ya os decimos que este ataque ya no funciona porque los sistemas operativos incorporan una gran cantidad de protecciones para evitarlo.

Ataques de Red

Ataque DoS o ataque de denegación de servicio

Tipos de ataques DoS

Tear Drop Attack

Este tipo de ataque consiste en enviar una serie de paquetes muy grandes, con el objetivo de que el destino (la víctima) no sea capaz de ensamblar esos paquetes, saturando el sistema operativo y bloqueándose. Es posible que una vez que el ataque pare, necesite que sea reiniciado para que pueda volver a funcionar correctamente. Hoy en día los kernel de los sistemas operativos incorporan protecciones frente a estos ataques.

Jolt Dos Attack

Este tipo de ataque consiste en fragmentar un paquete ICMP, con el objetivo que la víctima no pueda volver a reensamblarlo. Esto hace que el uso de CPU en la víctima aumente, y tenga cuello de botella importante. El resultado de este ataque suele ser que el PC de la víctima se vuelve muy lenta, debido a que la CPU está muy ocupada intentando reensamblar el paquete.

Ataques de Red

Ataque DoS o ataque de denegación de servicio

Tipos de ataques DoS

Land Attack

Este tipo de ataque consiste en enviar un paquete TCP SYN falso, donde la dirección IP del objetivo se utiliza tanto como origen y destino, con el objetivo de que cuando reciba el paquete, se confunda y no sepa dónde enviar el paquete, y bloquearse.

Este tipo de ataques normalmente es reconocido por los sistemas operativos, firewalls e incluso suites de antivirus.

Ataques de Red

Ataque DoS o ataque de denegación de servicio

Smurf Attack

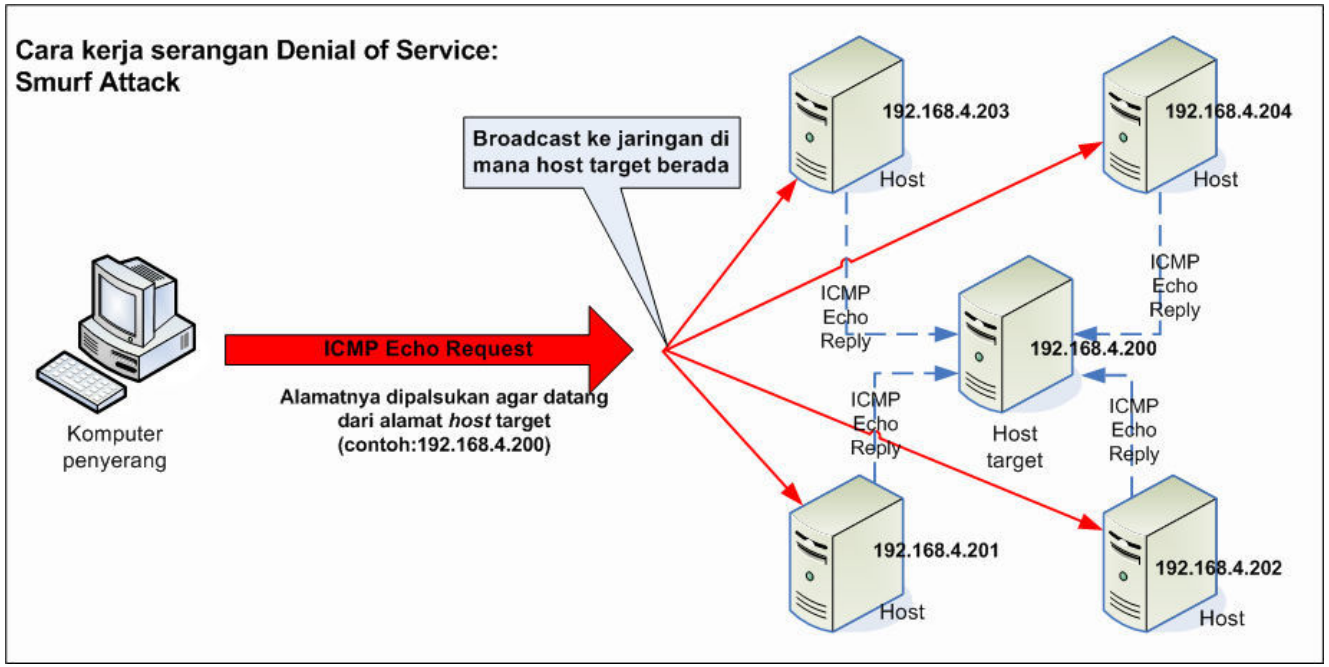
Este ataque consiste en enviar una gran cantidad de mensajes ICMP Echo request a la dirección IP de broadcast con la IP de origen de la víctima.

De esta forma, la víctima real recibirá todas las respuestas ICMP Echo Reply de toda la red, haciendo que se sature.

Antes de realizar este ataque, se debe hacer IP Spoofing para falsificar la dirección IP de origen del ICMP Echo Request, para posteriormente realizar este ataque masivo.

La red dejará de funcionar con normalidad mientras se realiza el ataque, porque tendremos un alto tráfico de broadcast.

Hoy en día los switches están preparados para evitar estos ataques automáticamente, en función de los PPS (Paquetes por segundo)., estas solicitudes t



Ataques de Red

Ataque DoS o ataque de denegación de servicio

Smurf Attack

Ataques de Red

Ataque DoS o ataque de denegación de servicio

Tipos de ataques DoS

SYN Flood

Este tipo de ataque es uno de los más utilizados en todo el mundo, consiste en enviar paquetes TCP con el flag SYN activado, con el objetivo de enviar cientos o miles de paquetes a un servidor y abrirle diferentes conexiones, con el objetivo de saturarle por completo. Normalmente se utiliza este ataque con una IP de origen falsa, para que todas las respuestas vayan a una IP que no existe, o a una IP víctima que también se verá saturado por todas las respuestas TCP que se envían del servidor.

Los ataques SYN Flood se pueden evitar fácilmente con el firewall, limitando el número de paquetes TCP SYN que se pueden recibir, e incluso poniendo un proxy intermedio para añadir una verificación adicional, antes de pasarle los mensajes al servidor web o cualquier otro servicio que haga uso del protocolo TCP.

Fraggle Dos Attack

Este ataque consiste en enviar mucho tráfico UDP a una dirección IP de broadcast, estos paquetes tienen la IP de origen de la víctima, lógicamente se ha realizado un IP Spoofing para realizar este ataque. La red entregará el tráfico de red a todos los hosts, porque estamos enviando paquetes UDP a la dirección de broadcast, y los equipos responderán. Esto ocasionará que la víctima reciba una gran cantidad de tráfico que no sea capaz de gestionar de manera adecuada, y será incapaz de trabajar con normalidad

Ataques de Red

Ataque de denegación de servicio distribuido – Distributed Denial of Service (DDos)

Este ataque de red consiste en colapsar a una víctima desde múltiples equipos de origen, por ejemplo, una botnet formada por mil ordenadores podrían atacar a un determinado objetivo.

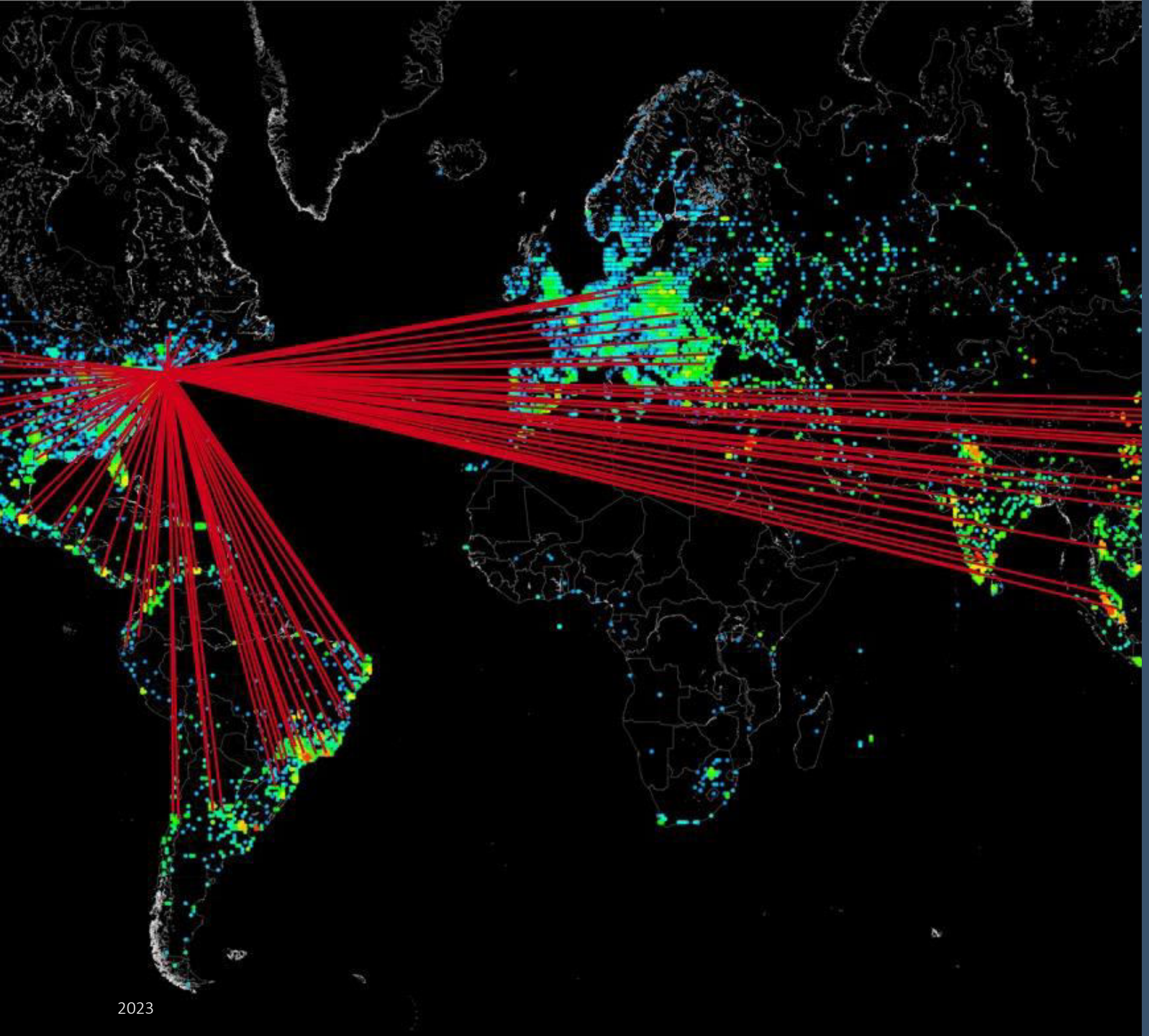
Este tipo de ataques son muy habituales, haciendo uso de las técnicas que os hemos explicado anteriormente, como el SYN Flood.

Aunque haya un servidor muy potente capaz de gestionar millones de solicitudes SYN Flood, si hacemos uso de una botnet con cientos o miles de ordenadores, no podrá aguantarlo y se terminará bloqueando.

Este ataque de «distribuye» entre diferentes equipos, ya sean ordenadores, otros servidores infectados, dispositivos IoT hackeados y mucho más.

Ataques de Red

Ataque denegación de servicio distribuido – DDos



Ataques de Red

Ataque denegación de servicio distribuido – Ddos

El ataque DDoS más grande registrado que afectó a sitios como Twitter, Spotify, Netflix, GitHub y Amazon (Octubre 2016)

2023

Ataques de Red

Ataque de denegación de servicio distribuido – Distributed Denial of Service (DDos)

- https://www.digitalattackmap.com/
- https://cybermap.kaspersky.com/es
- https://www.fireeye.com/cyber-map/threat-map.html
- https://threatmap.fortiguard.com/
- https://www.spamhaustech.com/threat-map/
- https://threatbutt.com/map/
- https://threatmap.bitdefender.com/
- https://map.lookingglasscyber.com/
- https://talosintelligence.com/fullpage_maps/pulse
- https://horizon.netscout.com/

Ataques de Red

DoS y DDoS Diferencias

DDoS y DoS son los ataques más utilizados para desestabilizar sistemas informáticos.

DDOS: el ataque consiste en **sobrecargar un servidor** desde diferentes IPs con una cantidad de peticiones muy superior a las que el servidor puede gestionar.

DoS: En un **ataque DoS** el que realiza todas las peticiones es un **único** ordenador con una cantidad de peticiones muy superior a las que el servidor puede gestionar.

De esta forma, los ataques DDoS y los ataques DoS producen una alteración del servicio; ya sea ralentizando la página o, directamente, haciendo que se caiga.

Ataques de Red

DoS y DDoS Diferencias

Ataques de Red

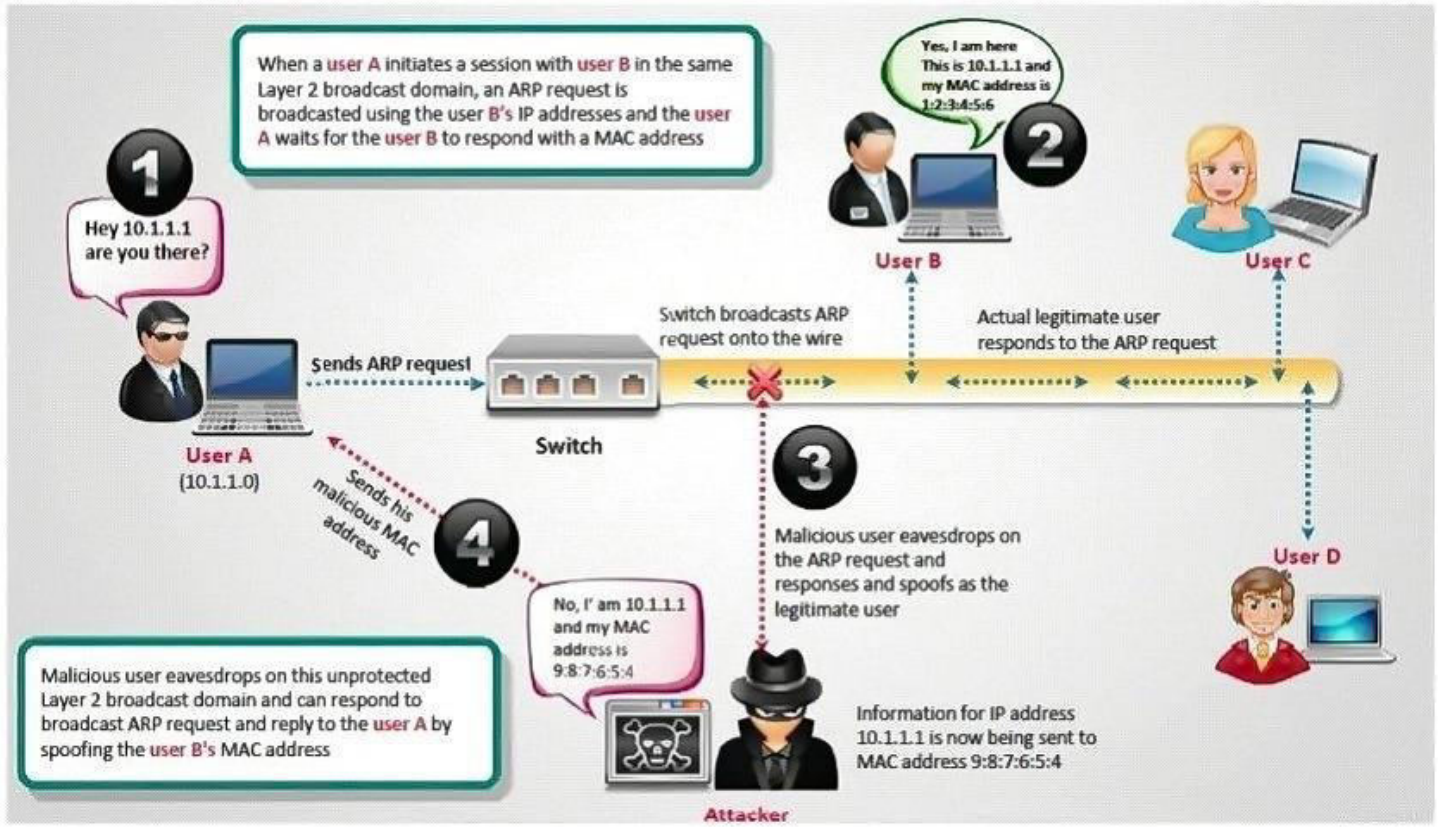
ARP Spoofing

Este ataque a las redes de datos es uno de los más populares, permite atacar a equipos que estén en la misma red local, ya sea cableada o inalámbrica.

Cuando se realiza un ataque ARP Spoofing, lo que estamos haciendo es que el atacante se pueda hacer pasar por el router o gateway, y que todo el tráfico de la red o desde un determinado PC (víctima) pase por él, permitiendo leer, modificar e incluso bloquear el tráfico de red.

Ataques de Red

ARP Spoofing



Ataques de Red

ARP Spoofing

Este ataque solamente funciona en redes IPv4, pero en redes IPv6 también existe un ataque similar, porque el protocolo ARP tan solo está disponible en redes IPv4.

Este ataque es lo más fácil para poder realizar un Man in the Middle y capturar toda la información a la víctima.

Para detectar estos ataques, se podría usar Reverse ARP, un protocolo que sirve para consultar las IP asociadas a una MAC, si tenemos más de una IP significa que estamos ante un ataque.

Algunas suites de seguridad ya detectan este tipo de ataques, e incluso los switches gestionables permiten evitar este tipo de ataques haciendo IP-MAC Binding.

Ataques de Red

Ataque de inundación MAC

Este es uno de los ataques más típicos en las redes de datos, consiste en inundar de direcciones MAC una red donde tengamos un switch, cada uno con diferentes direcciones MAC de origen, con el objetivo de llenar la tabla CAM de los switches y que el switch pase a funcionar como un hub.

No obstante, hoy en día todos los switches disponen de protecciones frente a este ataque, haciendo que se puedan eliminar las direcciones MAC rápidamente, y que no llegue a colapsarse nunca, pero la CPU del switch estará al 100% y notaremos lentitud en la red.

Ataques de Red

Ataque de inundación MAC

En el caso de switches gestionables con VLANs, el desbordamiento solamente estaría en la VLAN afectada, no afectando al resto de VLANs de la red.

Para prevenir este tipo de ataques, es recomendable configurar el Port Security en los switches, y limitar a un cierto número de direcciones MAC por puerto, de esta forma, el puerto se podría apagar automáticamente, o directamente restringir el alta de nuevas MAC hasta nueva orden.

Ataques de Red

Envenenamiento de caché DNS

Este tipo de ataque consiste en proporcionar datos falsos vía DNS; para que una víctima obtenga esa información y visite páginas web falsas o bajo nuestro control.

El equipo que haga solicitudes DNS podría recibir direcciones IP falsificadas en base a su solicitud DNS, de esta forma podremos redirigir a una víctima hacia cualquier web bajo nuestro control.

Ataques de Red

IP Spoofing

Este ataque consiste en suplantar la dirección IP de origen de un determinado equipo, de esta forma, se podrían enviar paquetes TCP, UDP o IP con una IP de origen falsa, suplantando la dirección IP real de un dispositivo.

Esto tiene varios objetivos, ocultar la identidad real del origen, o hacerse pasar por otro equipo para que todas las respuestas vayan a él directamente.

Ataques de Red

ACK Flood

Este ataque consiste en enviar un paquete de tipo TCP ACK a un determinado objetivo, normalmente se realiza con una IP falsificada, por tanto, el IP spoofing será necesario.

Es similar a ataques TCP SYN, pero si el firewall está bloqueando paquetes TCP SYN, esta es una alternativa para bloquear a la víctima.

Ataques de Red

TCP Session Hijacking

Este ataque consiste en tomar posesión de una sesión TCP que ya existe, donde la víctima la está utilizando.

Para que este ataque tenga éxito es necesario realizarse en un momento exacto, en el inicio de las conexiones TCP es donde se realiza la autenticación, es justo en ese punto cuando el cibercriminal ejecutará el ataque.

Ataques de Red

Ataque Man-In-The-Middle

Los ataques Man in the Middle es un tipo de ataque que permite posteriormente realizar otros.

Los ataques MITM consisten en colocarse entre la comunicación de dos o más equipos por el atacante, con el objetivo de leer, modificar al vuelo e incluso denegar el paso del tráfico desde un origen hacia un destino.

Este tipo de ataques permiten conocer toda la navegación en línea y cualquier comunicación que se vaya a realizar, además, se podría dirigir toda la información hacia otro equipo existente.

Un ejemplo de ataque MITM, sería cuando un cibercriminal intercepta una comunicación entre dos personas, o entre nosotros y un servidor web, y el cibercriminal puede interceptar y capturar toda la información sensible que nosotros enviamos al sitio.

Ataques de Red

Ataque Man-In-The-Middle

¿Cómo prevenir ataques Man-In-The-Middle?

Los ataques MITM no son imposibles de evitar, gracias a la tecnología de «Infraestructura de Clave Pública» podremos proteger los diferentes equipos de ataques, y es que esto nos permitiría autenticarnos frente a otros usuarios de forma segura, acreditando nuestra identidad y comprobando la identidad del destinatario con criptografía pública, además, podremos firmar digitalmente la información, garantizar la propiedad de no repudio, e incluso enviar información totalmente cifrada para conservar la confidencialidad.

Ataques de Red

Ataque Man-In-The-Middle

¿Cómo prevenir ataques Man-In-The-Middle?

En una operación criptográfica que use Infraestructura de Clave Pública, intervienen conceptualmente como mínimo las siguientes partes:

- Un usuario iniciador de la operación.
- Unos sistemas servidores que dan fe de la operación, y garantizan la validez de los certificados, la Autoridad de Certificación (CA), Autoridad de Registro y Sistema de Sellado de Tiempo.
- Un destinatario de los datos cifrados que están firmados, garantizados por parte del usuario iniciador de la operación.

Las operaciones criptográficas de clave pública, son procesos en los que se utilizan unos algoritmos de cifrado asimétrico que son conocidos y están accesibles para todos, como RSA o basados en curvas elípticas. Por este motivo, la seguridad que puede aportar la tecnología PKI, está fuertemente ligada a la privacidad de la llamada clave privada.

Ataques de Red

Ataques de ingeniería social

Aunque los ataques de ingeniería social no son un ataque a las redes de datos, es un tipo de ataque muy popular y utilizado por los cibercriminales.

Este tipo de ataques consisten en manipular a una persona para que proporcione credenciales de usuario, información privada y más.

Los cibercriminales siempre buscan todas las formas posibles para hacerse con credenciales de usuario, número de tarjetas de crédito, cuentas bancarias etc, para conseguir esto, intentarán mentir a las víctimas haciéndose pasar por otras personas.

Ataques de Red

Ataques de ingeniería social

Este tipo de ataques tienen mucho éxito porque se ataca al eslabón más débil de la ciberseguridad: el ser humano.

Es más fácil intentar conseguir las credenciales de usuario de una persona a través de ingeniería social, que intentar atacar un servicio como Google para extraer las contraseñas.

Es fundamental en quién confiar, cuándo hacerlo y también cuándo no debemos hacerlo.

No importa lo segura que sea nuestra red, si confiamos nuestra seguridad a quién no debemos, toda esa seguridad no valdrá de nada.

Ataques de Red

Ataques de ingeniería social

¿Cómo prevenir ataques de ingeniería social?

La primera recomendación es no tener prisa por responder a los ciberatacantes, muchos de estos ataques siempre se transmiten con cierta urgencia, por ejemplo, que es necesario urgentemente realizar una transferencia de dinero a un destinatario que nunca antes habíamos tenido.

Es necesario que sospeches de cualquier mensaje extraño o no solicitado, si el correo que nos llega es de un sitio web o empresa que solemos utilizar, debemos emprender una pequeña investigación por nuestra parte, que recaiga incluso en ponernos en contacto con dicha compañía para verificar la información.

Ataques de Red

Ataques de ingeniería social

¿Cómo prevenir ataques de ingeniería social?

- Cuidado con las solicitudes de información bancaria
- No proporcionar nunca contraseñas de acceso, ni siquiera a entidades bancarias.
- Rechazar cualquier tipo de ayuda de terceras personas, es posible que sean cibercriminales para robar información o dinero.
- No pinchar en enlaces por email, podrían ser phishing, evitar descargar cualquier documento sospechoso.
- Establecer filtros anti spam, configurar nuestro equipo con antivirus y firewalls, revisar los filtros de email y mantener todo actualizado.

Ataques de Red

OS Finger Printing

El término OS Finger Printing se refiere a cualquier método para determinar el sistema operativo utilizado en la víctima, con el objetivo de vulnerarlo.

Normalmente este tipo de ataques se realizan en la fase de pentesting, este reconocimiento del sistema operativo se realiza al analizar indicadores de protocolos, tiempo que tarda en responder a una solicitud en concreto, y otros valores.

Nmap es uno de los programas más utilizados a la hora de realizar el OS Finger Printing.

¿Para qué le servirá a un atacante saber el sistema operativo de la víctima?

Para realizar ataques más dirigidos a ese sistema operativo, conocer las vulnerabilidades y explotarlas, y mucho más.

Ataques de Red

OS Finger Printing

Existen dos tipos diferentes de OS Finger Printing:

- **Activo**: se consigue enviando paquetes especialmente modificados y creados para el equipo objetivo, y mirando en detalle la respuesta y analizando la información recopilada.
  - Nmap realiza este tipo de ataques para obtener toda la información posible.
- **Pasivo**: en este caso se analiza la información recibida, sin enviar paquetes específicamente diseñados al equipo objetivo.

Ataques de Red

Escaneo de puertos

En cualquier pentesting, el escaneo de puertos es lo primero que se realiza para intentar vulnerar a un objetivo.

Es una de las técnicas de reconocimiento más utilizada por los cibercriminales para descubrir servicios expuestos con los puertos abiertos, si se está usando un firewall e incluso qué sistema operativo está usando la víctima.

Todos los equipos que están conectados en la red local o en Internet, hacen uso de una gran cantidad de servicios que escuchan en determinados puertos TCP y UDP.

Estos escaneos de puertos permiten saber cuáles están abiertos, e incluso qué servicio hay detrás de ellos, con el objetivo de explotar una vulnerabilidad a dicho servicio.

Ataques de Red

Escaneo de puertos

En los escaneos de puertos, enviaremos mensajes a cada puerto, uno por uno, dependiendo del tipo de respuesta recibida, el puerto estará abierto, filtrado o cerrado.

Uno de los programas más usados para escaneo de puertos es Nmap, es la navaja suiza del escaneo de puertos porque también disponemos de Nmap NSE que permite usar scripts para explotar vulnerabilidades conocidas, o para atacar a servidores Samba, FTP, SSH etc.

Conoce los puertos que tenemos abiertos es también algo muy importante, porque un puerto identifica a un servicio que hay corriendo en el sistema. Por ejemplo, el protocolo FTP usa el puerto 21, si está abierto podría deberse a que tenemos un servidor FTP escuchando, y podríamos atacarlo.

El escaneo de puertos es la primera fase de un pentesting.

Ataques de Red

Escaneo de puertos

¿Cómo prevenir el escaneo de puertos?

El escaneo de puertos no podemos evitarlo, porque no podemos evitar que un ciberdelincuente o cibercriminal intente ver qué puertos tenemos abiertos, pero lo que sí está en nuestra mano es proteger todos los puertos con un firewall bien configurado de forma restrictiva.

Debemos tener en cuenta que realizar un escaneo de puertos es ilegal, según se han declarado en varios juzgados, porque es el primer paso de la intrusión o para explotar una vulnerabilidad.

Ataques de Red

Escaneo de puertos

¿Cómo prevenir el escaneo de puertos?

Para limitar la información que vamos a proporcionar a un atacante en un escaneo de puertos, debemos hacer lo siguiente:

- Cerrar todos los puertos en el firewall, excepto los que tengan que estar abiertos para el buen funcionamiento del sistema.
- Utilizar una política del firewall restrictiva, solamente se abre lo que se vaya a utilizar.
- Cerrar servicios del sistema operativo que no sean necesarios.
- Configurar los servicios web, SSH, FTP de tal forma que nos proporcionen información como el número de versión, para evitar la explotación de posibles vulnerabilidades.
- Usar TCP Wrappers, un encapsulador de TCP que darán al administrador mayor flexibilidad para permitir o denegar el acceso a determinados servicios.
- Hacer uso de programas como fail2ban para bloquear direcciones IP que realicen ataques.
- Usar IDS/IPS como Snort o Suricata, para que bloqueen las IPs de los atacantes.

Ataques de Red

Escaneo de puertos

ICMP Tunneling

Este tipo de ataques se utiliza principalmente para evadir los firewalls, porque normalmente los cortafuegos no bloquean los paquetes ICMP.

También podrían usarse para establecer un canal de comunicación cifrado y difícil de rastrear.

Un túnel ICMP lo que hace es establecer una conexión encubierta entre dos equipos, esto mismo también se puede usar con UDP haciendo uso de DNS.

Para prevenir los túneles ICMP, es necesario inspeccionar el tráfico ICMP en detalle, y ver qué tipo de mensajes se intercambian.

Además, esto se complica si se utiliza cifrado de datos, pero podremos detectarlo porque será tráfico ICMP que no es «normal», por tanto, saltarán todas las alertas de los IDS/IPS si los configuramos correctamente.

Ataques de Red

Ataque LOKI

Esto no es un ataque a las redes de datos, es un programa cliente/servidor que permite exfiltrar información a través de protocolos que normalmente no contienen carga útil, por ejemplo, se podría tunelizar tráfico SSH dentro del protocolo ICMP con ping e incluso con UDP para DNS.

Esto se puede utilizar como puerta trasera en sistemas Linux para extraer información y enviarla remotamente sin levantar sospechas.

Esto es algo que también deberíamos controlar a través de los firewalls.

Ataques de Red

Ataque de secuencia TCP

Este tipo de ataque consiste en intentar predecir el número de secuencia de un tráfico TCP, con el objetivo de identificar los paquetes de una conexión TCP, y secuestrar la sesión.

El típico ejemplo es un escenario donde un atacante está monitorizando el flujo de datos entre dos equipos, el atacante podría cortar la comunicación con el equipo real, y establecerse él como el equipo real, todo ello prediciendo el número de secuencia del siguiente paquete de TCP.

El atacante «eliminaría» al equipo real, haciendo uso de un ataque de denegación de servicio (DoS) o similar.

Gracias a esta predicción del número de secuencia, el paquete podrá llegar a su destino antes que cualquier información del host legítimo, porque este último está bajo un ataque DoS y no permitirá la comunicación al host víctima.

Este paquete del atacante se podría usar para obtener acceso al sistema, terminar una conexión por la fuerza, o directamente enviar una carga maliciosa.

Ataques de Red

Ataque de secuencia TCP

¿Cómo prevenir el ataque de secuencia TCP?

La IETF en 2012 lanzó un nuevo estándar para establecer un algoritmo mejorado, y evitar que un atacante pueda adivinar el número de secuencia inicial en las comunicaciones TCP.

Este estándar está diseñado para aumentar la robustez de las comunicaciones TCP frente al análisis predictivo y monitorización de los atacantes.

Actualmente todos los sistemas operativos hacen uso de este nuevo estándar para evitar este ataque, por tanto, un atacante no podrá predecir los números de secuencia, pero los atacantes en ciertas circunstancias todavía puedan adivinarlos, aunque es mucho más difícil que antes.

Ataques de Red

Ataques de redireccionamiento ICMP

Este ataque de red llamado ICMP Redirect, permite redirigir a un host de origen que use otra puerta de enlace diferente para que pueda estar más cerca del destino.

Lógicamente, un atacante se pondrá a sí mismo como puerta de enlace, con el objetivo de que todo el tráfico pase por él para capturarlo, modificarlo o bloquearlo.

Estos mensajes se envían a los diferentes hosts, pero hoy en día este tipo de ataques ICMP Redirect en sistemas Linux no están afectados, porque internamente lo tienen desactivado, pero es posible que en otros sistemas operativo sí se vean afectados.

Ataques de Red

Ataque de transferencia de zona DNS

Este ataque afecta a los servidores DNS, consiste en que el servidor DNS devuelve una lista de nombre de host y direcciones IP en el dominio, estas transferencias de zona normalmente se realizan entre servidores DNS autoritativos, pero este ataque podría hacer que los ciberdelincuentes consulten los servidores DNS para tener un listado de host a los que atacar.

Seguridad en Informática - Módulo 7

Docente: Carlos Cagnani

Este documento fue realizado en concepto de capacitación en Formación Profesional y dictada para el ***Sindicato CePETel*** *a contar del mes de mayo del año 2023.*

Temas

- SIEM
- SOC
- NOC
- Analisis Forense

SIEM
Security Information Event Management

La evolución de los sistemas SIEM frente a la correlación de eventos de seguridad de la información

SIEM

Evolución de los sistemas frente a la correlación de eventos

RESUMEN

- Diferenciar las tecnologías SIM contra SEM.
- Encontrar un punto en común entre correlación de eventos de seguridad y SIEM.
- Conocer los beneficios en términos de negocios que habilitan esas tecnologías.
- Pensar en el futuro próximo de SIEM y su influencia en la inseguridad de la computación en la nube.
- Ver un resumen de implementaciones internacionales según Gartner.
- Ver la arquitectura de estas soluciones en nuestras redes…

SIEM

Problemática de Infraestructura:

- Crecientes amenazas PERSISTENTES Y CAMBIANTES internas contra los recursos de TI como: BD, servidores de correos, servidores web…
- No es fácil detectar donde esta el problema de la red que nos llevo al caos con los sistemas críticos del negocio!

SIEM

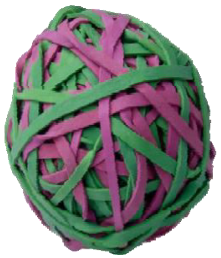
Problemática de Infraestructura:

- No hay suficientes tableros de control
- Poca o ninguna Visibilidad de toda la infraestructura
- No hay suficiente evidencia para sustentar un incidente en IT
- Difícil gerenciamiento de incidentes
- No es fácil buscar y descubrir evidencias

SIEM

Problemática de Inseguridad:

- Debemos ajustar políticas de seguridad cuando crece el riesgo basado en evidencias/incidentes que no anticipe
- Hay Malware en mi infraestructura que se aprovecha de las vulnerabilidades y generan: DDoS, DoS (Denegacion de servicios)
- IPS/IDS generan muchos falsos positivos



SIEM

Problemática de cumplimiento:

- No tengo suficientes registros para cumplir las auditoría de red internas y externas
- No tengo la materia prima para sustentar los Análisis forenses cuando se dan los incidentes
- Cuando se da un incidente no se donde conseguir toda la evidencia en forma correlacionada

SIEM

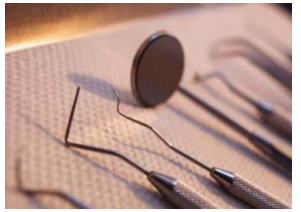
Problemática de cumplimiento de normas

Regulaciones: Health Insurance Portability Accountability Act (HIPAA), Gramm-Leach-Bliley Act (GLBA), Sarbanes-Oxley (SOX), y Payment Card Industry Data Security Standards (PCI),

EVOLUCION DE LOS SISTEMAS SIEM

Security Information Management (SIM)

- Nos ayuda con la centralización y Administración de logs
- Reportes de logs (análisis)
- Reportes de cumplimiento
- Conclusión: Esto es monitorización tradicional necesario en infraestructura
- NO es seguridad de la información



Security Event Management (SEM)

- Monitorización en tiempo real de eventos.
- Captura eventos de seguridad en dispositivos de red.
- Captura eventos de aplicaciones*.
- Correlación de eventos.

Security Event Management(SEM)

- Respuesta a incidentes
- Visibilidad de los sistemas de seguridad (FW, IDS, IPS, DLP, EndPoint security…)

Security Information Event Management (SIEM)

- SIM + SEM (…que ya los vimos) +
- Disminuir los falsos positivos (*)
- Detección de anomalías de red y amenazas
- Análisis antes, durante y después del ataque
- Captura total de los paquetes en la red
- Comportamiento del usuario y su contexto
- Cumplimiento de nuevas normas/leyes

Security Information Event Management (SIEM)

… + Administración del riesgo:

- Topología de red y vulnerabilidades
- Configuración errada de dispositivos
- Análisis de fallas y simulación de exploits
- Priorización de vulnerabilidades

Security Information Event Management (SIEM)

- Correlación avanzada y profunda de eventos
- Interface para obtener logs de:

  CRM (Customer Relationship Management), ERP (Enterprise Resource Planning), sistemas de Marketing, etc
- Conclusión: Plataforma de inteligencia de la seguridad

Security Information Event Management (SIEM)

¿Cuál es la evolución de los SIEM?

- Uso de SIEM como un Data Warehouse
- Recibir información respecto de la posición de una empresa en el mercado
- Recibir ventajas competitivas de su mercado
- Dan la habilidad de acceder a varios tipos de datos y metadatos para específicos atributos relevantes para tomar decisiones de negocios

Security Information Event Management (SIEM)

…evolución de los SIEM?

- Fuentes externas:
- Security and Exchange Commission (SEC): Reportes de informes financieros y forecast
- Electronic Data Gatering Analisys and Retrieval (EDGAR): Automatiza los colectores, validación, indexamiento, competidores, proveedores y distribuidores.

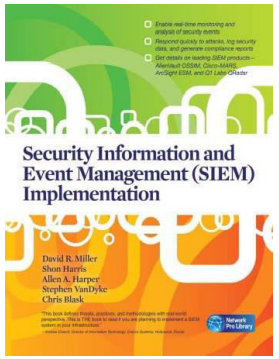
Security Information Event Management (SIEM)

…evolución de los SIEM?

- Asiste en la evaluación de la administración por objetivos (MBO) y en los indicadores claves de rendimiento (KPI *key performance indicator*)
- SIEM puede correlacionar varios eventos de aplicaciones ERP y CRM para verificar varios MBO específicos
- Puede saber cuanto tiempo demora una orden y su procesamiento [3]

SIEM

DEFINICIONES FORMALES DE OTROS AUTORES



Security Information Event Management (SIEM)

- **“The SIEM system is a complex collection of technologies designed to provide vision and clarity on the corporate IT system as a whole, benefitting Security analyst and TI administrator as well”**

Security Information and Event Management (SIEM) implementation, McGraw Hill, David Miller, Shon Harris, Allen Harper, Stephen VanDyke and Cris Blask 2011, isbn 978- 07-170109-9

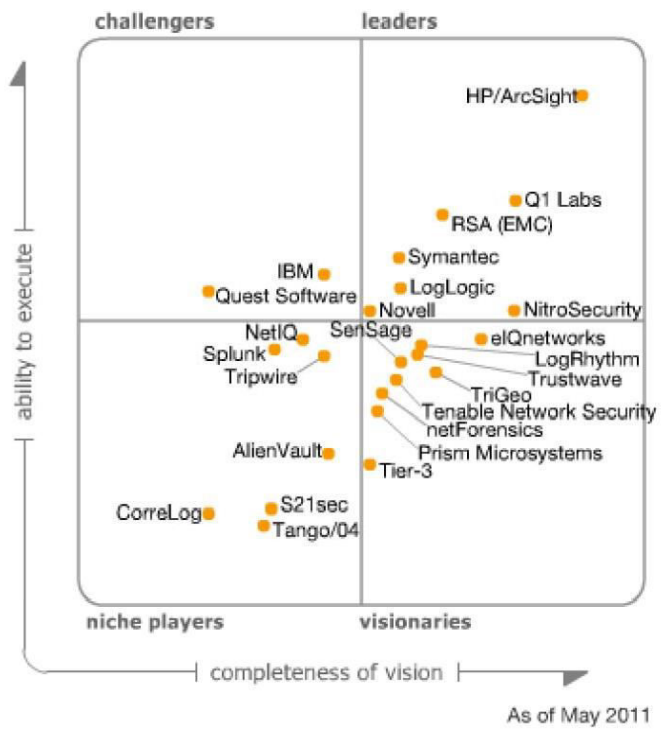
Security Information Event Management (SIEM)

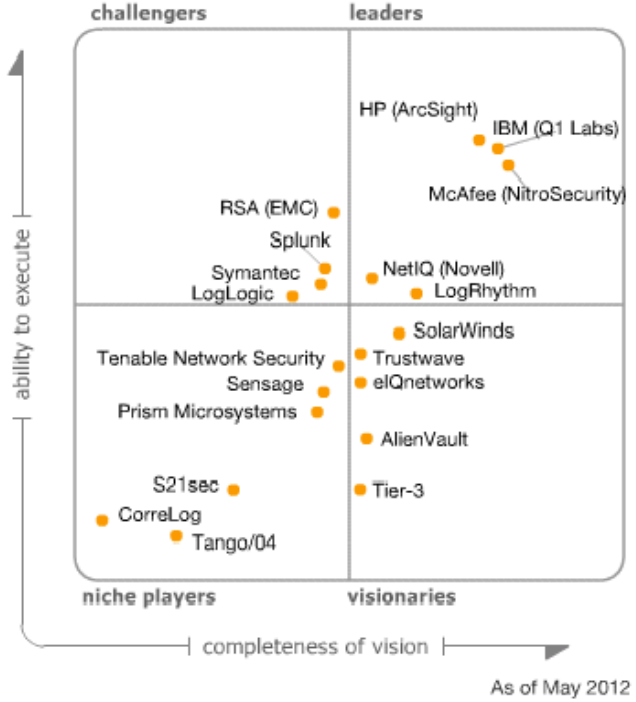
- “Much more powerful than data aggregation, Takes multiple isolated events, combining them into a single relevant security incident, Requires comparative observations based on multiple parameters such as– Source/destination IP addresses– Identifiable network routes– Type of attack– Type of malware installed on compromised systems – The time the activity began or ended”

The In’s and Out’s of SIEM Technology, Dr. Eugene Schultz, CISSP, CISM Chief Technology Officer Emagined Security
EugeneSchultz@emagined.com, IX National Computer and Information Security Conference, Bogota, Colombia, June 18, 2009

Security Information Event Management (SIEM)

- No todos los fabricantes en este cuadrante de Gartner se enfocan en lo mismo
- SIEM se compone de dos mercados diferentes:SIM y SEM





Security Information Event Management (SIEM)

Servicios Concretos (SIEM)

- Administración de logs
- Cumplimiento de regulaciones de IT
- Correlación de eventos (*)
- Respuestas activas
- Seguridad en el punto final (*)

Security Information Event Management (SIEM)

Ej Correlación de eventos ( ): *

Si la CPU de un servidor crítico del negocio está al 100%:

- A) ¿El AV(Anti Virus) identificó malware en ese servidor?
- B) ¿Otros AV de otros servidores reportaron actividades de malware?
- C) ¿Están otros servidores al 100% y el AV detecto actividades de malware?

Security Information Event Management (SIEM)

Correlación de eventos (*):

- D) ¿Hay aplicaciones o servicios que no responden?
- E) ¿Hay picos de tráfico de red generados por ese servidor?
- F) ¿Si hay picos de tráfico de red, es por DoS o DDoS?

Security Information Event Management (SIEM)

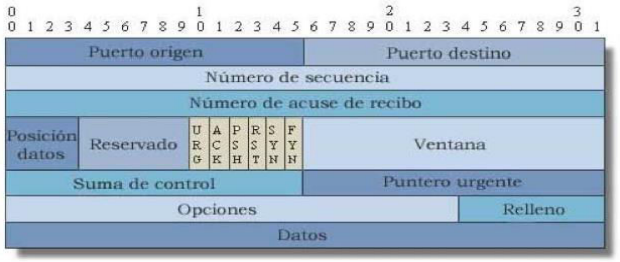
Correlación de eventos ( ):*

- Esto es correlación de eventos y se recomienda verificar manualmente.
- Al principio no se deben tener acciones automáticas (mientras aprende)!!
- Las reglas que se deben crear o que vienen pre-configuradas son el secreto mas preciado de las soluciones SIEM.

Security Information Event Management (SIEM)

Syn Flood (DoS y DDoS)

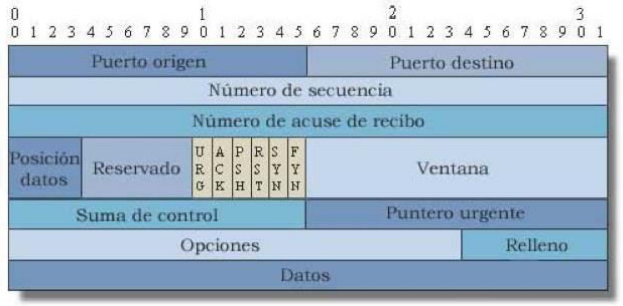
- # hping2 10.30.30.45 –-rand-source –S --destport 80 –- faster --debug –w 2048 -i u10000
- 100 paquetes por segundo para iniciar una sesion (*)
- Depende del contexto esto significa algo diferente?



Security Information Event Management (SIEM)

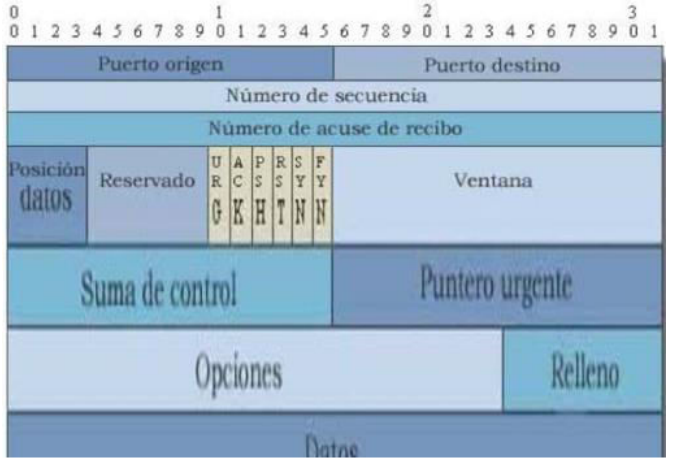
Logs de Snort/IDS:

- alert tcp $EXTERNAL_NET any -> $HOME_NET any (msg:"Ataque SYN a mas de 100 paquetes por segundo";flags:S;classtype:web-application- activity;threshold: type threshold, track by_src, count 100, seconds 1;)



Security Information Event Management (SIEM)

Scan: Xmas Tree

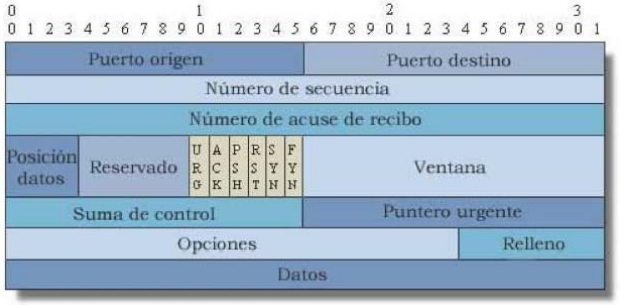


- # nmap -sX -P0 -v -p 80 127.0.0.1
- # tcpdump -i lo –l
- 03:04:06.818438 IP Knoppix.36655 > Uoc.globalteksecurity.com.http: FP 3608167536:3608167536(0) win 1024 urg0
- Depende del contexto esto significa algo diferente?

Security Information Event Management (SIEM)

Logs de Snort/IDS:

- alert tcp $EXTERNAL_NET any -> $HOME_NET any (msg:"Escaneo Xmas Tree nmap";flags:FPU;ack:0; reference:arachnids,28;classtype:attempted-recon; sid:628; rev:1;)



Security Information Event Management (SIEM)

Logs de Snort/IDS:

[**] [1:628:1] Escaneo Xmas Tree nmap [**] [Classification: Attempted Information Leak] [Priority: 2] 06/11-16:11:13.715613 192.168.100.12:46874 -> 192.168.100.11:603

TCP TTL:42 TOS:0x0 ID:26374 IpLen:20 DgmLen:40

U*PF Seq: 0x0 Ack: 0x0 Win: 0xC00 TcpLen: 20 UrgPtr: 0x0

[Xref => arachnids 28]

Security Information Event Management (SIEM)

Antes de implementar un SIEM

- ¿Se tiene la información clasificada?
- ¿A qué dispositivos se le tomarán eventos o logs, con que prioridad?
- ¿Qué clase de eventos se colectarán?
- ¿Por cuánto tiempo se debe retener esos logs?
- ¿Qué cantidad de esos logs se retendrán?

Security Information Event Management (SIEM)

Antes de implementar un SIEM

- ¿Donde se almacenarán esos logs cifrados, localmente o en la nube?
- ¿Que regulaciones (GRC) se deben cumplir?

Nota:GRC ="Governance,Risk and Compliance"

- ¿Hay que cumplir algun RFP(Request for Proposals)?

Security Information Event Management (SIEM)

Ejm de RFP

- Arquitectura: Modo de implementación que la empresa necesita, plataforma, recolección, Integración de componentes…
- Especificaciones técnicas: Colección, correlación, Análisis forense por incidente, gestión de datos, operación del producto…

Security Information Event Management (SIEM)

Estándares de logs

- Syslog (RFC5424, linux/unix, mac, etc)
- Alertas propietarias (Antivirus, IDS, IPS, Windows, AS400, etc)
- Flujo de datos (HTTP):
- Netflow (Cisco), J-Flow (Juniper),
- Q-Flow (Q1Labs), sFlow (RFC3176)

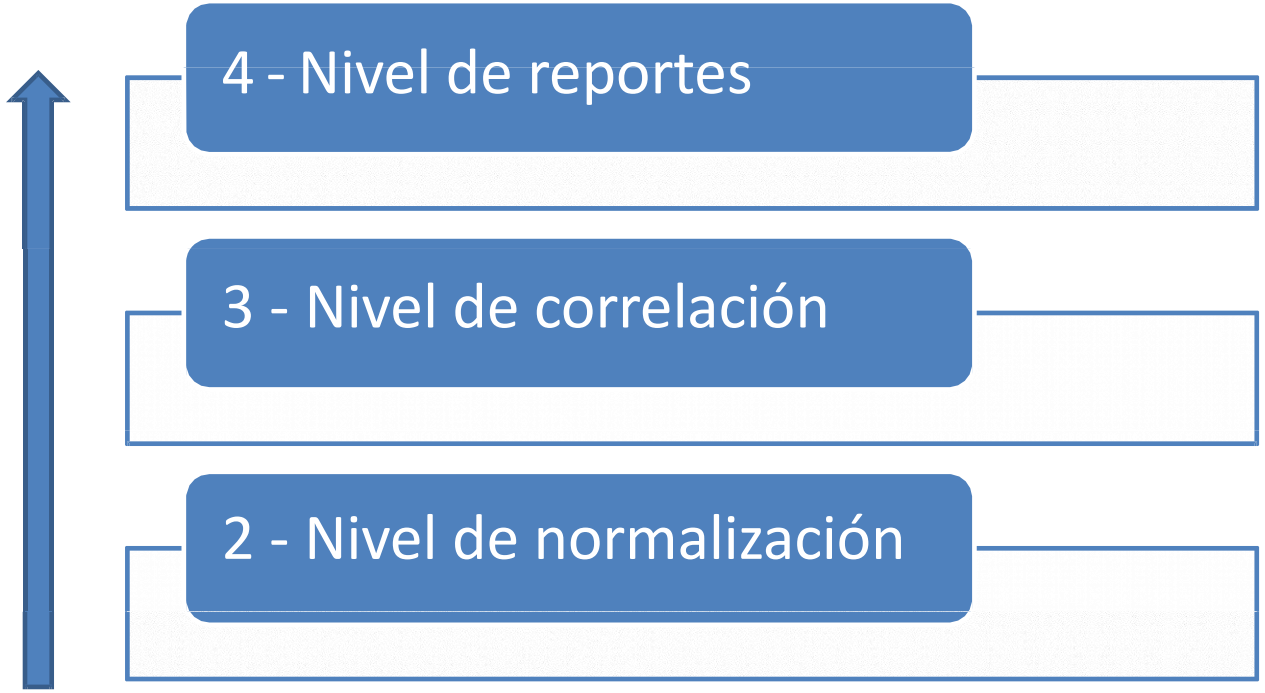
Security Information Event Management (SIEM)

Colectores (Agentes invasivos):

- Libres: CAIDA cflowd, mindrot.org flow, splintered.net flow-tools y SNARE para el endpoint.
- Comerciales: Vendedores de routers y switchs, Lancope's Stealthwatch, Tivoli, Arbor Network Peak Flow.

ARQUITECTURA DE LOS SISTEMAS SIEM

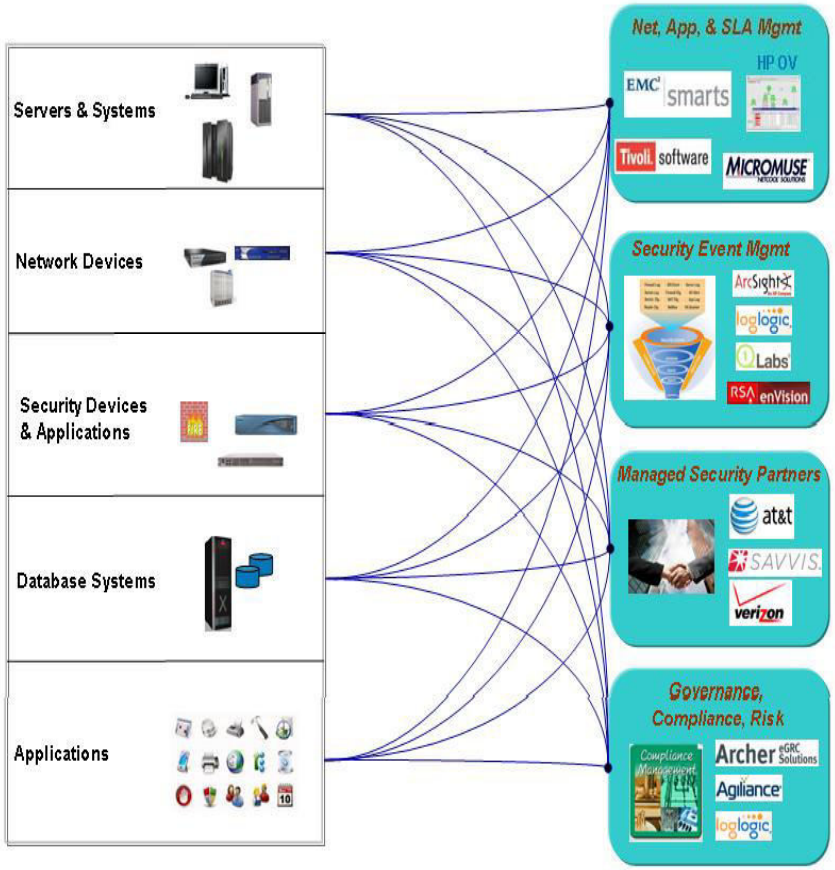
Security Information Event Management (SIEM)



Pila de capas de los SIEM: 1 Nivel de captura eventos

Security Information Event Management (SIEM)

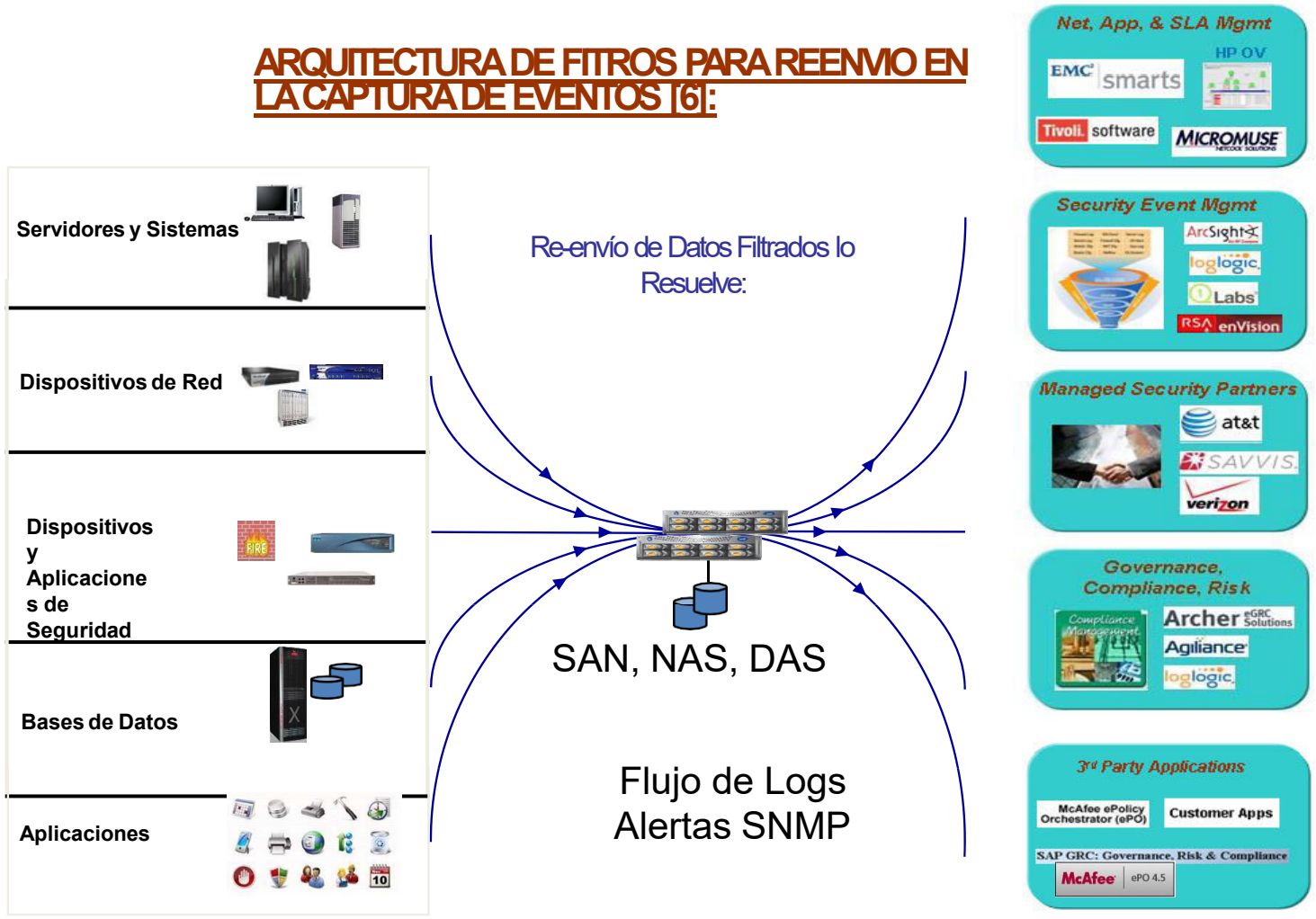
ARQUITECTURA ACCIDENTAL PARA CAPTURA DE EVENTOS [6]:



- Requiere que los datos de logs, flujo, y SNMP se obtengan varias veces de cada sistema
- Puede requerir múltiples agentes para recolectar datos
- Almacenamient o Duplicado
- Altísimo Costo Operacional

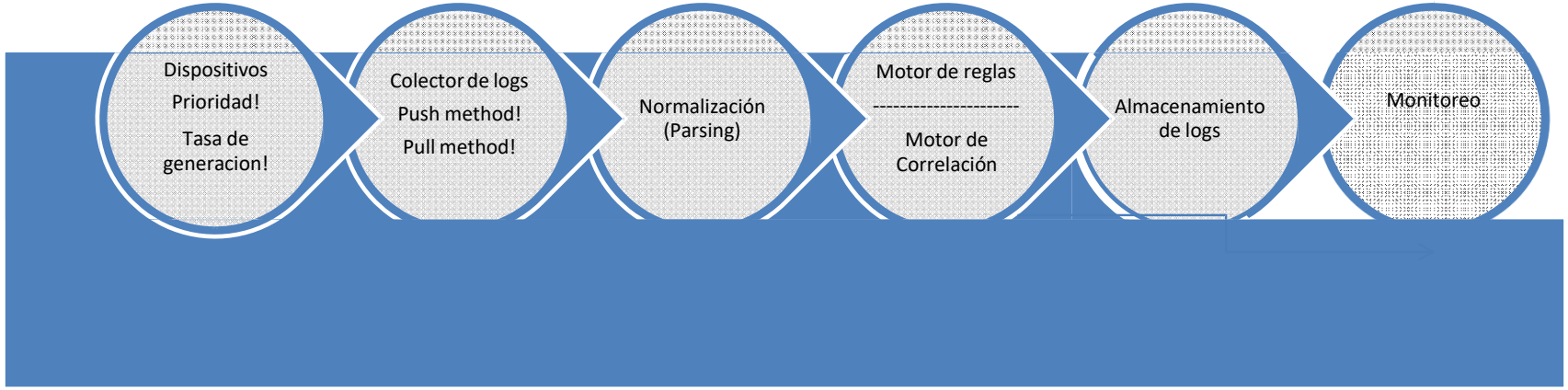
Security Information Event Management (SIEM)

ARQUITECTURA DE FITROS PARA REENVIO EN LA CAPTURA DE EVENTOS [6]:



Security Information Event Management (SIEM)

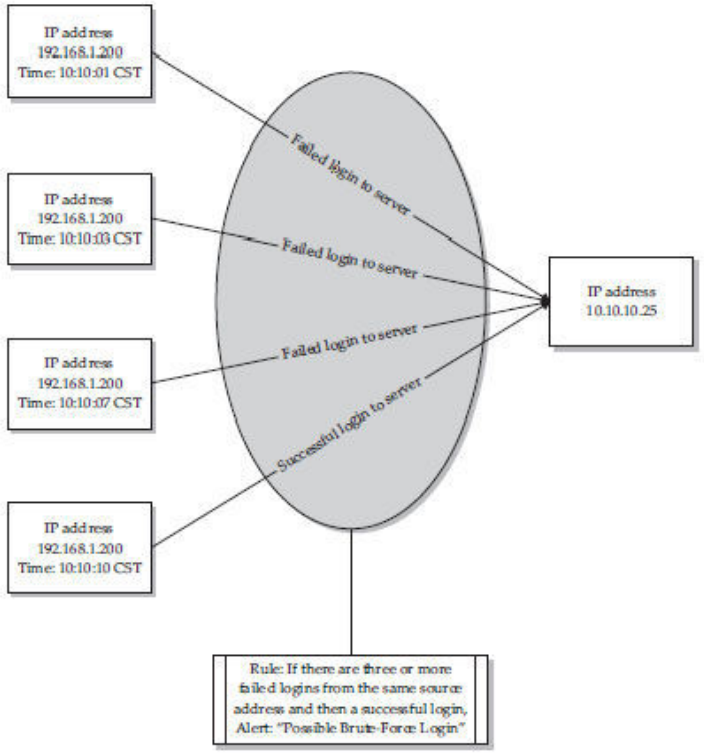
Anatomía de un sistema SIEM [2]



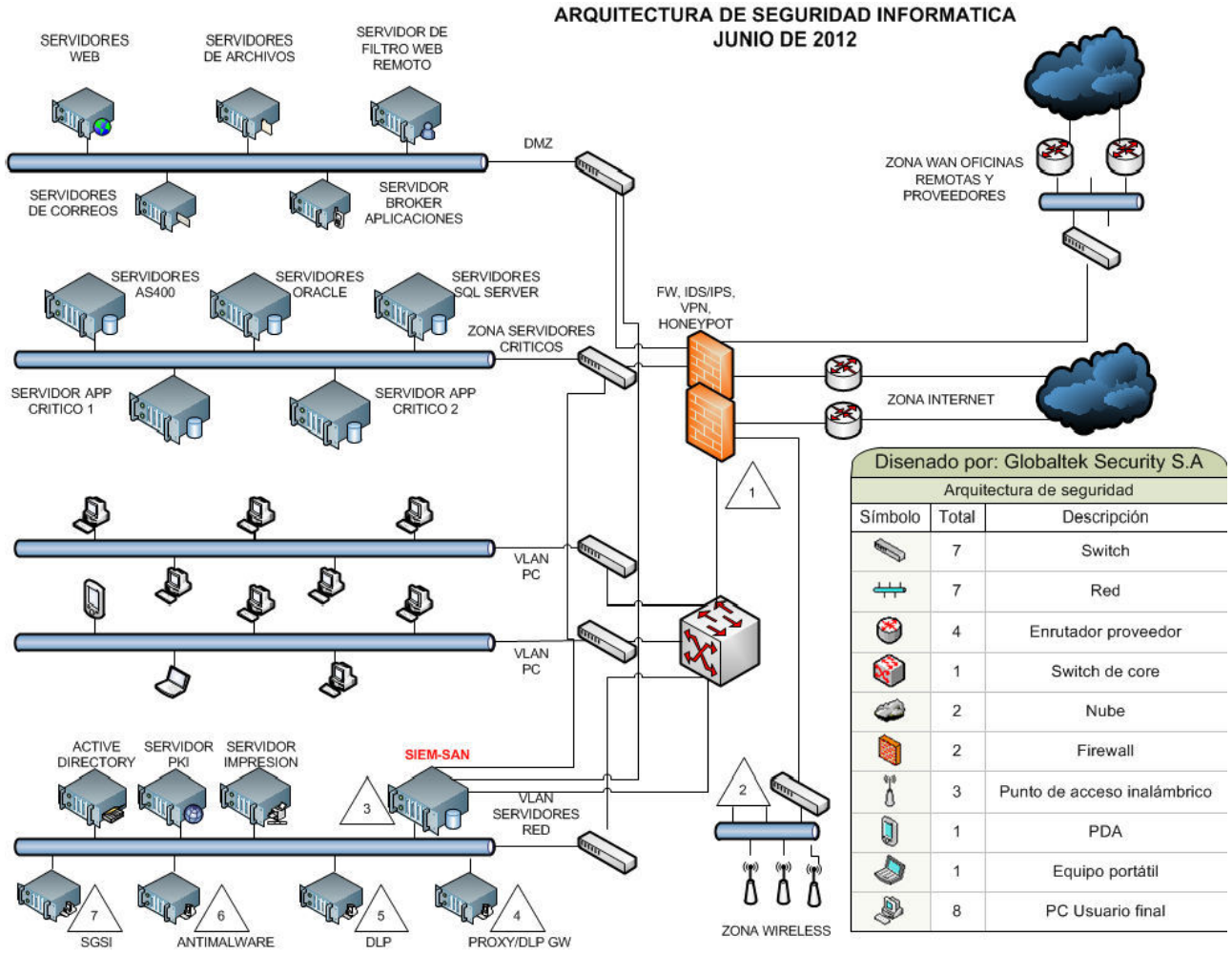
Security Information Event Management (SIEM)

Motor de Correlación [2]:

Time	Event Number	Source	Destination	Event
10:10:01 CST	1035	192.168.1.200	10.10.10.25	Failed login to server
10:10:02 CST	1036	192.168.1.90	10.10.10.21	Successful login to server
10:10:03 CST	1037	192.168.1.200	10.10.10.25	Failed login to server
10:10:04 CST	1038	192.168.1.91	10.10.10.35	Failed login to server
10:10:05 CST	1039	192.168.1.10	10.10.10.2	Successful login to server
10:10:06 CST	1040	192.168.1.10	10.10.10.3	Successful login to server
10:10:07 CST	1041	192.168.1.200	10.10.10.25	Failed login to server
10:10:08 CST	1042	10.10.10.54	192.168.1.201	Failed login to server
10:10:09 CST	1043	10.10.10.34	192.168.1.10	Failed login to server
10:10:10 CST	1045	192.168.1.200	10.10.10.25	Successful login to server



Security Information Event Management (SIEM)

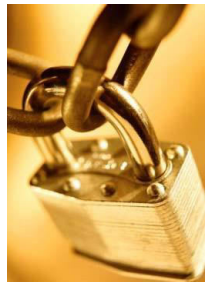


FUTURO DE LOS SISTEMAS SIEM

Security Information Event Management (SIEM)

Futuro de SIEM

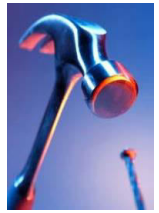
- Arquitectura menos intrusiva
- Consola única,
- El análisis del incidente debe incluir el flujo de red
- Fuentes de datos empresariales para la captura de los eventos de CRM(*Customer Relationship Management)*, ERP,(*Enterprise Resource Planning)* Ventas, etc
- SDK(*software development kit)*…



Security Information Event Management (SIEM)

…Futuro de SIEM (La nube)

- Ilimitado número de dispositivos
- Ilimitado número de eventos capturados por segundo
- Ilimitado almacenamiento apalancado en la infraestructura que provee la nube
- Posibilidad de capturar eventos de usuarios basados en el negocio



Security Information Event Management (SIEM)

Conclusiones

- SIM nos entrega logs de IT
- SEM nos entrega logs o la materia prima para sustentar como ocurrio una falla o un incidente de seguridad (dispositvos seguridad)
- No se puede hacer gestion de incidentes sin un sistema de gestion y correlacion de eventos

Security Information Event Management (SIEM)

Conclusiones

- No puedo preveer si no tengo tendencias basados en mi realidad
- SIEM esta en linea haciendo push a la estrategia “Defensa en profundidad” para suplir las falencias de los IPS, IDS, Firewalls…

Security Information Event Management (SIEM)

Conclusiones

- El autor cree que es mejor hacer PoC con las soluciones mas relevantes de gartners antes de inclinarse por una marca en especial
- Haga su lista especifica de dispositivos y priorice la clase de logs

Security Information Event Management (SIEM)

Conclusiones

- Haga su lista de deseables de la solucion y concrete respuestas de proveedores mediante RFI
- SIEM es una tecnologia madura y un mercado emergente
- La computacion en la nube bajara los costos de almacenamiento cifrado (Confidencialidad/Privacidad)

SOC

Security Operation Center

SOC

Security
Operation
Center

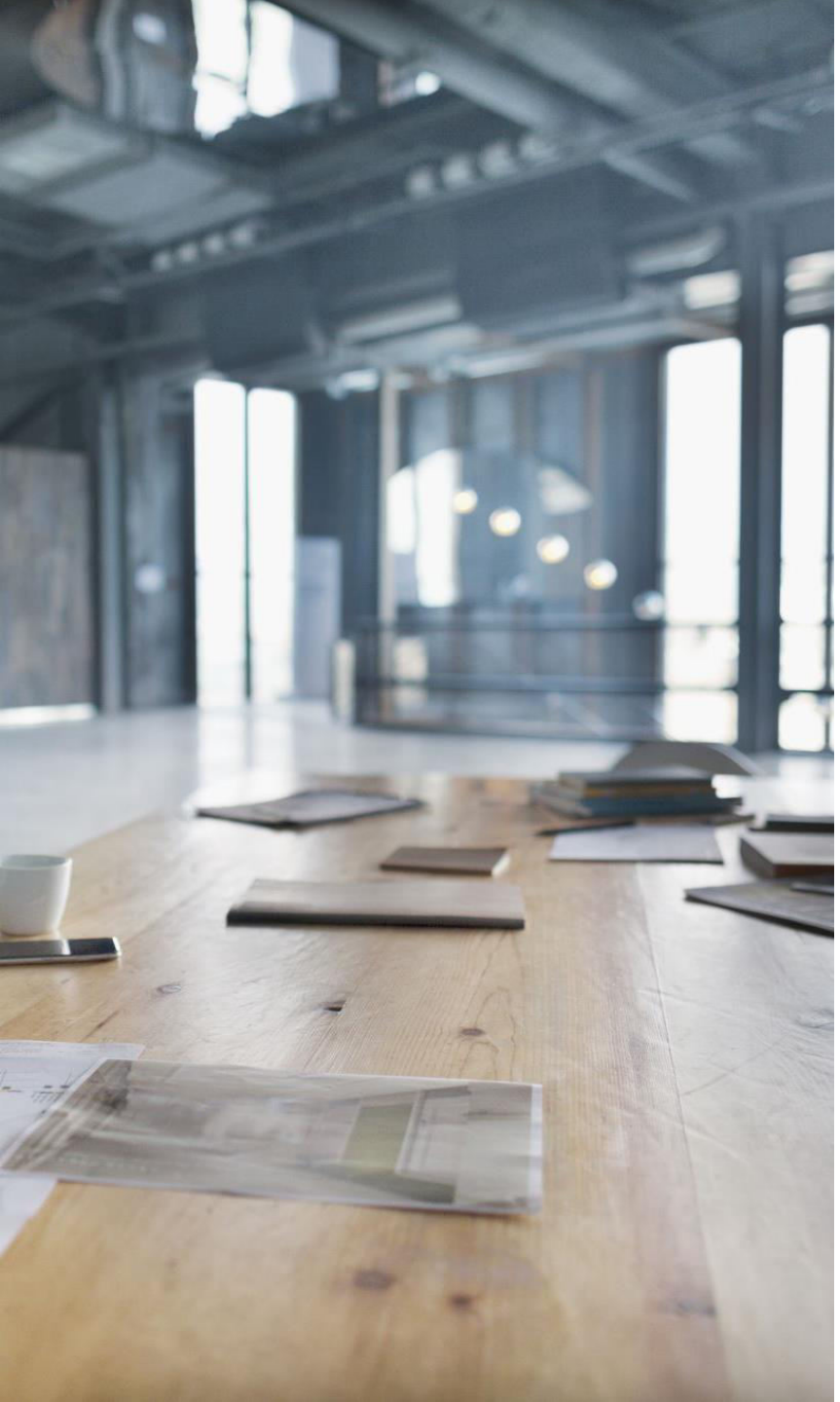
Definición de un SOC

- El Centro de Operaciones de Seguridad, SOC, se refiere al equipo responsable de garantizar la seguridad de la información.
- El SOC es una plataforma que permite la supervisión y administración de la seguridad del sistema de información a través de herramientas de recogida, correlación de eventos e intervención remota.
- El SIEM (Security Information Event Management) es la principal herramienta del SOC ya que permite gestionar los eventos de un SI.

SOC

Objetivo del SOC

- El objetivo de un SOC es detectar, analizar y corregir incidentes de ciberseguridad utilizando soluciones tecnológicas y enfoques diferentes.
- Supervisan y analizan la actividad en redes, servidores, terminales, bases de datos, aplicaciones, sitios web y otros sistemas en busca de señales débiles o comportamientos anormales que puedan indicar un incidente de seguridad o un compromiso.
- El SOC debe garantizar que los posibles incidentes de seguridad se identifiquen, analicen, defiendan, investiguen e informen adecuadamente.
- Los SOC están generalmente compuestos por analistas e ingenieros de seguridad, así como por gerentes que supervisan las operaciones de seguridad.
- Las capacidades adicionales de algunas SOC pueden incluir el análisis avanzado, el criptoanálisis y la ingeniería inversa del malware para analizar los incidentes.
- Los equipos de SOC trabajan en estrecha colaboración con los equipos de respuesta para garantizar que el problema de seguridad se aborde adecuadamente una vez que se ha descubierto.



SOC

¿Cómo funciona un SOC?

- El primer paso para establecer un SOC es definir claramente una estrategia que integre los objetivos específicos de la empresa de los distintos departamentos.
- Una vez desarrollada la estrategia, se establece la infraestructura necesaria para apoyarla.
- Una infraestructura SOC típica incluye cortafuegos, IPS/IDS, soluciones de detección de brechas, sondas y un sistema de gestión de eventos e información de seguridad (SIEM).
- Debe existir la tecnología para recolectar datos a través de flujos de datos, mediciones, entrada de paquetes, syslog y otros métodos para que la actividad de datos pueda ser correlacionada y analizada por los equipos de SOC.
- El Centro de Operaciones de Seguridad también supervisa las vulnerabilidades de la red y de los puntos finales para proteger los datos confidenciales y cumplir con las normativas de la industria o gubernamentales.

SOC

¿Cómo se organiza el SOC?

Para la consecución de estos objetivos, un SOC se divide por niveles en función del grado de especialización de los analistas que lo conforman:

1. **En el nivel 1, se encuentran los analistas de alertas, que monitorizan continuamente las alertas que recibe el SOC. Los analistas evalúan estas alertas de seguridad y, si alcanzan el umbral predefinido según la política del SOC, se escalan al nivel 2.**
2. **Los analistas de nivel 2 determinan si los datos o el sistema se han visto afectados y, de ser así, recomendarán una respuesta.**
3. **Por último, el nivel 3 está compuesto por profesionales altamente capacitados, que se encargan de resolver los incidentes, pero también de buscar posibles incidentes con el fin de prevenirlos.**

A diferencia de un departamento de TI tradicional, el personal de un SOC incluye principalmente un equipo de analistas y técnicos de ciberseguridad altamente experimentados y especializados.

La especialización de estos analistas, aunque han de compartir una base técnica común, varía mucho.

Ello beneficia al SOC y, por consiguiente, a la organización, ya que es de gran utilidad que los analistas tengan perfiles provenientes de diferentes disciplinas.

NOC

Network
Operation
Center

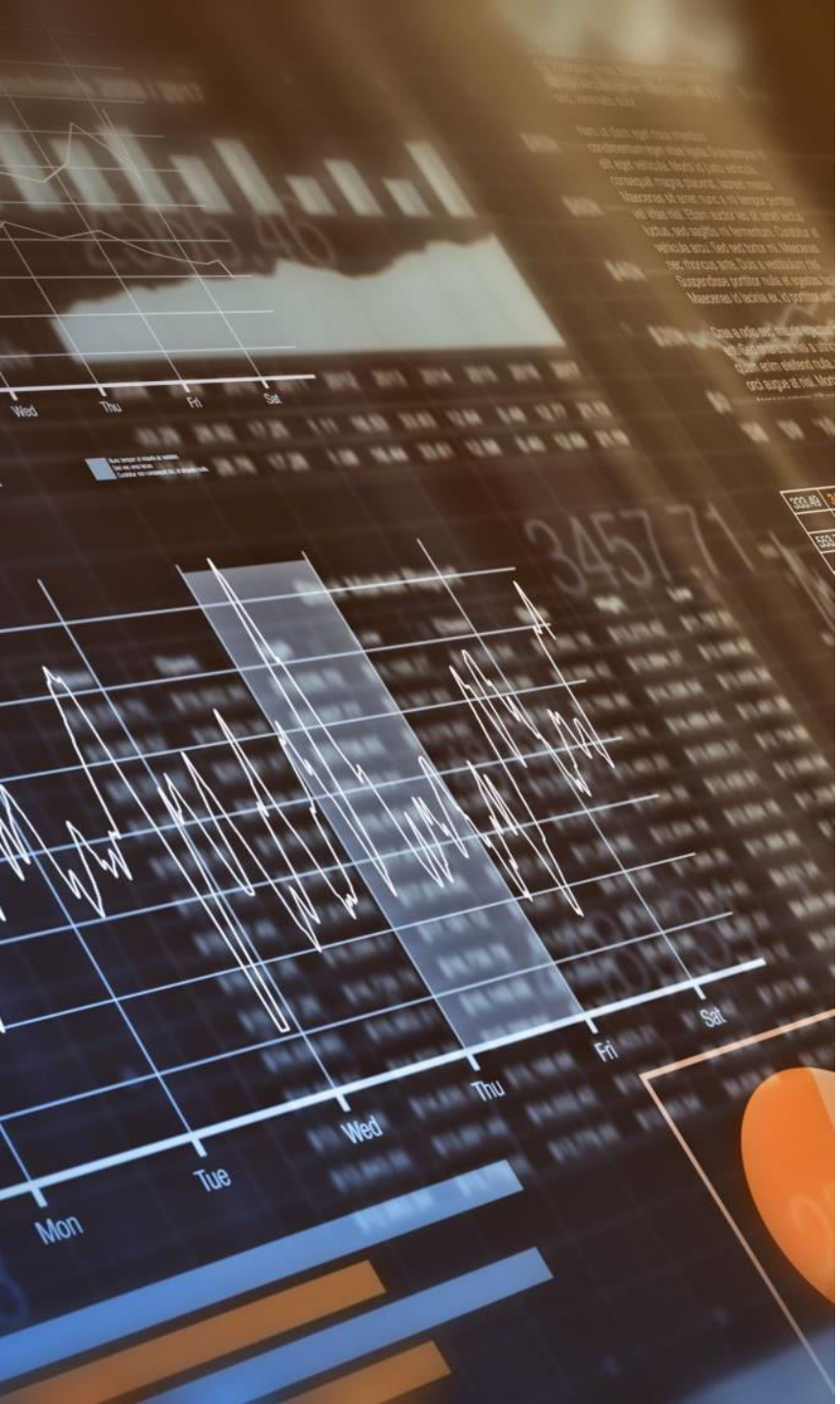
NOC

Definición

Un Centro de Operaciones de Red (NOC) se refiere a una ubicación centralizada donde el monitoreo y la gestión de los servicios de tecnología e infraestructura se lleva a cabo las 24 horas del día, los 7 días de la semana y los 365 días del año.

El equipo del centro de operaciones de red o Network Operation Center (NOC) es el responsable de garantizar que la infraestructura de la red corporativa pueda satisfacer sus demandas.

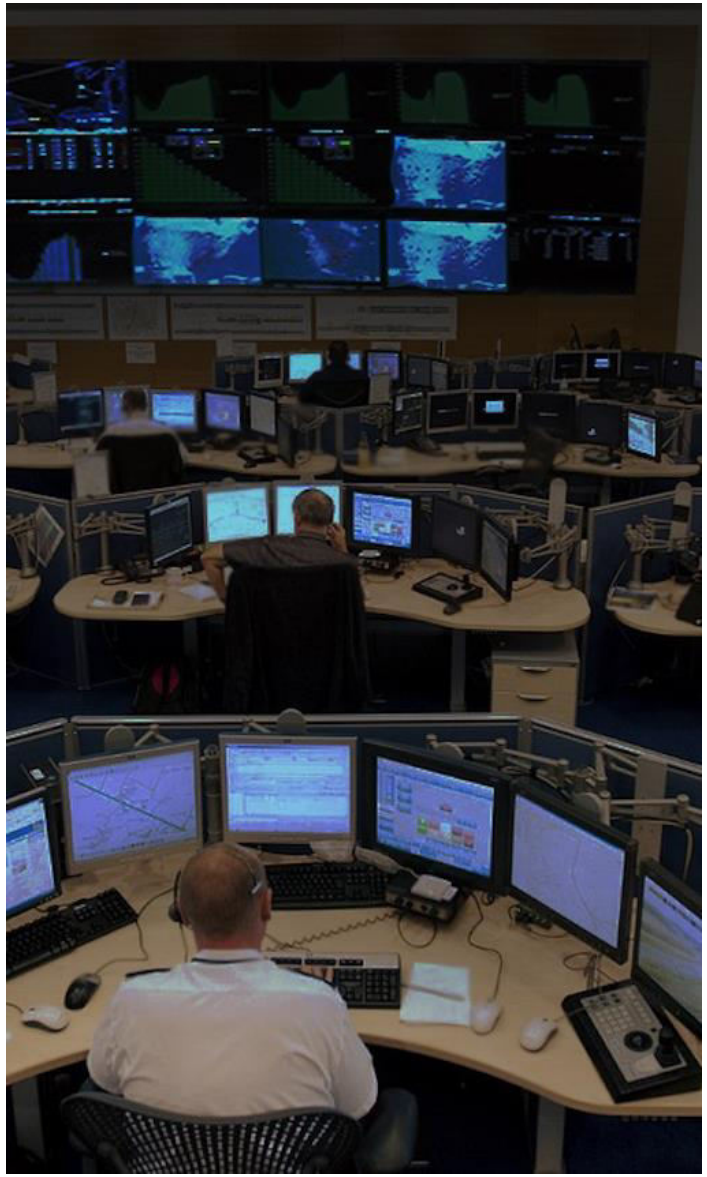
El NOC optimiza la red corporativa y soluciona los problemas para garantizar que las necesidades de la empresa sean cubiertas.



NOC

Funciones generales

- Comprobar el estado y rendimiento de la red, los servidores y las aplicaciones.
- Identificar proactivamente los cuellos de botella, analizando el ancho de banda.
- Optimizar la configuración de red según los requisitos específicos.
- Reducir el tiempo medio de reparación, gracias a la rápida identificación y resolución de problemas.
- Asegurar la operación diaria de la red.
- Supervisar las alarmas del sistema, analizar el nivel de gravedad y la clasificación.
- Crear *tickets* de incidentes basados en alarmas y asignar al equipo correspondiente para su solución.
- Seguir el proceso de escalamiento adecuado, según la gravedad del incidente o alerta.
- Ser el primero en actuar en caso de que se presente un evento que afecte la estabilidad de la red.



NOC

¿Qué hay dentro de un NOC?

Las pantallas son la marca registrada de cualquier NOC, por lo general tienen dos tipos:

Pantallas grandes: como Video Walls, para compartir indicadores importantes como el tráfico y el estado de los nodos.

Monitores más pequeños: parte de la consola del escritorio del operador, para ver elementos específicos.

La mayoría de las veces, las pantallas principales muestran los resultados de un sistema de monitoreo centralizado que recopila, sintetiza y correlaciona datos de múltiples fuentes, de ahí la necesidad de que una gran cantidad de personas la vean.

Las mesas de operaciones muestran información de eventos reales, que incluye:

Estado de alarma

Fuente

Tiempo

Otros datos relevantes

NOC

Otros recursos que pueden ser necesarios son:

- Teléfonos para ponerse en contacto con el personal de apoyo experto / de campo relevante y con terceros
- Computadoras con software de oficina para correo electrónico, herramientas de colaboración y herramientas de informes
- Herramientas de software de gestión de servicios para registrar y escalar eventos importantes
- Herramientas de software para acceso remoto y resolución de problemas de elementos afectados
- Bases de conocimientos para consultar información del sistema y guías de resolución de problemas
- Pantallas de televisión que muestran noticias, feeds de redes sociales y otras fuentes de información relevantes.

NOC vs SOC

¿Que tareas exactamente se realizan en un NOC?

- Se centra en la disponibilidad y el rendimiento.
- Monitorear la red, los servidores y las aplicaciones para la salud y el rendimiento
- Analizar el ancho de banda e identificar proactivamente los cuellos de botella
- Modificar las configuraciones de la red según las necesidades de la empresa
- Detectar y soluciona rápidamente los fallos para reducir el tiempo medio de reparación

El trabajo del NOC es cumplir los acuerdos de nivel de servicio (SLA) y gestionar los incidentes de forma que se reduzca el tiempo de inactividad.

¿Qué es un SOC?

El SOC se centra en los incidentes y las alertas que afectan a la seguridad de los activos de información.

Son los encargados de administrar y/o operar El “System Information and Event Management (**SIEM**)”, que ayuda a tener una visión global de los eventos de seguridad informática de todos los dispositivos de la red.

Análisis Forense

Porque la Informática Forense?

La brecha es cada vez menor entre fraude e informática.

Las pérdidas asociadas a fraudes informáticos van en aumento.

Las áreas con mayor riesgo de fraude dependen de la tecnología.

La auditoría de sistemas la informática forense y las áreas legales siguen trabajando en forma aislada

Porque la Informática Forense?

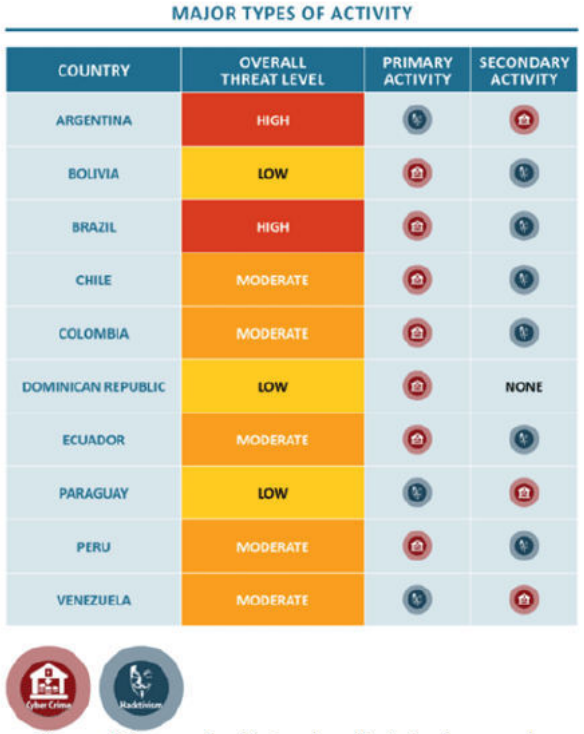
Los ataques informáticos revisten mayor complejidad cada dia
y la auditoría forense debe abarcar aspectos técnicos.

Una investigación integral requiere de herramientas y recursos tecnológicas.

La evidencia digital aporta información
valiosa para el esclarecimiento de los hechos.

Porque la Informática Forense?

- Robo de identidad
- Espionaje empresarial
- Ransomware
- Fraudes bancarios
- Manipulación en BD*
- Hurtos y estafas informáticas
- Otras manipulaciones (contabilidad otros)
- Fuga de información

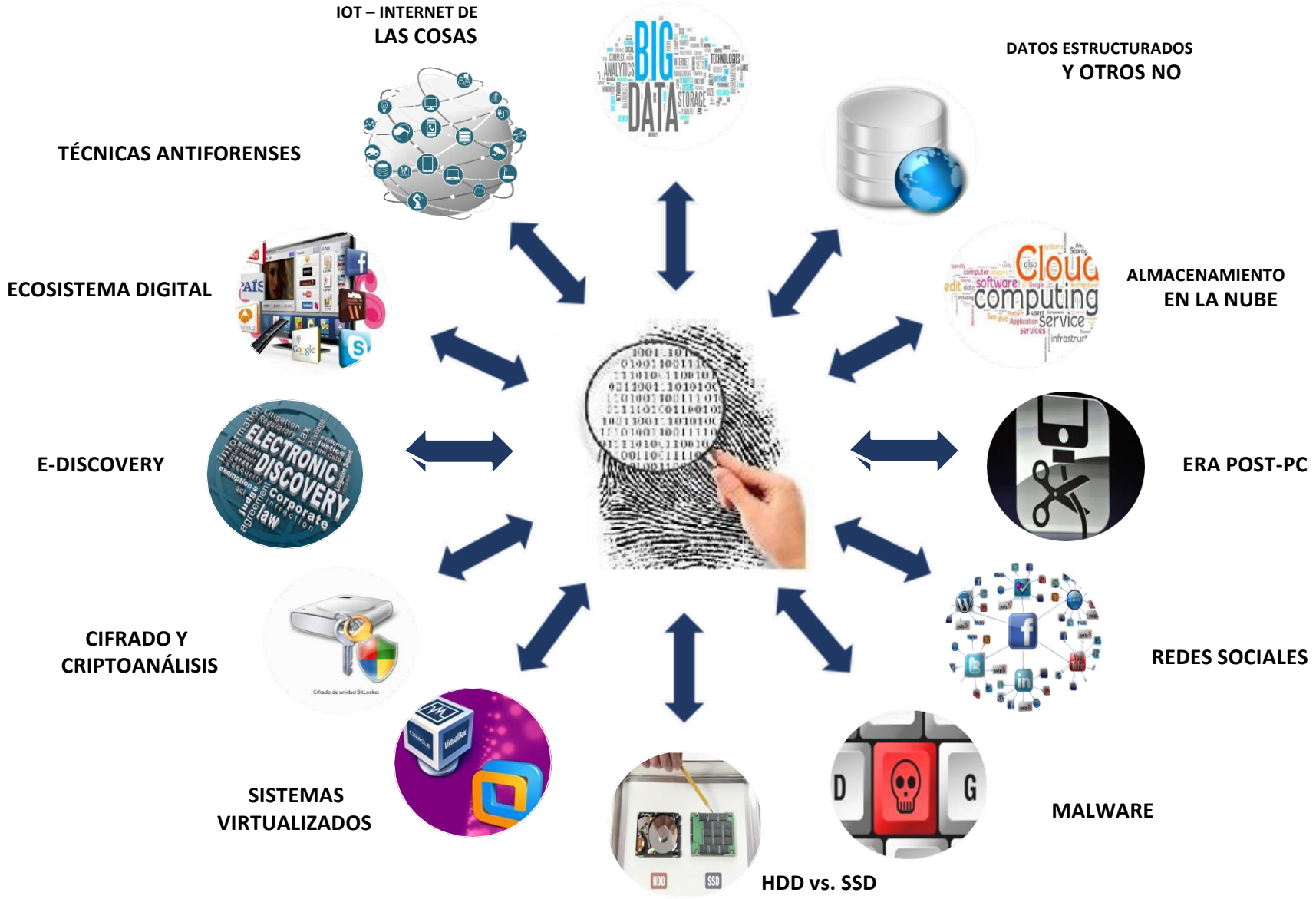


MAJOR TYPES OF ACTIVITY

COUNTRY	OVERALL THREAT LEVEL	PRIMARY ACTIVITY	SECONDARY ACTIVITY
ARGENTINA	HIGH	Hacktivism	Cyber Crime
BOLIVIA	LOW	Cyber Crime	Hacktivism
BRAZIL	HIGH	Cyber Crime	Hacktivism
CHILE	MODERATE	Cyber Crime	Hacktivism
COLOMBIA	MODERATE	Cyber Crime	Hacktivism
DOMINICAN REPUBLIC	LOW	Cyber Crime	NONE
ECUADOR	MODERATE	Cyber Crime	Hacktivism
PARAGUAY	LOW	Hacktivism	Cyber Crime
PERU	MODERATE	Cyber Crime	Hacktivism
VENEZUELA	MODERATE	Hacktivism	Cyber Crime

Figure 1: Major types of activity in selected Latin American countries

Retos y actuales desafios



Informática Forense

Disciplina de las ciencias forenses que, considerando las tareas propias asociadas con la evidencia procura descubrir e interpretar la información en los medios Informáticos para establecer los hechos y formular las hipótesis relacionadas con el caso.

Entendiendo los equipos de computación ofrece un análisis de la información residente en dichos equipos.

Guía para preservación de evidencia digital.

https://www.ietf.org/rfc/rfc3227.txt

Informática Forense

ANALIZA: evidencia que colabore a llevar adelante una causa judicial o una negociación extrajudicial

DETERMINA: datos potenciales o relevantes
Posibilidades reales de la evidencia existente o supuesta.

Los destinatarios son los procesos judiciales aunque cualquier empresa o persona puede contratarlo.


La informática forense, a la caza del empleado traidor

Principios básicos

1. Aprenda y aplique las Reglas de ORO de la informática Forense.
2. Conozca los tres pilares de la informática forense (C.I.A.).
3. Prepare su equipo de herramientas I.R. (Incident Response – software).
4. Use guantes de látex, pulseras y bolsas antiestática, documentos para rotular.
5. Identifique y fije la evidencia digital (smartphone, correos, cd, diskettes,xbox)
6. Utilice medios estériles (wipping) y contenedores de mayor tamaño.
7. Siempre preserve la data volátil (Running process) www.accessdata.com
8. Solicite al experto una imagen forense (FTK Imager 3.1.1.8): Lógica y Física.
9. Registre siempre el valor Hash de los archivos o dispositivos en investigación.
10. Recuerde que lo que NO está escrito NUNCA ocurrió.

1. CONOZCA LAS REGLAS DE ORO DE LA INFORMÁTICA FORENSE.

Proteja la evidencia original ….

Proteja la evidencia original ….

Proteja la evidencia original ….

10 +

2. APLIQUE LOS TRES PILARES DE LA SEGURIDAD INFORMÁTICA (C.I.A.).

•Confidencialidad: No tenga acceso quien no deba ver la información
•Integridad: No se modifique durante todo el proceso
•Disponibilidad=Availabity : Pueda acceder en cualquier momento del proceso

=

Hash
Imagen forense
Cadena de custodia
Bodega de evidencia
Wipping

10 +

3. PREPARE SU EQUIPO DE HERRAMIENTAS FORENSES

www.e-fense.com

www.forwarddiscovery.com

www.deftlinux.net/

www.accessdata.com

AccessData

FTK IMAGER 3.1.1.8

www.sumuri.com

PALADIN 4.0

PERMITE:

- Hacer imágenes forenses
- Hacer hash archivos de interés
- Búsquedas preliminares
- Garantizar integridad

10 +

4. Use guantes de látex, pulseras, bolsas antiestática documentos para rotular, otros mecanismos de protección de la evidencia en su recolección.

10 +

5. IDENTIFIQUE Y FIJE LA EVIDENCIA DIGITAL

- **Fotografía: Numerador, señalador, testigo métrico**
- **Estampado cronológico**

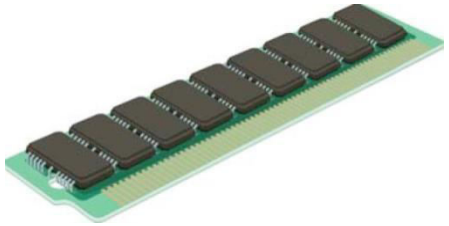
10 +

Lógico :

Datos volátiles

6. Siempre preserve la data volátil

- RAM RANDOM ACCESS MEMORY
- OPCIÓN CAPTURE MEMORY FTK IMAGER



- Procesos, historial de comandos
- Direcciones IP, Conexiones
- Puertos Abiertos
- Contraseñas
- Información del sistema, usuarios

10 +

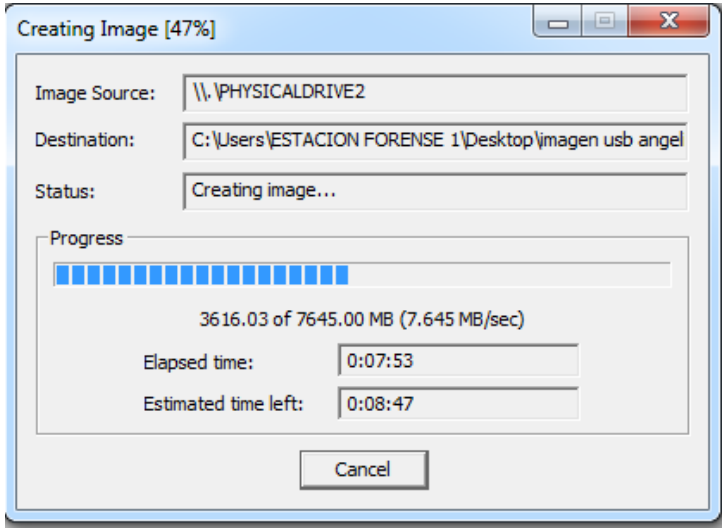
Los "Datos Volátiles", son aquellos que desaparecen cuando un sistema se apaga o se reinicia, por lo que hay que extraer la máxima información de estos datos, puesto que es muy importante a la hora de recopilar pruebas cuando un sistema ha sido comprometido.

7. Utilice medios estériles (wipping) y contenedores de mayor tamaño.

8. Solicite a los expertos una imagen forense : Física-Lógica

AccessData

FTK IMAGER 3.1.1.8

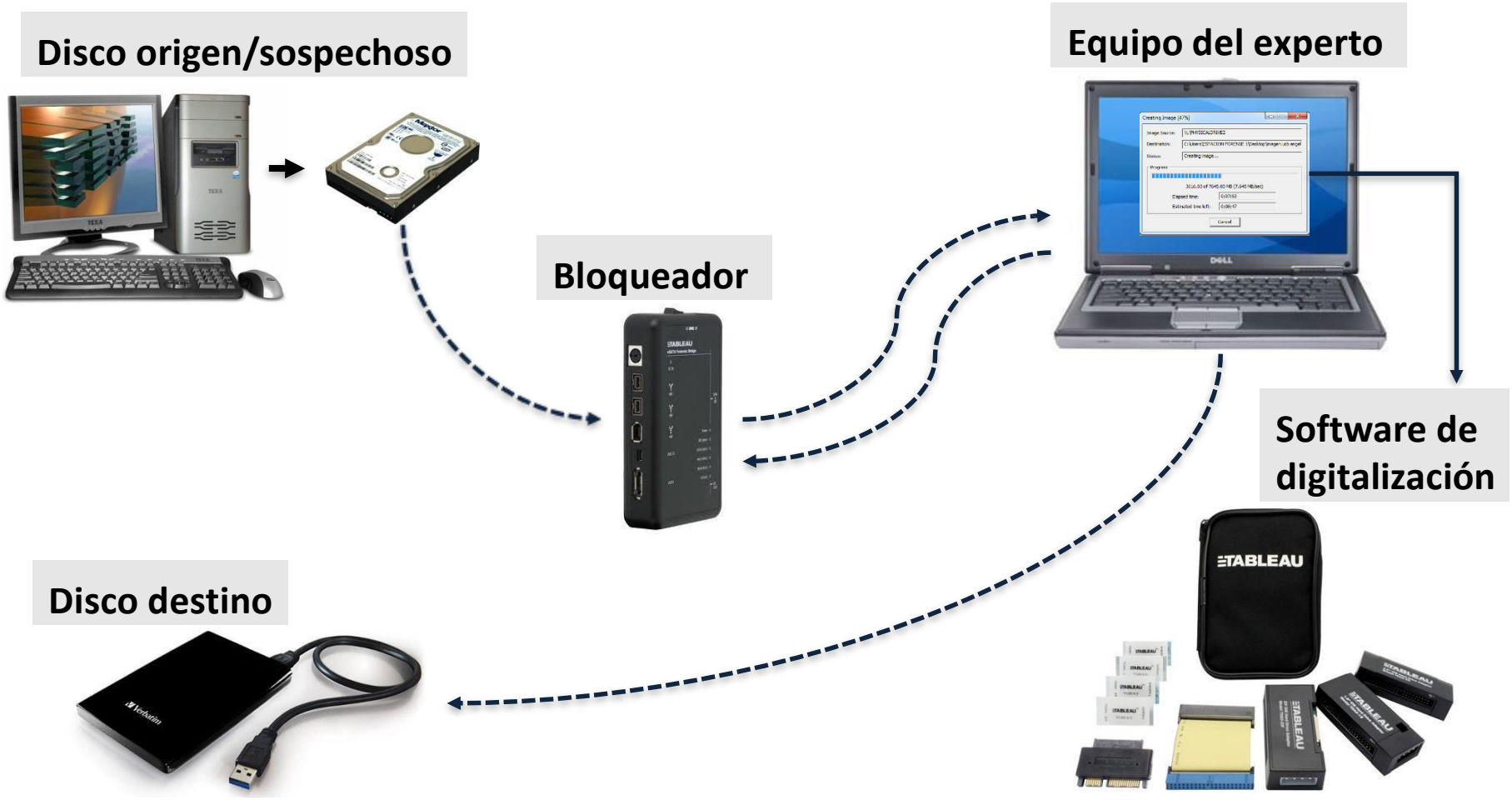


- Proteje la evidencia de daños no deliberados
- Garantiza la integridad de la misma
- Permite realizar varias copias de la imagen
- Sólo se puede abrir con software forense

?

- Software de digitalización de imagen
- Disco de origen= sospechoso o víctima
- Disco de destino= Mayor tamaño y Wipping
- Bloqueadores= Software o Hardware de bloqueo escritura-lectura
- Equipo del experto

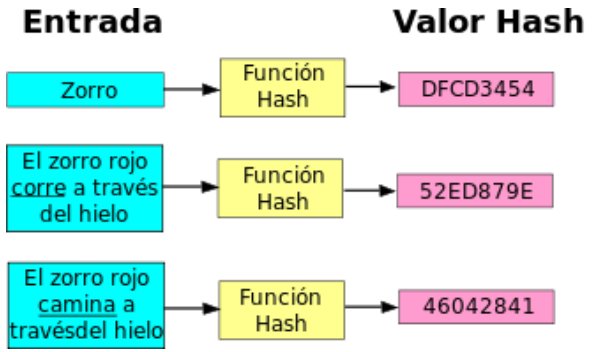
8. Solicite a los expertos una imagen forense: Física-Lógica

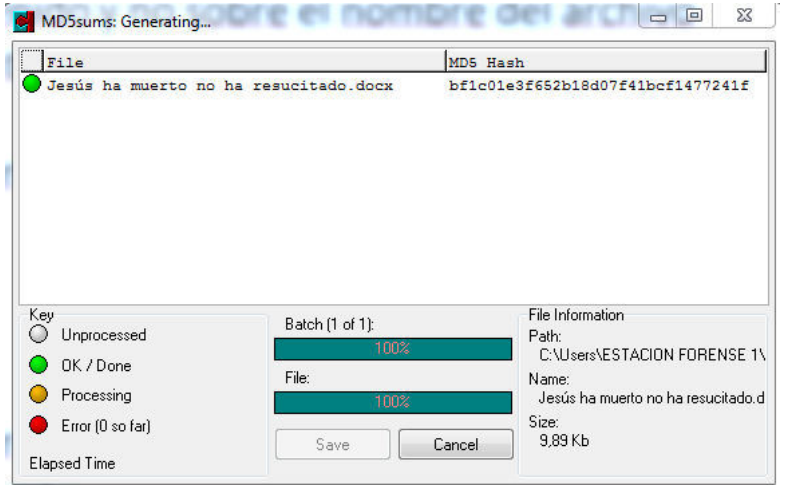


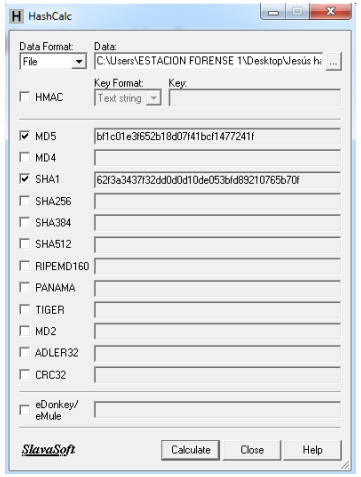
9. Registre el valor Hash de los archivos y dispositivos a incautar

HASH : High Algorithm Secure Hash

- Valor numérico que se da a los datos.
- Función o algoritmo Criptográfico.
- Sobre el contenido y no sobre el nombre del archivo.
- Garantiza la integridad del archivo.

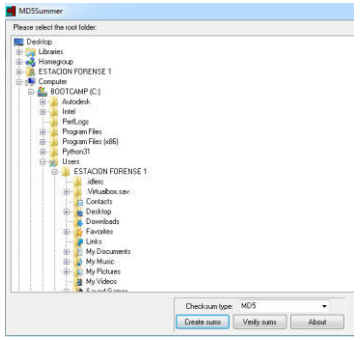


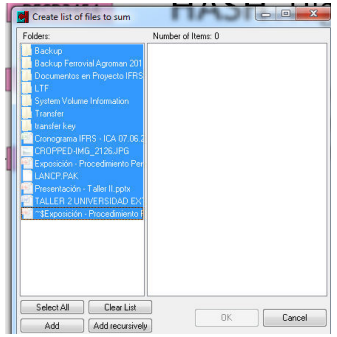


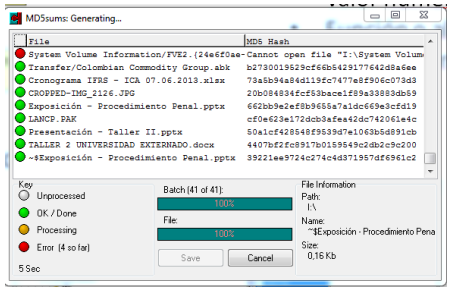


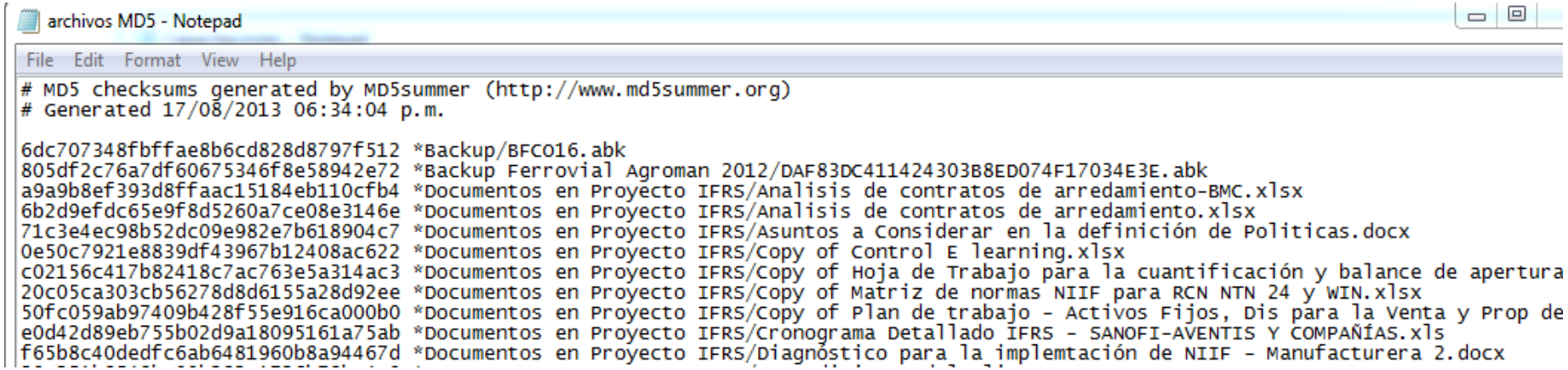
10 +

9. Registre el valor Hash de los archivos y dispositivos a incautar









www.md5summer.org

10. Recuerde que lo que NO está escrito NUNCA ocurrió

10 +

FIRMA AUDITORA - LA UNIVERSAL

CADENA DE CUSTODIA

Número del caso	0012548			
¿Quién halló?	**DIANA MARCELA GUTIERREZ**			29.328.252
¿Quién rotuló?	**DIANA MARCELA GUTIERREZ**			29.328.252
¿Quién embalo?	**DIANA MARCELA GUTIERREZ**			29.328.252
Tipo de embalaje		Plástica		Papel	X	Otra: Antiestática
Descripción del elemento						

Un dispositivo de almacenamiento digital externo color negro, marca maxell, con capacidad de almacenamiento de 4 GB.

Registro de continuidad

17	08	13	16:22	Diana Marcela Gutierrez	9.125.541	Custodia	
17	08	13	16:22	Yenny Sánchez	4.587.152	Transportadora	
17	08	13	16:22	Carla García	8.458.365	Almacenista	
D	M	A	Hora	Nombres y Apellidos	Cédula	Observaciones	Firma
D	M	A	Hora	Nombres y Apellidos	Cédula	Observaciones	Firma
D	M	A	Hora	Nombres y Apellidos	Cédula	Observaciones	Firma
D	M	A	Hora	Nombres y Apellidos	Cédula	Observaciones	Firma
D	M	A	Hora	Nombres y Apellidos	Cédula	Observaciones	Firma
D	M	A	Hora	Nombres y Apellidos	Cédula	Observaciones	Firma
D	M	A	Hora	Nombres y Apellidos	Cédula	Observaciones	Firma
D	M	A	Hora	Nombres y Apellidos	Cédula	Observaciones	Firma
D	M	A	Hora	Nombres y Apellidos	Cédula	Observaciones	Firma

Seguridad en Informática - Módulo 8

Docente: Carlos Cagnani

*Este documento fue realizado en concepto de capacitación en Formación Profesional y dictada para el **Sindicato CePETel** a contar del mes de mayo del año 2023.*

Seguridad Informática

CLASE 8 Normativas y Estándares

Indice

Fase Final

- Estándares que describen la visión general y vocabularios
- Estándares que especifican requisitos
- Estándares que describen guías generales
- Estándares que describen guías para sectores específicos
- Estándares de la Serie 27000
- Ley Sarbanes – Oxley (SOX)
- Estándar COSO
- Consideraciones previas a la implementación de ISO / IEC 27001
- Firma Digital
- DNIe

Entorno regulatorio
Seguridad de la Información

Principales organismos de referencia **Internacionales**

- International Organization for Standardization (ISO)
  - La Organización Internacional para la Normalización es un organismo encargado de promover el desarrollo de normas internacionales de **fabricación** (tanto de productos como de servicios), **comercio** y **comunicación** para todas las ramas industriales a excepción de la eléctrica y la electrónica.
  - Su función principal es la de buscar la **estandarización** de normas de productos y seguridad para las empresas u organizaciones (públicas o privadas) a nivel internacional.
  - Las normas desarrolladas por ISO son **voluntarias**, comprendiendo que ISO es un organismo no gubernamental y no depende de ningún otro organismo internacional, por lo tanto, no tiene autoridad para imponer normas a ningún país.

Principales organismos de referencia **Internacionales**

- International Electrotechnical Commission (IEC)
  - La Comisión Electrotécnica Internacional es una organización de normalización en los campos **eléctrico, electrónico** y **tecnologías relacionadas.**
  - Numerosas normas se desarrollan conjuntamente con la ISO (normas ISO/IEC).
  - A la IEC/CEI se le debe el desarrollo y difusión de los estándares para algunas **unidades de medida,** particularmente el gauss, hercio y weber; así como la primera propuesta de un sistema de unidades estándar, el sistema Giorgi, que con el tiempo se convertiría en el sistema internacional de unidades.

Principales organismos de referencia **Internacionales**

- British Standards Institution (BSI / BSI Group)
  - Multinacional cuyo fin se basa en la creación de normas para la **normalización** de procesos.
  - BSI es un organismo **colaborador de ISO** y proveedor de estas normas.
  - Entre sus actividades principales se incluyen la **certificación, auditoría** y **formación** en las normas.
  - BSI es una de las **certificadoras de sistemas de gestión** más importantes del mundo, con mas de 60.000 clientes registrados a nivel internacional, líder en certificación en el Reino Unido y Norte América.

    BSI también es líder en el desarrollo de normas basadas en soluciones de negocio, como la norma **BS 25999 Gestión de Continuidad de Negocio.**

Principales organismos de referencia **Internacionales**

- PCI Security Standards Council (PCI SSC)
  - Foro mundial abierto formado por las principales compañías emisoras de **tarjetas de crédito** (Visa, Mastercard, American Express, JCB y Discover).
  - Está destinado a forzar y facilitar a comercios, proveedores de servicios y bancos a reducir el **riesgo de fraude** con tarjetas de crédito, mediante la protección de las infraestructuras que procesan, transmiten o almacenan datos relativos a tarjetas de crédito.

Principales organismos de referencia **Internacionales**

- National Institute of Standards and Technology (NIST)
  - El Instituto Nacional de Normas y Tecnología (NIST por sus siglas en inglés) es una agencia de la Administración de Tecnología del Departamento de Comercio de los **Estados Unidos**.
  - Su misión es promover la **innovación** y la **competencia industrial** en Estados Unidos mediante avances en patrones de medición (metrología), normas y tecnología con el fin de realzar la productividad, garantizar la estabilidad económica, facilitar el comercio y mejorar la calidad de vida.
  - La **serie 800 del NIST (NIST SP 800)** son una serie de documentos de interés general sobre **Seguridad de la Información**. Estas publicaciones comenzaron en 1990 y son un esfuerzo de industrias, gobiernos y organizaciones académicas para todos los interesados en la seguridad. Además, las guías también pueden consultarse por Categorías y Productos y Templates de Políticas.

Principales organismos de referencia **Internacionales**

- SANS Institute
  - El Instituto SANS (SysAdmin Audit, Networking and Security Institute) es una institución que agrupa a 165.000 profesionales de la seguridad informática (consultores, administradores de sistemas, universitarios, agencias gubernamentales, etc.). Asimismo, es una universidad formativa en el ámbito de las tecnologías de seguridad; y una referencia habitual en la prensa sobre temas de auditoría informática.
  - Sus principales **objetivos** son:
    1. Reunir información sobre todo lo referente a seguridad informática (OS, routers, firewalls, aplicaciones, IDS, etc.).
    2. Ofrecer capacitación y certificación en el ámbito de la seguridad informática.

Principales organismos de referencia **Internacionales**

- Information Systems Audit and Control Association (ISACA)
  - La Asociación de Auditoría y Control de Sistemas de Información (ISACA) es una asociación internacional que apoya y patrocina el desarrollo de metodologías y certificaciones para la realización de actividades de auditoría y control en **sistemas de información.**
  - Está formada por más de 100.000 miembros y profesionales con certificaciones ISACA distribuidos en unos 160 países (formando una red de 170 capítulos). Trabajan en casi todas las categorías de la industria y sus capítulos proporcionan educación y formación constante, recursos compartidos, promoción, creación de redes y otros beneficios.
  - Son los custodios del framework **COBIT** (Control Objectives for Information and related Technology), los creadores del **ITGI** (IT Governance Institute), y han desarrollado cuatro certificaciones profesionales: **CISA** (Certified Information Systems Auditor), **CISM** (Certified Information Security Manager), **CGEIT** (Certified in the Governance of Enterprise IT), **CRISC** (Certified in Risk and Information Systems Control).

Principales organismos de referencia
Argentina

Argentina

- Infraestructuras Críticas de Información y Ciberseguridad (ICIC)
- Coordinanción de Emergencias en Redes Teleinformáticas de la República Argentina (CERT).
- Policía Federal – División Delitos Tecnológicos.
- Policía Metropolitana – Investigaciones Telemáticas.
- Fiscalía de Delitos Informáticos de CABA.
- Dirección Nacional de Protección de Datos Personales (DNPDP).
- Instituto Nacional contra la Discriminación, la Xenofobia y el Racismo (INADI).
- Subsecretaría de Tecnologías de Gestión – AgendaDigital

Principales normas y reglamentos

Internacionales

- ISO 27001 – Sistemas de Gestión de la Seguridad de la Información
- ISO 22301 – Sistemas de Gestión de la Continuidad del Negocio
- ISO 20000 – Sistemas de Gestión de Servicios de TI
- ISO 9000 – Sistemas de Gestión de la Calidad
- ISO 14000 – Sistemas de Gestión Ambiental
- Payment Card Industry – Data Security Standard (PCI-DSS)
- Sarbanes-Oxley Act (SOX)

Principales normas y reglamentos
Argentina

- Protección de Datos Personales
  - La Ley **25.326** de Protección de los Datos Personales (incluye artículos vetados por Decreto Nº 955/2000 y las modificaciones introducidas por las Leyes.

    26.343 y 26.388) tiene por objeto la protección integral de los datos personales asentados en archivos, registros, bancos de datos u otros medios técnicos de tratamiento de datos, sean estos públicos o privados destinados a dar informes para garantizar el derecho al honor y a la intimidad de las personas, así como también el acceso a la información que sobre las mismas se registre, de conformidad a lo establecido en el artículo 43, párrafo tercero de la Constitución Nacional.
  - El **Decreto 1.558/2001** reglamenta la Ley de Protección de los Datos Personales.

Principales normas y reglamentos

Argentina

- Delitos informáticos
  - La norma de referencia es la **Ley 26.388** de Delitos Informáticos (Sancionada el 4 de junio de 2008. Promulgada de Hecho el 24 de junio de 2008). No es una ley especial, que regula este tipo de delitos en un cuerpo normativo separado del Código Penal (CP) con figuras propias y específicas, sino una ley que modifica, sustituye e incorpora figuras típicas a **diversos artículos del CP** actualmente en vigencia, con el objeto de regular las nuevas tecnologías como medios de comisión de delitos previstos en el CP.

Principales normas y reglamentos

Argentina

A lo largo de su articulado tipifica, entre otros, los siguientes **delitos informáticos**:

1. Pornografía infantil por internet u otros medios electrónicos (art. 128 CP).
2. Violación, apoderamiento y desvío de comunicación electrónica (art. 153, párrafo 1º CP).
3. Intercepción o captación de comunicaciones electrónicas o telecomunicaciones (art. 153, párrafo 2º CP).

Acceso a un sistema o dato informático (artículo 153 bis CP).

5. Publicación de una comunicación electrónica (artículo 155 CP).
6. Acceso a un banco de datos personales (artículo 157 bis, párrafo 1º CP).
7. Revelación de información registrada en un banco de datos personales (artículo 157 bis, párrafo 2º CP).
8. Inserción de datos falsos en un archivo de datos personales (artículo 157 bis, párrafo 2º CP; anteriormente regulado en el artículo 117 bis, párrafo 1º, incorporado por la Ley de Hábeas Data).
9. Fraude informático (artículo 173, inciso 16 CP).
10. Daño o sabotaje informático (artículos 183 y 184, incisos 5º y 6º CP).

Principales normas y reglamentos
Argentina

- Grooming
  - **Ley 26.904** de Grooming, que incorpora el art. 131 del Código Penal que pena con prisión de 6 meses a 4 años el que, por medio de comunicaciones electrónicas, telecomunicaciones o cualquier otra tecnología de transmisión de datos, contacte a una **persona menor de edad**, con el propósito de cometer cualquier delito contra la integridad sexual de la misma.

- Plan Nacional de Gobierno Electrónico
  - La norma de referencia es el **Decreto 378/2005**.

Leyes, regulaciones y órganos de normalización
Argentina

- Órganos de normalización y autoridades de control
  - IRAM (Instituto Argentino de Normalización y Certificación): www.iram.org.ar
  - Centro de Protección de Datos de la Ciudad de Buenos Aires: www.cpdp.gov.ar
  - Dirección Nacional de Protección de Datos Personales: www.jus.gov.ar/datos-personales.aspx
- Leyes y regulaciones de interés
  - Ley 25.326 de Protección de Datos (Habeas Data) del 2 noviembre de 2000.
  - Decreto 1558/2001, Reglamentación de la ley de Protección de Datos.
- Proyectos
  - Anteproyecto de Ley de Delitos Informáticos. Resolución nº 476/2001 de 21 de noviembre de 2001.
  - Proyecto de Ley sobre protección del correo electrónico de 24 de julio de 2002.

Ley Sarbanes – Oxley (SOX)

Ley Sarbanes – Oxley (SOX)

INTRODUCCIÓN Y ANTECEDENTES

La ley Sarbanes-Oxley Act del 2002 constituyó un hito en la protección de la confiabilidad de la información pública (estados financieros).

Algunos la han llamado “La reforma de la contabilidad de las compañías públicas” y otros “La protección del inversionista de 2002”.

SOX fue redactada por dos congresistas que le dieron el nombre (Sarbanes y Oxley) y fue aprobada como ley, el 30 de julio de 2002, por el presidente de los EEUU, George Bush.

Esta nueva ley surge como resultado de los escándalos financieros corporativos desencadenados con el caso Enron, Worldcom y otros, los cuales implicaron fraudes millonarios y, en consecuencia, catástrofes financieras, inclusive entre los inversores y compañías que nada tenían que ver con los ilícitos.

Ley Sarbanes – Oxley (SOX)

Se agrupa en seis áreas:

1. MEJORA EN LA CALIDAD DE LA INFORMACIÓN PÚBLICA Y EN LOS DETALLES DE LA MISMA.

2. REFORZAMIENTO DE RESPONSABILIDADES EN EL GOBIERNO CORPORATIVO DE LAS SOCIEDADES.

3. MEJORA EN LAS CONDUCTAS Y COMPORTAMIENTOS ETICOS EXIGIBLLES: MAYORES EXIGENCIAS DE RESPONSABILIDAD EN LOS TEMAS DE GESTIÓN INDEBIDA DE INFORMACION CONFIDENCIAL.

4. AUMENTO DE LA SUPERVISION A LAS ACTUACIONES EN LOS MERCADOS COTIZADOS.

5. INCREMENTO DEL REGIMEN SANCIONADOR ASOCIADO A INCUMPLIMIENTOS.

6. AUMENTO DE EXIGENCIA Y PRESIÓN SOBRE LA INDPENDENCIA EFCTIVA DE LOS AUDITORES.

Ley Sarbanes – Oxley (SOX)

1. MEJORA EN LA CALIDAD DE LA INFORMACIÓN PÚBLICA Y EN LOS DETALLES DE LA MISMA.

La información Pública presentada deberá ser legitimada por los directivos de la sociedad.

-Evaluación del control interno financiero: valorado, documentado y certificado por la dirección de la sociedad y auditado por el auditor de cuentas.

-Los cambios en formación publica de la sociedad, que tenga impacto potencial significativo, en la situación financiera o en las operaciones, deberán ser informados de forma mucho más rápida y efectiva.

Ley Sarbanes – Oxley (SOX)

2. REFORZAMIENTO DE RESPONSABILIDADES EN EL GOBIERNO CORPORATIVO DE LAS SOCIEDADES

-Incremento de comunicaciones directas entre el Auditor y el comité de Auditoría en materias como: políticas contables significativas, tratamientos contables alternativos, etc.

-Regulaciones para los comités de Auditoría: - serán responsables directos en designar, retribuir y supervisar al auditor.

-Sus miembros deberán ser consejeros independientes, no ejecutivos.etc.

-Obligación de contar con expertos financieros en el comité de Auditoría e informar explícitamente sobre quienes con los consejeros con esta experiencia.

Ley Sarbanes – Oxley (SOX)

3. MEJORA EN LAS CONDUCTAS Y COMPORTAMIENTOS ETICOS EXIGIBLLES: MAYORES EXIGENCIAS DE RESPONSABILIDAD EN LOS TEMAS DE GESTIÓN INDEBIDA DE INFORMACION CONFIDENCIAL

-es ilegal la actuación de cualquier consejero o directivo destinado a influir de forma fraudulenta o confundir al auditor.

-las operaciones realizadas por los agentes que pueden disponer de información reservada están Sometidas a una exigencia de información a los mercados en tiempo muy corto y de forma veraz.

-Obligatoriedad de un código de Ética para los Ejecutivos del Área financiera. Los cambios o incumplimientos al Código deben ser informados públicamente.

-Protección especial para los denunciantes anónimos de conducta ilícitos e irregularidades de la sociedad.

Ley Sarbanes – Oxley (SOX)

4. AUMENTO DE LA SUPERVISION A LAS ACTUACIONES EN LOS MERCADOS COTIZADOS.

-Creación de un organismo público de supervisión: el Public Company Acounting Oversight Board (PACAOB).

-El PACAOB desarrollara programas continuos de supervisar del trabajo de las firmas de auditoría.

-La SEC podrá reconocer los principios contables establecidos por organismos reguladores como el FASB

-Los emisores de valores en los mercados americanos contribuirán mediantes cuotas según las actividades del PCAOB y del FASB.

-La SEC ampliara las revisiones periódicas sobre los depósitos de las compañías.

Ley Sarbanes – Oxley (SOX)

5. INCREMENTO DEL REGIMEN SANCIONADOR ASOCIADO A INCUMPLIMIENTOS.

-Deberán reintegrarse los incentivos cobrados o los beneficios realizados en la venta de acciones por el Consejero Delegado (CEO) o por el Director Financiero (CFO).

-Extensión de los plazos en que puede perseguirse un fraude cometido y/o identificado.

-Obligación para CEO y CFO de certificar su buena fe en cuanto a que los informes públicos periódicos.

-Responsabilidades penales por manipular, alterar o destruir documentos.

-Aumento importante de las sanciones a los contables/financieros por no testificar, facilitar información.

Ley Sarbanes – Oxley (SOX)

6. AUMENTO DE EXIGENCIA Y PRESIÓN SOBRE LA INDPENDENCIA EFCTIVA DE LOS AUDITORES.

-Prohibición total para que el auditor de cuentas pueda prestar determinados servicios a sus clientes de auditoria.

-El comité de Auditoria deberá autorizar, de forma previa la contratación de los servicios del auditor de cuentas.

-El socio firmante y el socio revisor deberán rotar cada 5 años.

-se establecen restricciones a la contratación del personal de auditoria.

Ejemplo: se establece un periodo de enfriamiento de un año en el que no se puedan reproducir estas contrataciones

para puestos de relación directa con la supervisión financiera de la información del emisor

Financial Accounting Standards Board (FASB)

The Financial Accounting Standards Board (FASB) is an independent nonprofit organization responsible for establishing accounting and financial reporting standards for companies and nonprofit organizations in the United States, following generally accepted accounting principles (GAAP).

The FASB was formed in 1973 to succeed the Accounting Principles Board and carry on its mission. It is based in Norwalk, Conn.

U.S. Securities & Exchange Commission (SEC)

Estándar COSO

Estándar COSO

The Committee of Sponsoring Organizations of the Treadway Commission (COSO)

Es una iniciativa conjunta de cinco organizaciones profesionales y se dedica a ayudar a las organizaciones a mejorar su rendimiento mediante el desarrollo de un liderazgo de pensamiento que mejore el control interno, la gestión de riesgos, el gobierno y la disuasión del fraude.

Estándar COSO

El Informe COSO es un documento que contiene las principales directivas para la implantación, gestión y control de un sistema de control.

Debido a la gran aceptación de la que ha gozado, desde su publicación en 1992, el Informe COSO se ha convertido en el estándar de referencia.

Existen en la actualidad 2 versiones del Informe COSO.

La versión del 1992 y la versión del 2004, que incorpora las exigencias de ley Sarbanes Oxley a su modelo.

Esta diseñado para identificar los eventos que potencialmente puedan afectar a la entidad y para administrar los riesgos, proveer seguridad razonable para la administración y para la junta directiva de la organización orientada al logro de los objetivos del negocio.

Estándar COSO

COSO II

Hacia fines de Septiembre de 2004, como respuesta a una serie de escándalos, e irregularidades que provocaron pérdidas importantes a inversionistas, empleados y otros grupos de interés.

Nuevamente el Committee of Sponsoring Organizations of the Treadway Commission, publicó el Enterprise Risk Management – Integrated Framework y sus aplicaciones técnicas asociadas.

Amplía el concepto de control interno, proporcionando un foco más robusto y extenso sobre la identificación, evaluación y gestión integral de riesgo.

En septiembre de 2004 se publica el estudio ERM (Enterprice Risk Management) como una ampliación de Coso 1, de acuerdo a las conclusiones de los servicios de Pricewaterhouse a la comision.

Estándar COSO

Que se puede Obtener a través de COSO?

- Proporciona un marco de referencia aplicable a cualquier organización.
- Para COSO, este proceso debe estar integrado con el negocio, de tal manera que ayude a conseguir los resultados esperados en materia de rentabilidad y rendimiento.
- Trasmitir el concepto de que el esfuerzo involucra a toda la organización: Desde la Alta Dirección hasta el último empleado.

Estándar COSO

Ventajas de Coso

- Permite a la dirección de la empresa poseer una visión global del riesgo y accionar los planes para su correcta gestión.
- Posibilita la priorización de los objetivos, riesgos clave del negocio, y de los controles implantados, lo que permite su adecuada gestión, toma de decisiones más segura, facilitando la asignación del capital.
- Alinea los objetivos del grupo con los objetivos de las diferentes unidades de negocio, así como los riesgos asumidos y los controles puestos en acción.
- Permite dar soporte a las actividades de planificación estratégica y control interno.
- Permite cumplir con los nuevos marcos regulatorios y demanda de nuevas prácticas de gobierno corporativo.
- Fomenta que la gestión de riesgos pase a formar parte de la cultura del grupo.

GPDR

General Data Protection Regulation

GDPR

¿Qué es GDPR?

GDPR, del inglés, General Data Protection Regulation o, en español, Reglamento General de Protección de Datos. Ella es una ley creada por la Unión Europea que garantiza la protección y privacidad de datos de los usuarios.

Ella es consecuencia de la cuarta revolución industrial y del rápido avance de la tecnología, de la globalización y del flujo internacional de datos personales cada vez mayor. Esa ley reglamenta cómo las empresas deben tratar los datos personales de millares de usuarios que acceden sus redes.

GDPR determina 6 elementos que las empresas deben respetar y seguir al procesar información personal. Continúe leyendo y descubre cuáles son y porqué debes implementar en tu sitio.

GDPR

¿Qué es reglamentación GDPR?

Ella reglamenta el procesamiento de los datos de usuarios individuales de UE, lo que puede incluir colecta, almacenamiento, transferencia, uso y hasta mismo exclusión de eses datos. Esa ley es aplicada en empresas con y sin presencia física en territorio europeo, basta que el sitio de la empresa atienda a los usuarios de la unión para que se sometan a la reglamentación.

Debido a las diferentes aplicaciones posibles la reglamentación divide las organizaciones entre “controladoras” y “procesadoras”. La primeira son las organizaciones que detienen los datos, mientras que las segundas se ocupan apenas de procesarlos siguiendo los comandos de las controladoras. La ley se aplica para los dos tipos de organización.

GDPR

¿Cómo GDPR afecta mi empresa en América Latina?

Caso tu empresa guarde, procese información personal, realice transacciones comerciales u ofrezca productos y servicios a la Unión Europea precisas seguir las reglas de la GDPR.Procesar información personal significa operar com cualquier dato que identifique el usuario como único. Por ejemplo, desde la activación de cookies en el navegador hasta el rastreo de comportamiento de eses usuarios por CRM, es preciso adecuarse a la ley, una vez que esas actividades son pasibles de identificación.

GDPR

¿Qué ocurre con la empresa que no cumplir com la GDPR?

Quién no cumplir la ley será multado entre dos niveles posibles de castigo. El primero castigo implica en una multa de hasta 10 millones de euros o 2% de la facturación anual global, lo que sea mayor. La multa en el segundo nivel es de hasta 20 millones de euros o 4% de la facturación anual global, también conforme con lo que sea mayor. De manera general, la primera multa es destinada a la violación de controladores y procesadores, mientras que la violación de privacidad de los datos de los usuarios resulta en la multa de mayor valor.Hay diversos criterios que se deben tener en cuenta para ser determinado el valor de la multa, tales como naturaleza, gravedad y duración de la infracción. Las autoridades que definen la multa pueden aún considerar los tipos de datos afectados, las infracciones previas y el nivel de cooperación de la empresa infractora.

GDPR

Guía de implementación de la GDPR

Los 6 elementos que tu empresa deberá seguir son:

1 Transparencia

Tu empresa debe tratar datos personales dentro de la ley, de manera justa y transparente. Eso significa decir que precisas siempre notificar que estás recolectando información y debe, aún, especificar cuál información y cómo ella será utilizada.

GDPR

Guía de implementación de la GDPR

Los 6 elementos que tu empresa deberá seguir son:

2 Propósito Delimitado

Tu empresa debe recolectar apenas datos específicos con intenciones específicas. Jamás puedes procesar información más allá de las que contemplan las intenciones específicas e informadas al usuario.

GDPR

Guía de implementación de la GDPR

Los 6 elementos que tu empresa deberá seguir son:

3 Minimización de datos

Así como en el propósito delimitado, puedes apenas recolectar datos personales adecuados y relevantes para tus intenciones. Eso significa que recolectar o cuestionar cualquier información no relacionada al servicio ofrecido es prohibido. Por ejemplo, al descargar algo, el desarrollador no debe acceder la localización exacta o la agenda de contactos del usuario si no fueren relevantes para el servicio fornecido por la aplicación o si el usuario no permitir.

GDPR

Guía de implementación de la GDPR

Los 6 elementos que tu empresa deberá seguir son:

4 Eliminación de Datos

Los datos personales de los usuarios solo deben ser mantenidos mientras son necesarios y sean útiles para el propósito original. Por ejemplo, al cerrar una cuenta en el banco, es deber de la organización deletar toda información del usuario que no tenga un propósito legítimo.

GDPR

Guía de implementación de la GDPR

Los 6 elementos que tu empresa deberá seguir son:

5 Precisión

Todo dato personal que recolectar debe ser correcto, claro y, cuando necesario, ser actualizado para estar en día con la información personal del usuario.

GDPR

Guía de implementación de la GDPR

Los 6 elementos que tu empresa deberá seguir son:

6 Seguridad

Organizaciones deben usar técnicas apropiadas y medidas de seguridad para proteger datos personales contra el procesamiento no autorizado o vaciamiento. Acceso, pérdida o alteración indebida de los datos implica en penalidades. Dependiendo del caso, es recomendado, cuando no obligatorio, el uso de datos segregados, criptografados, seudonimizados o anonimizados.

Índice de temas

1. Certificados y Firma Digital
2. Documento Nacional de Identidad Electrónico DNIe
3. Procedimiento de Firma Digital
4. Caso de Uso
5. Firma Digital en Argentina

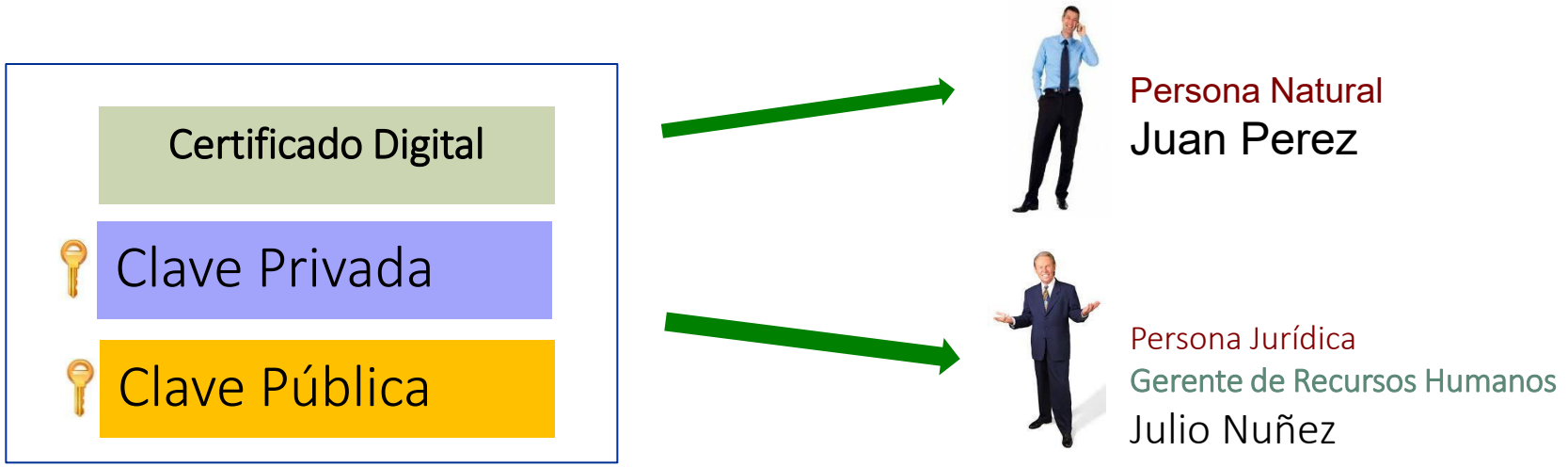
Certificados Digitales

y Firma Digital

Certificados Digitales y Firma Digital

Certificado digital

Es un documento digital emitido por una entidad autorizada o Entidad de Certificación (EC). El certificado digital vincula un par de claves (una pública y otra privada) con una persona y asegura su identidad digital. Con esta identidad digital la persona podrá ejecutar acciones de comercio y gobierno electrónico con seguridad, confianza y pleno valor legal.



¿Qué nos permite hacer un certificado digital?

Dependiendo del tipo de certificado, éste nos permitirá: autenticarnos en un servicio electrónico o firmar digitalmente documentos electrónicos.

Autenticación

Firma digital

Certificados Digitales y Firma Digital

Medios portadores de certificados digitales y dispositivos para lectura

Tarjeta criptográfica

Lector de tarjeta

Token criptográfico

Instalado en el Equipo

Funciones de la firma manuscrita

Sus funciones son: Vincular, identificar, autenticar y preservar la integridad. La consecuencia de estas funciones genera el no repudio del documento firmado.

Firma electrónica

Se trata de cualquier símbolo o carácter, conjunto de símbolos o caracteres basados en medios electrónicos que cumple con alguna de las funciones de la firma manuscrita.

Certificados Digitales y Firma Digital

Firma Digital

Es aquella firma electrónica que utilizando una técnica de criptografía asimétrica, permite la identificación del signatario y ha sido creada por medios que éste mantiene bajo su control, de manera que está vinculada únicamente al signatario y a los datos a los que refiere, lo que permite garantizar la integridad del contenido y detectar cualquier modificación ulterior, tiene la misma validez y eficacia jurídica que el uso de una firma manuscrita, siempre y cuando haya sido generada por un Prestador de Servicios de Certificación Digital debidamente acreditado que se encuentre dentro de la Infraestructura Oficial de Firma Electrónica - IOFE, y que no medie ninguno de los vicios de la voluntad previstos en el Título VIII del Libro II del Código Civil.

Fuente: Decreto Supremo Nº 026-2016-PCM; Aprueban medidas para el fortalecimiento de la infraestructura oficial de firma electrónica y la implementación progresiva de la firma digital en el Sector Público y Privado (Articulo 6 – De la Firma Digital)

Certificados Digitales y Firma Digital

… Firma Digital

Las firmas digitales son las generadas a partir de certificados digitales que son:

a) Emitidos conforme a lo dispuesto en el presente Reglamento por Entidades de Certificación acreditadas ante la Autoridad Administrativa Competente.

b) Incorporados a la Infraestructura Oficial de Firma Electrónica bajo acuerdos de certificación cruzada, conforme al artículo 73 del presente Reglamento.

c) Reconocidos al amparo de acuerdos de reconocimiento mutuo suscritos por la Autoridad Administrativa Competente conforme al artículo 71 del presente Reglamento.

d) Emitidos por Entidades de Certificación extranjeras que hayan sido incorporados por reconocimiento a la Infraestructura Oficial de Firma Electrónica conforme al artículo 72 del presente Reglamento"

Fuente: Decreto Supremo Nº 026-2016-PCM; Aprueban medidas para el fortalecimiento de la infraestructura oficial de firma electrónica y la implementación progresiva de la firma digital en el Sector Público y Privado (Articulo 6 – De la Firma Digital)

Funciones de la firma digital

Tiene como funciones las mismas que la firma manuscrita, es decir:

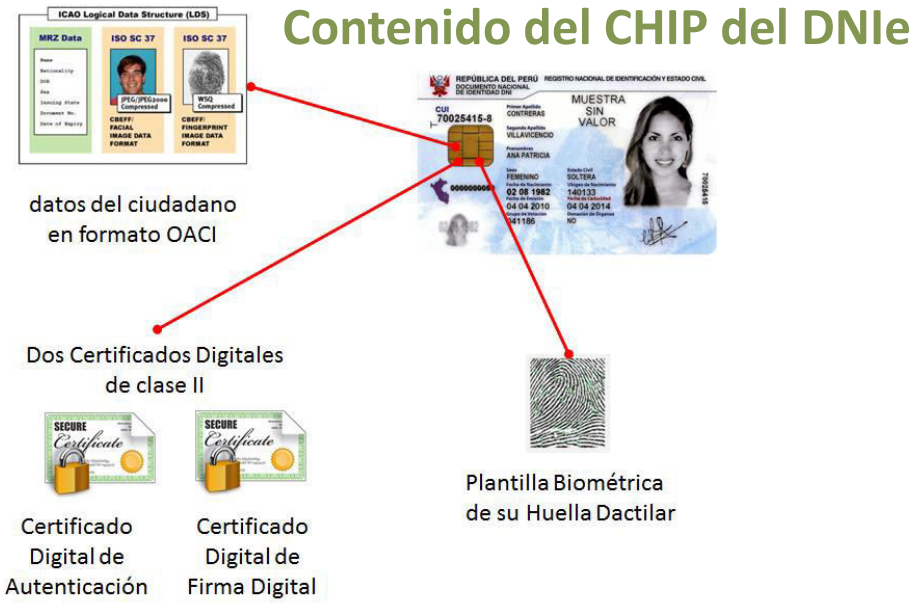
- identificar (a la persona que firma),
- vincular (al documento con la persona que lo firma),
- autenticar (el documento que será firmado) y
- preservar la integridad (no alterar el documento firmado).

La consecuencia de estas funciones genera el no repudio del documento firmado.

Documento Nacional de Identidad Electrónico (DNIe)

Documento Nacional de identidad Electrónico (DNIe)

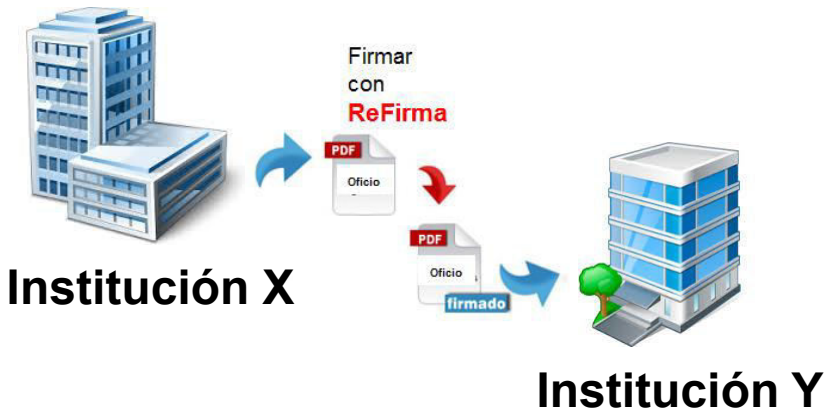
El DNI electrónico o DNIe es el Documento Nacional de Identidad que acredita presencial y electrónicamente la identidad de su titular. El DNIe consiste en un dispositivo de almacenamiento electrónico (tarjeta inteligente) que alberga los principales datos que permiten la identificación del ciudadano y además contiene un certificado digital, permitiendo al ciudadano el acceso a servicios de gobierno y comercio electrónico.



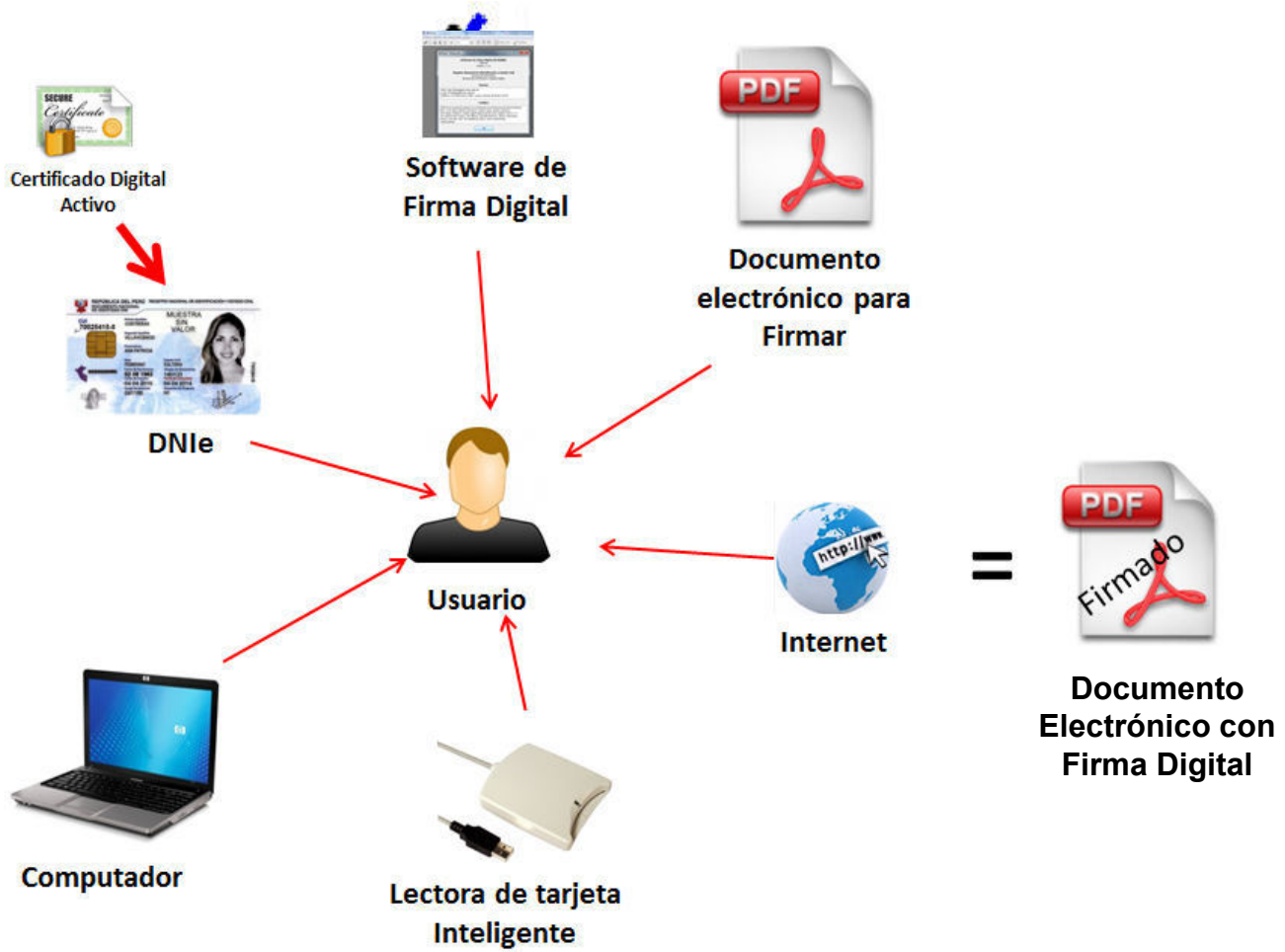
Proceso de Firma Digital

Caso práctico

Firma de un documento electrónico con el software Refirma

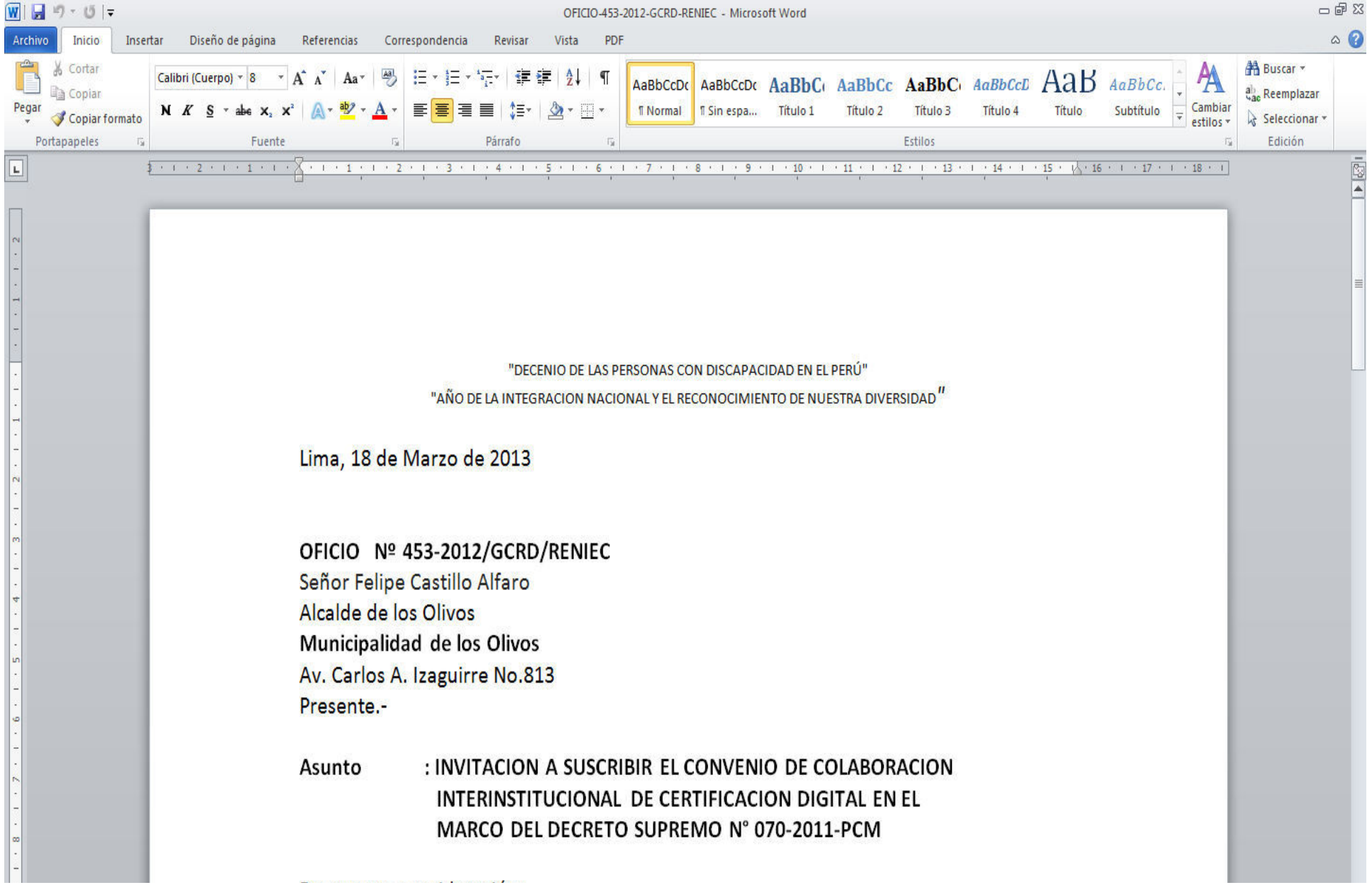


Requerimientos para Firmar un Documento Electrónico

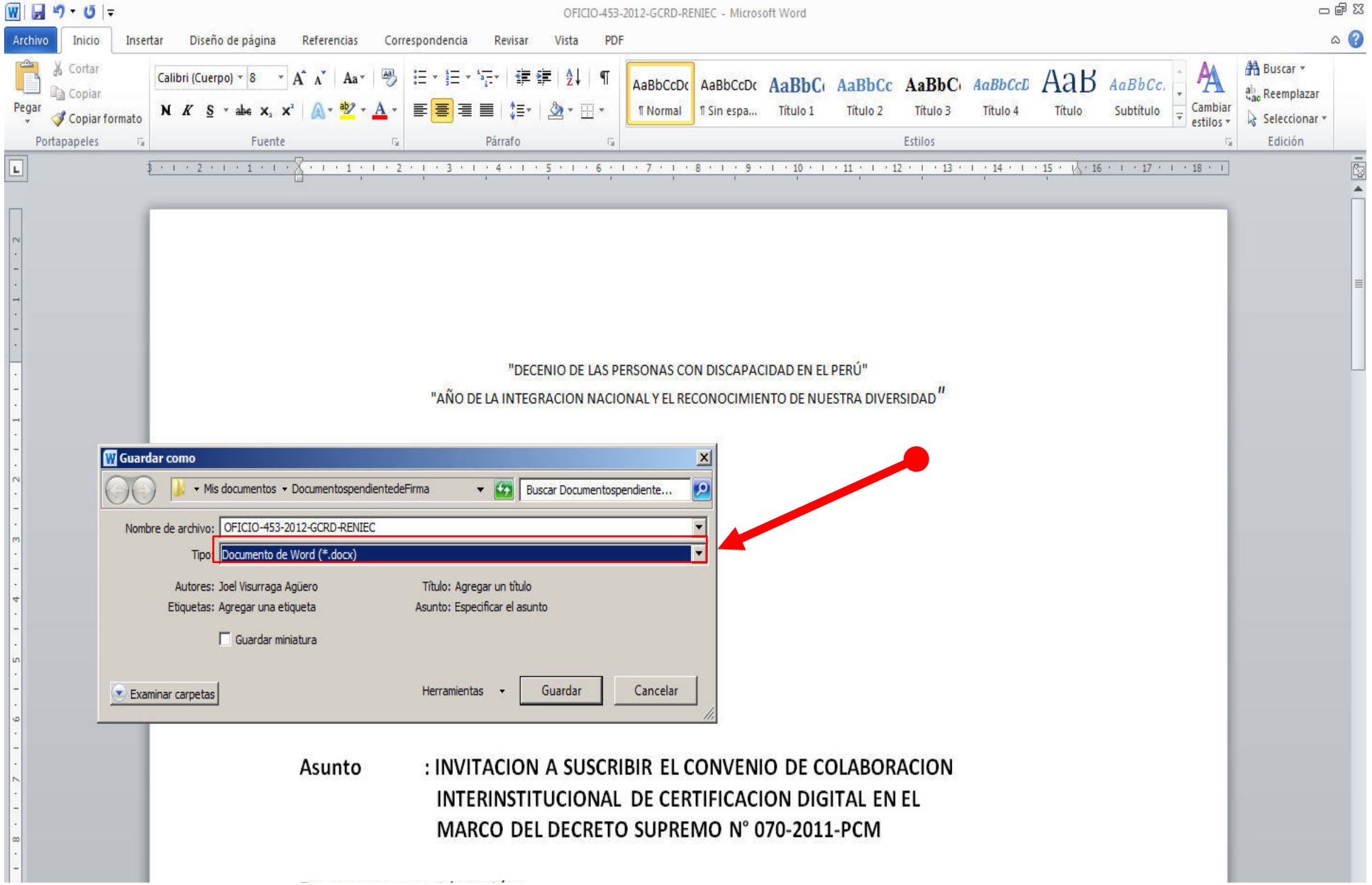


Paso 1

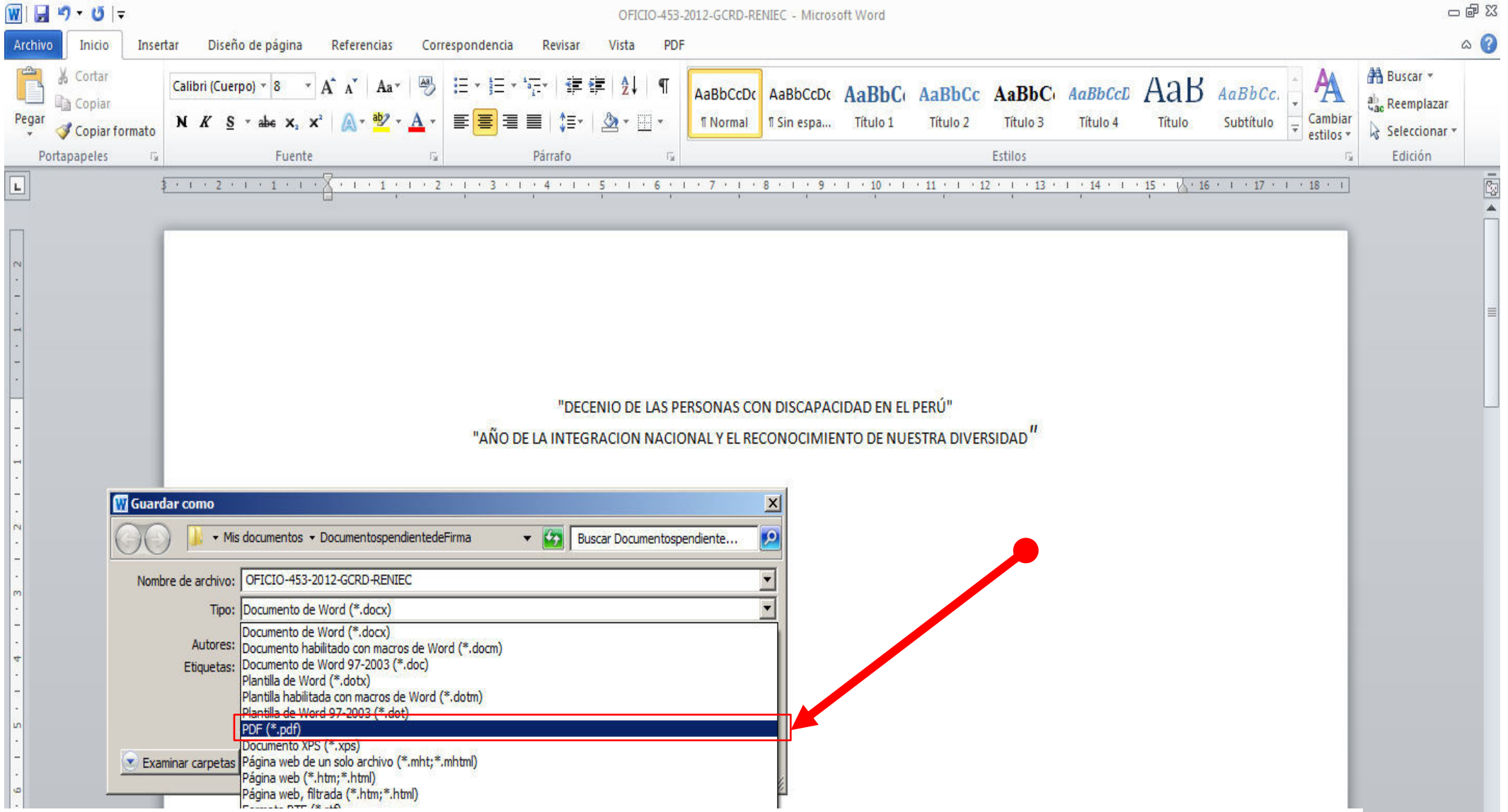
Elaboración del documento electrónico que será enviado a la Empresa x



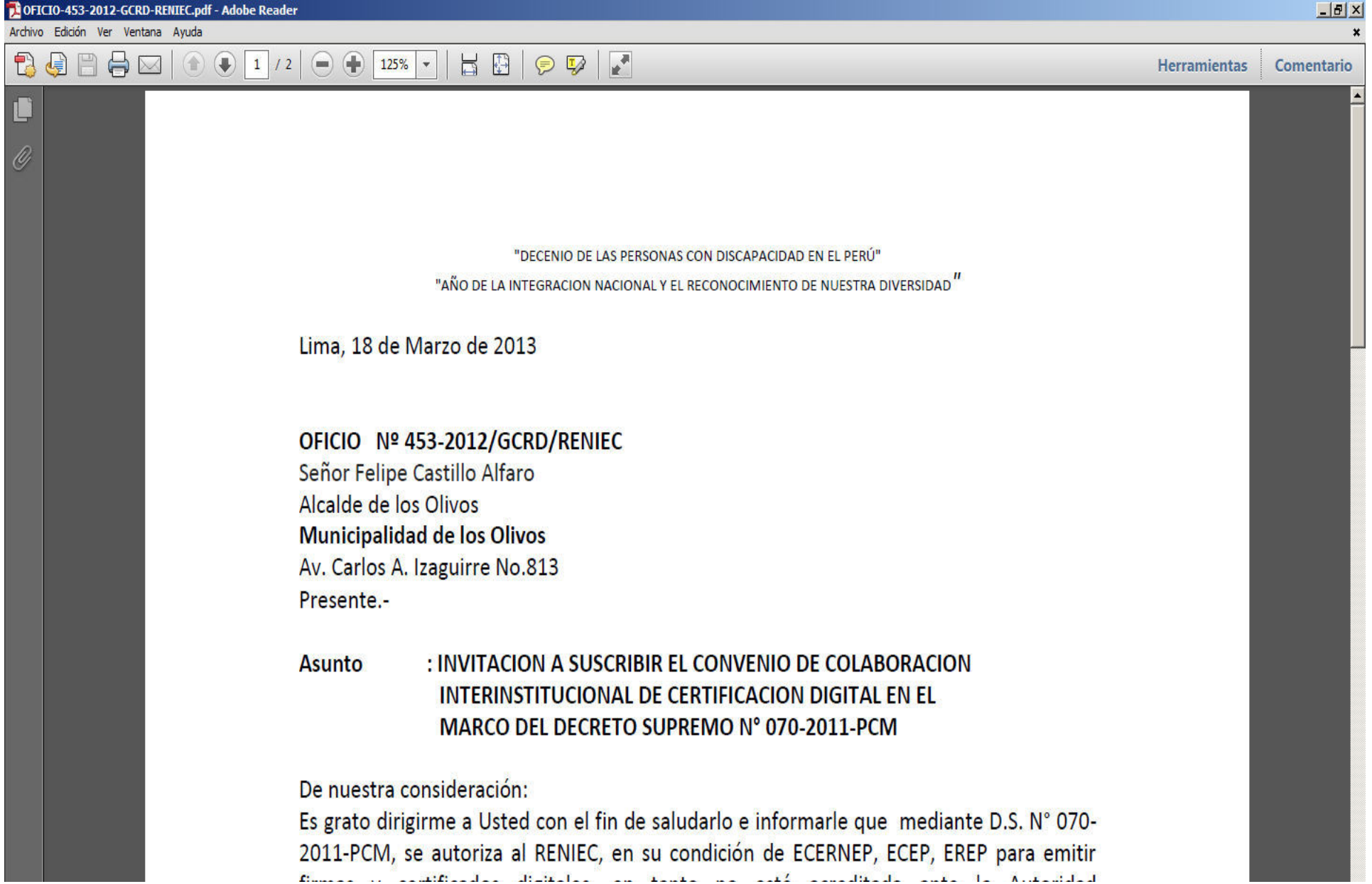
Se elabora el documento electronico utilizando un procesador de textos. En este caso utilizamos Microsoft Word versión 11.0.



Se guarda el documento elaborado en formato word ".doc«



Debido a que el software de firma digital que usaremos, firma documentos sólo en formato ".pdf" debemos convertirlo de ".doc" a ".pdf«. Para esto guardaremos el documento seleccionando el formato “.pdf”.



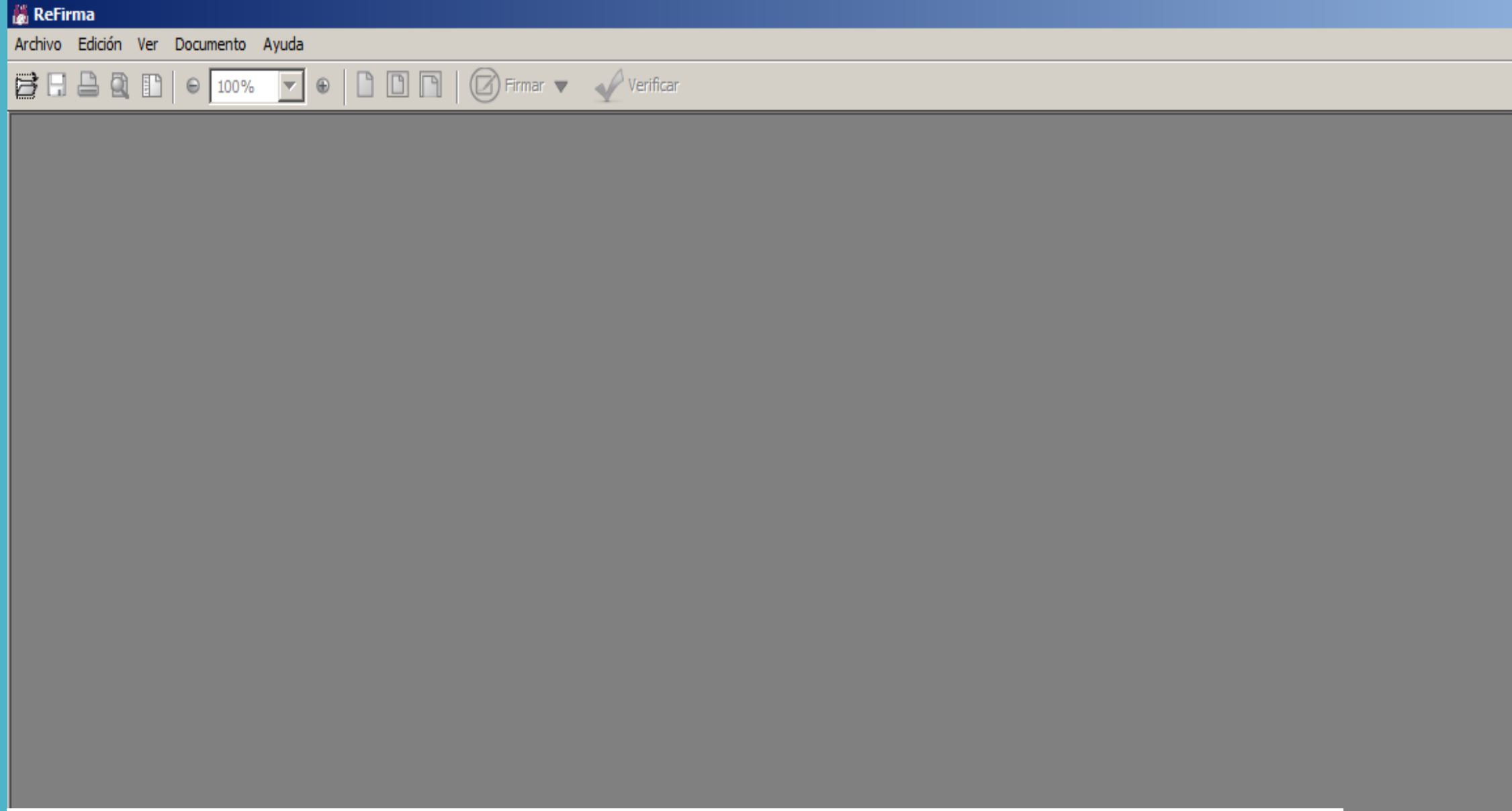
Ahora se cuenta con el documento ".pdf" que podrá ser firmado digitalmente.

Paso 2

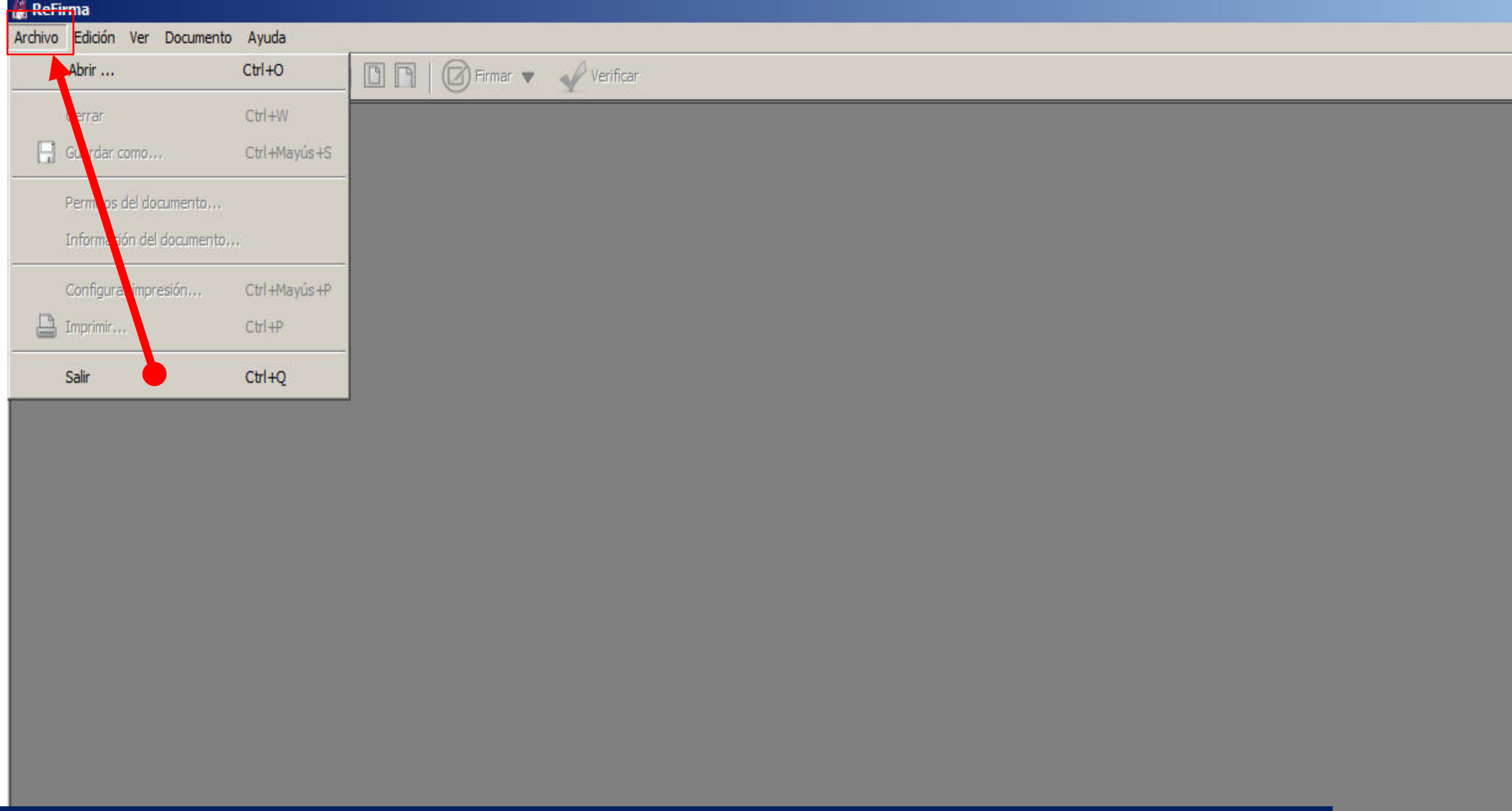
Firma Digital del documento electrónico que será enviado a la Empresa Y

Ubicamos el ícono del software de firma digital "ReFirma 1.1.0" en el escritorio del computador y damos doble click para ejecutar el software.

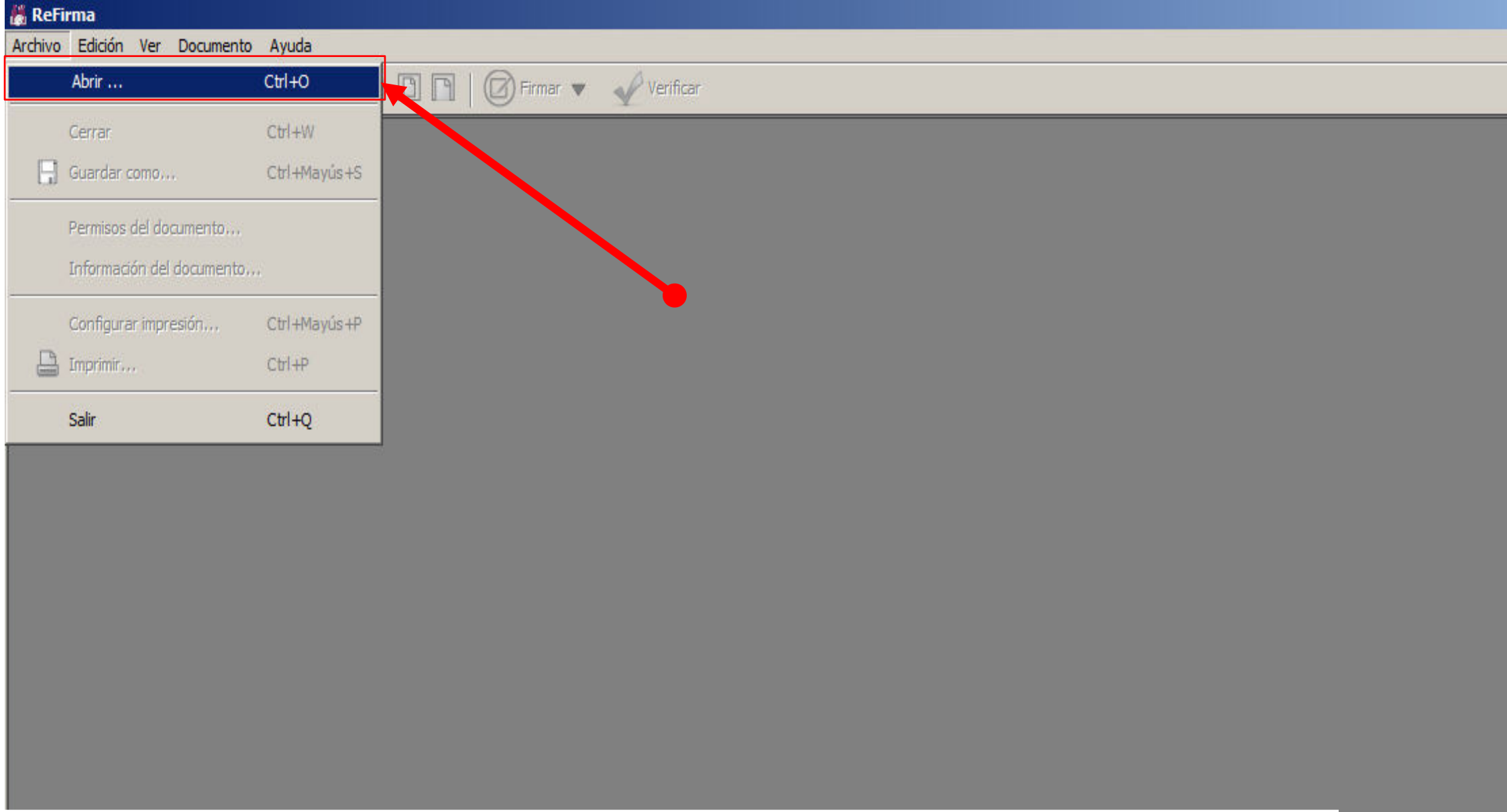
Ubicamos el ícono del software de firma digital "ReFirma 1.1.0" en el escritorio del computador y damos doble click para ejecutar el software.



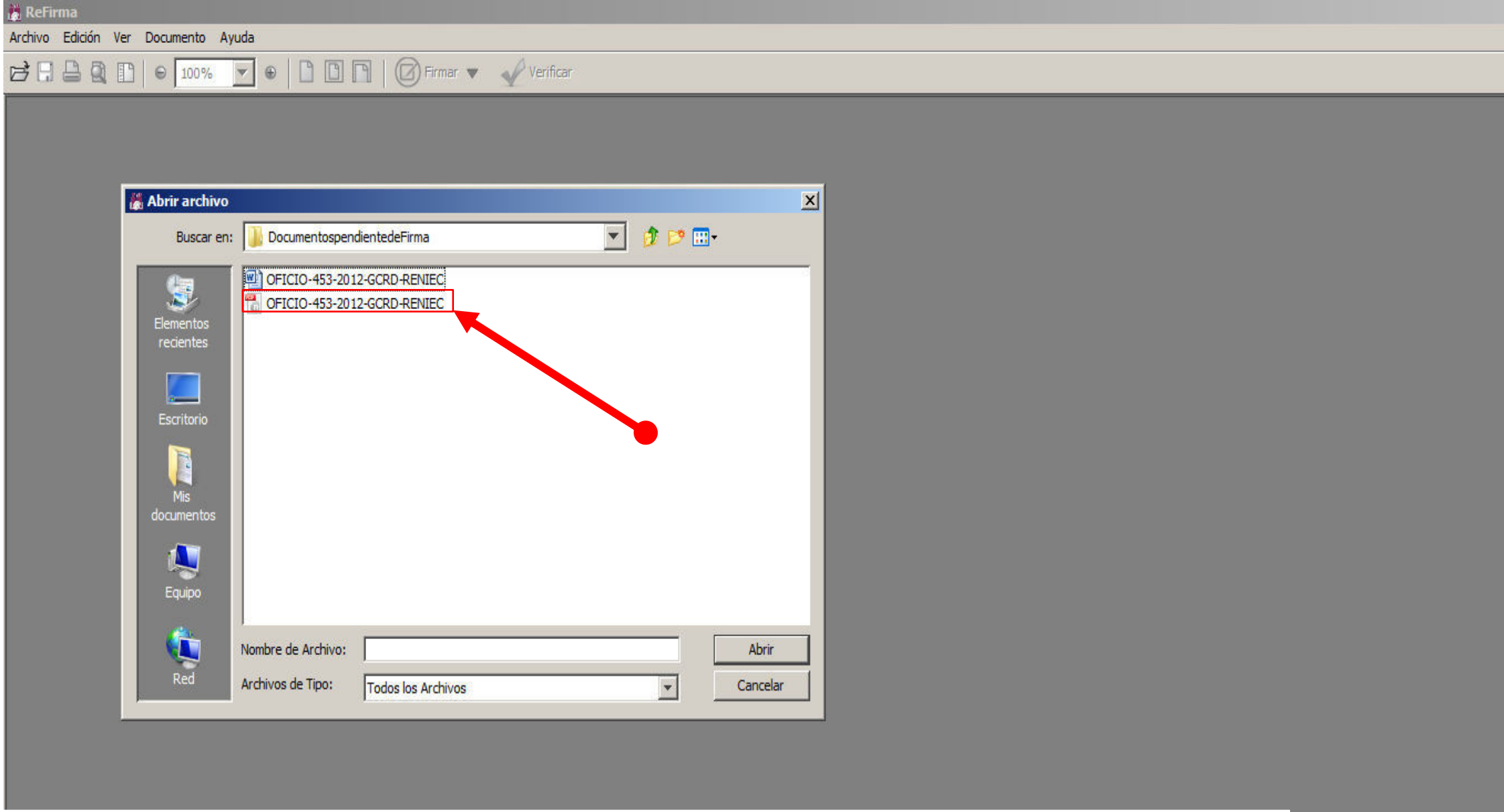
A continuación se muestra la ventana principal del software de firma digital "ReFirma 1.1.0".



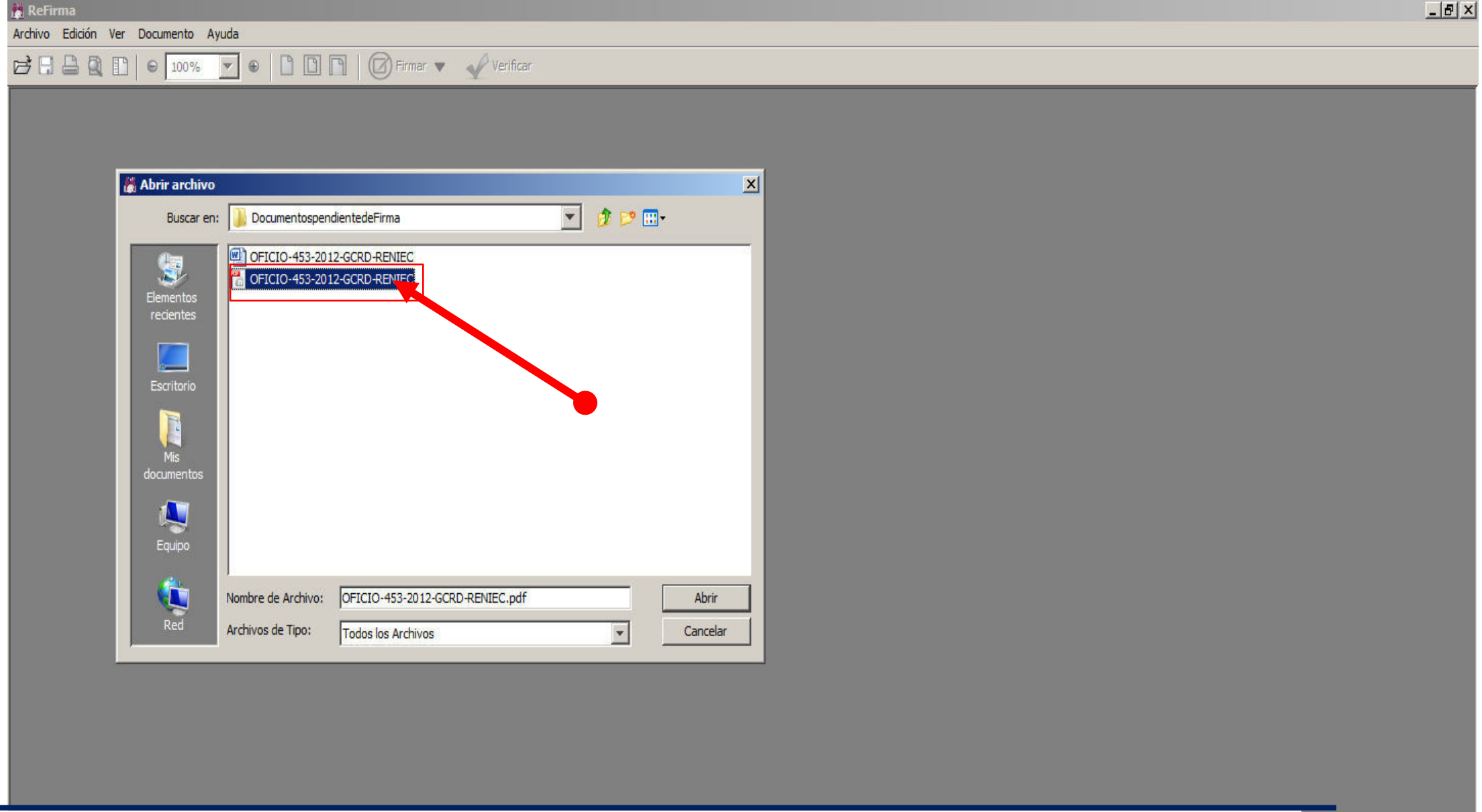
Ubicamos la opción <Archivo> en la barra del menú principal y damos clik para que se desplieguen las sub opciones.



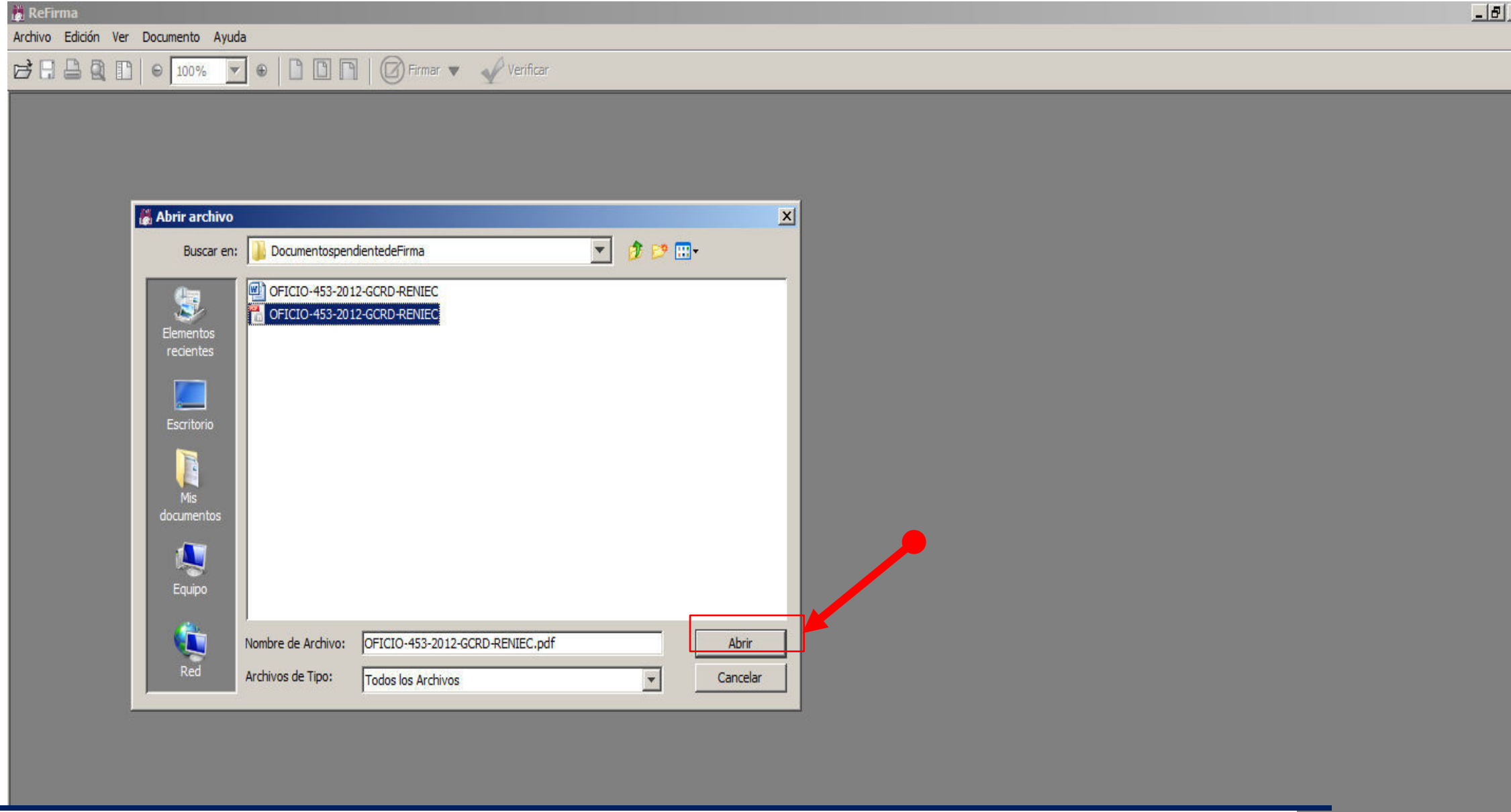
Ubicamos la subopción <Abrir> y le damos click.



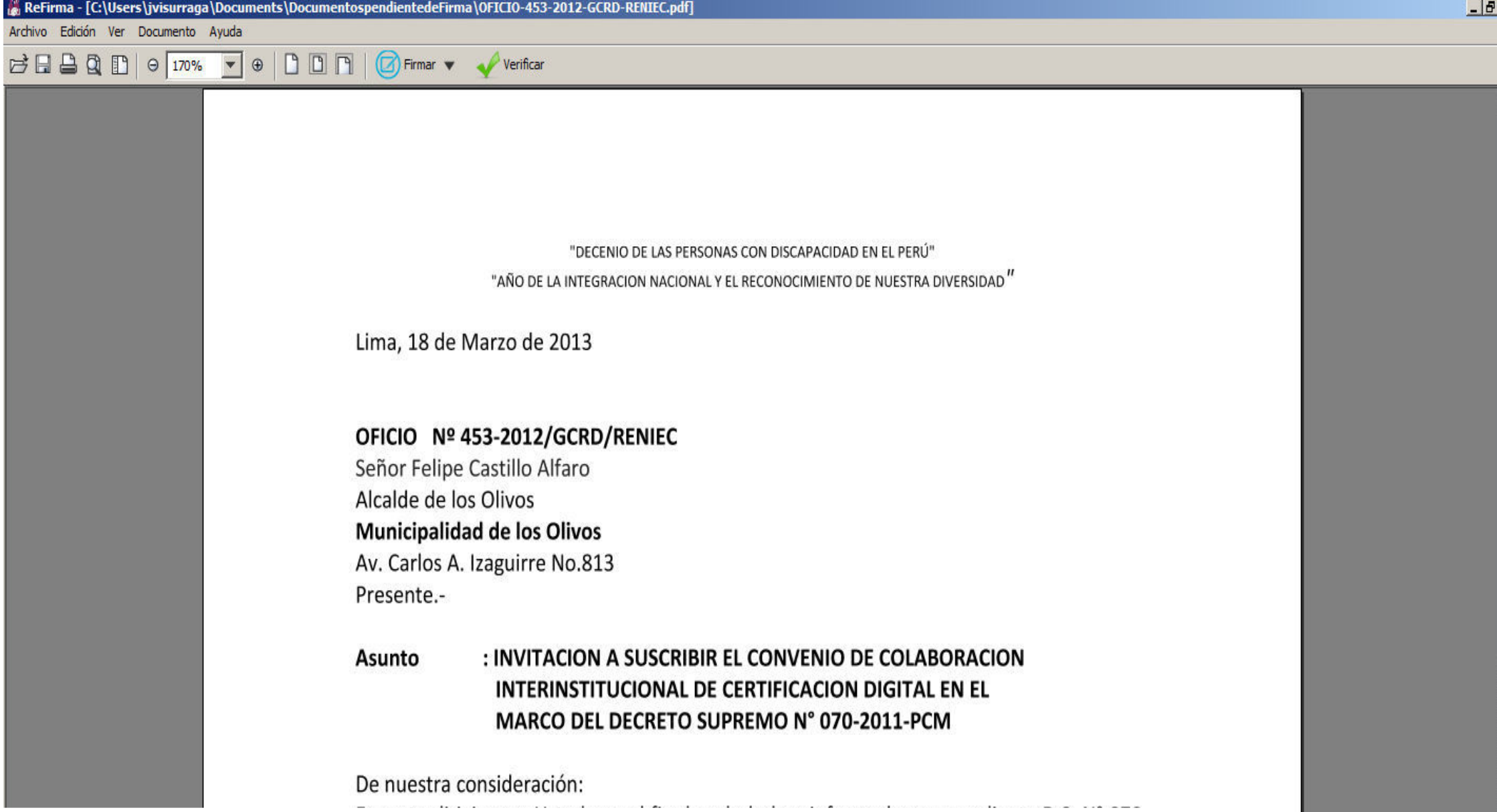
Al mostrarse la ventana "Abrir archivo", ubicamos y seleccionamos el documento que deseamos firmar digitalmente y como ya mencionamos, debe contar con la extensión ".pdf".



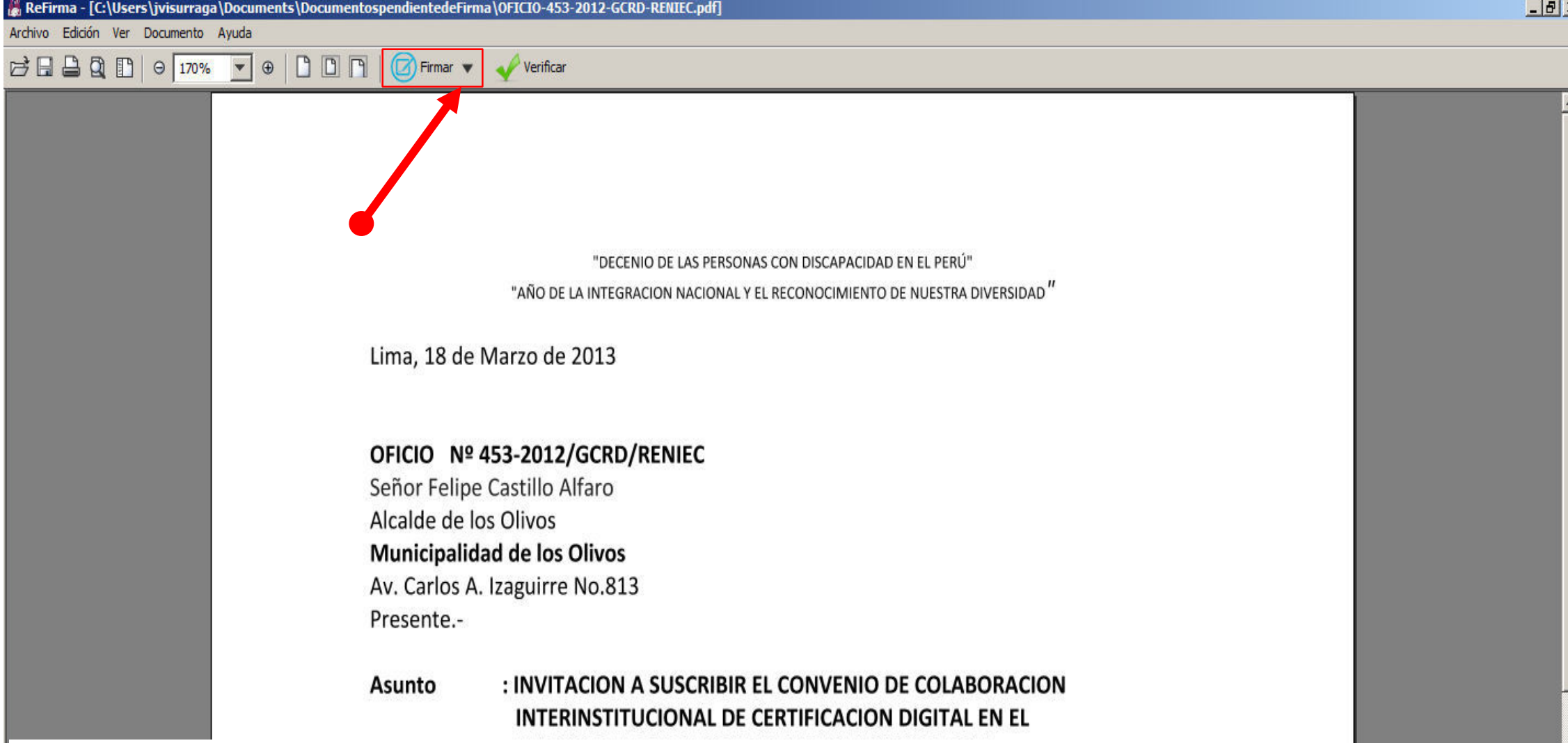
Al mostrarse la ventana "Abrir archivo", ubicamos y seleccionamos el documento que deseamos firmar digitalmente y como ya mencionamos, debe contar con la extensión ".pdf".



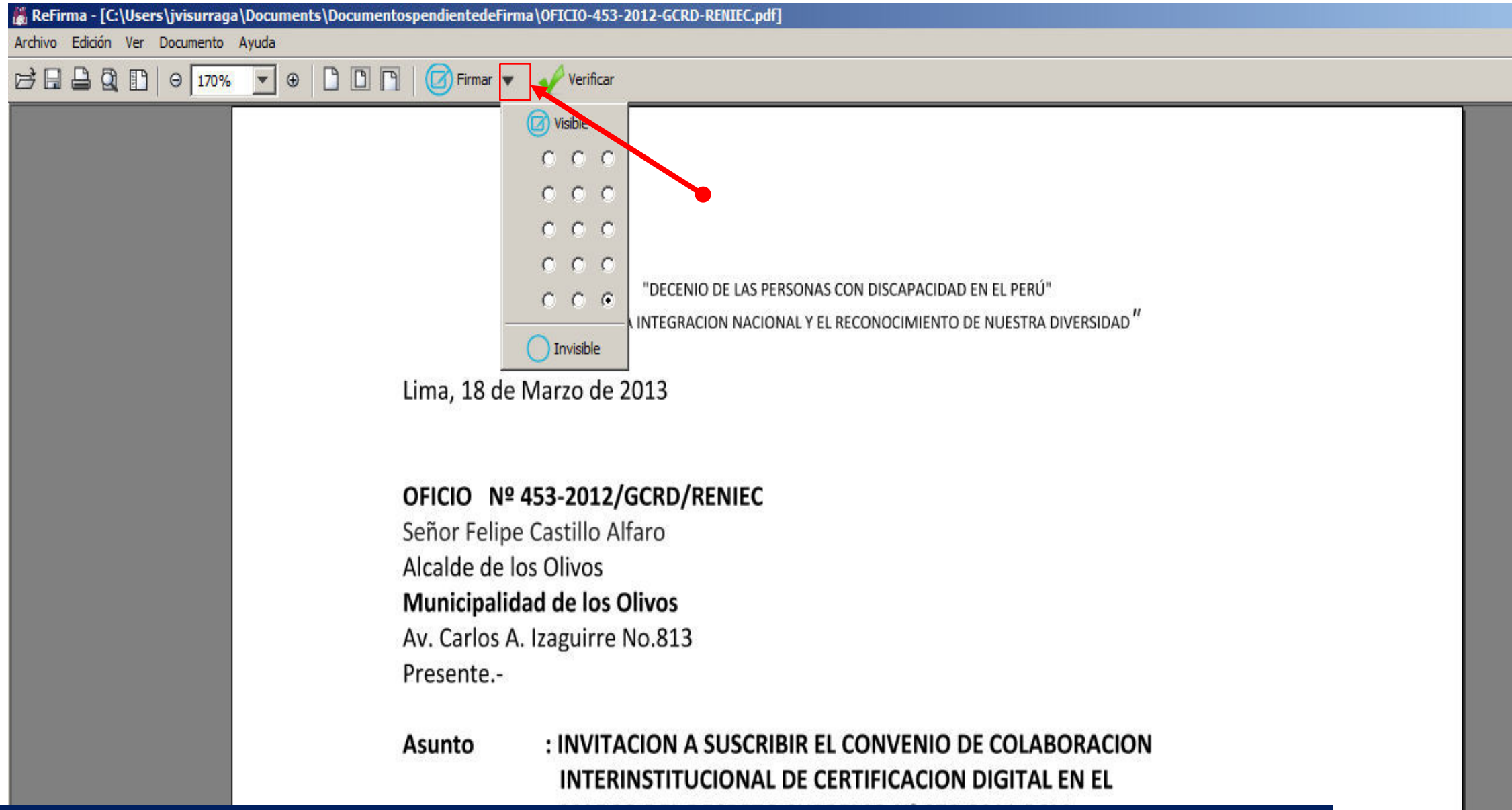
Posteriormente damos click en el botón [Abrir] para que se nos muestre el contenido del documento.



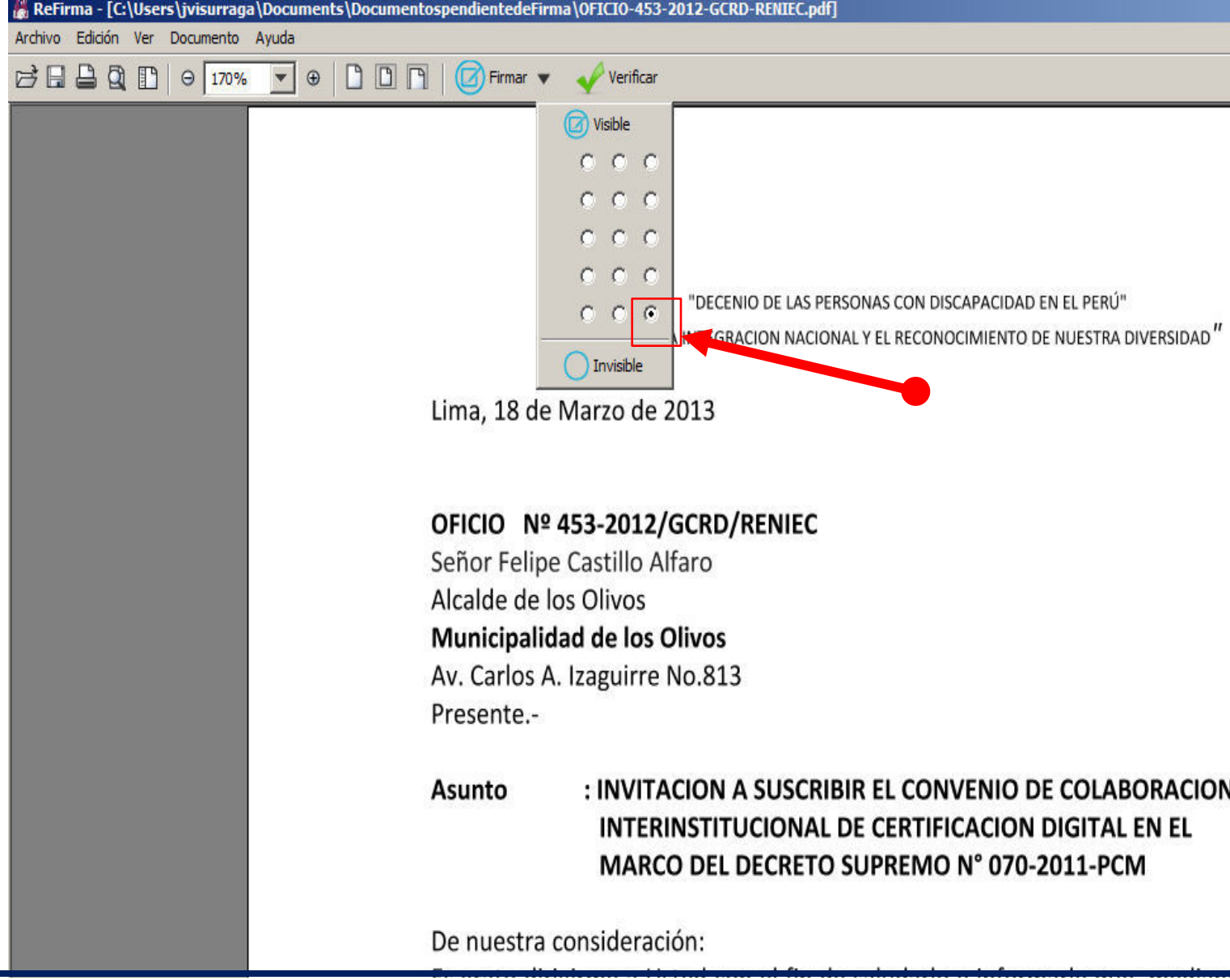
Podemos observar el documento listo para firmar digitalmente.



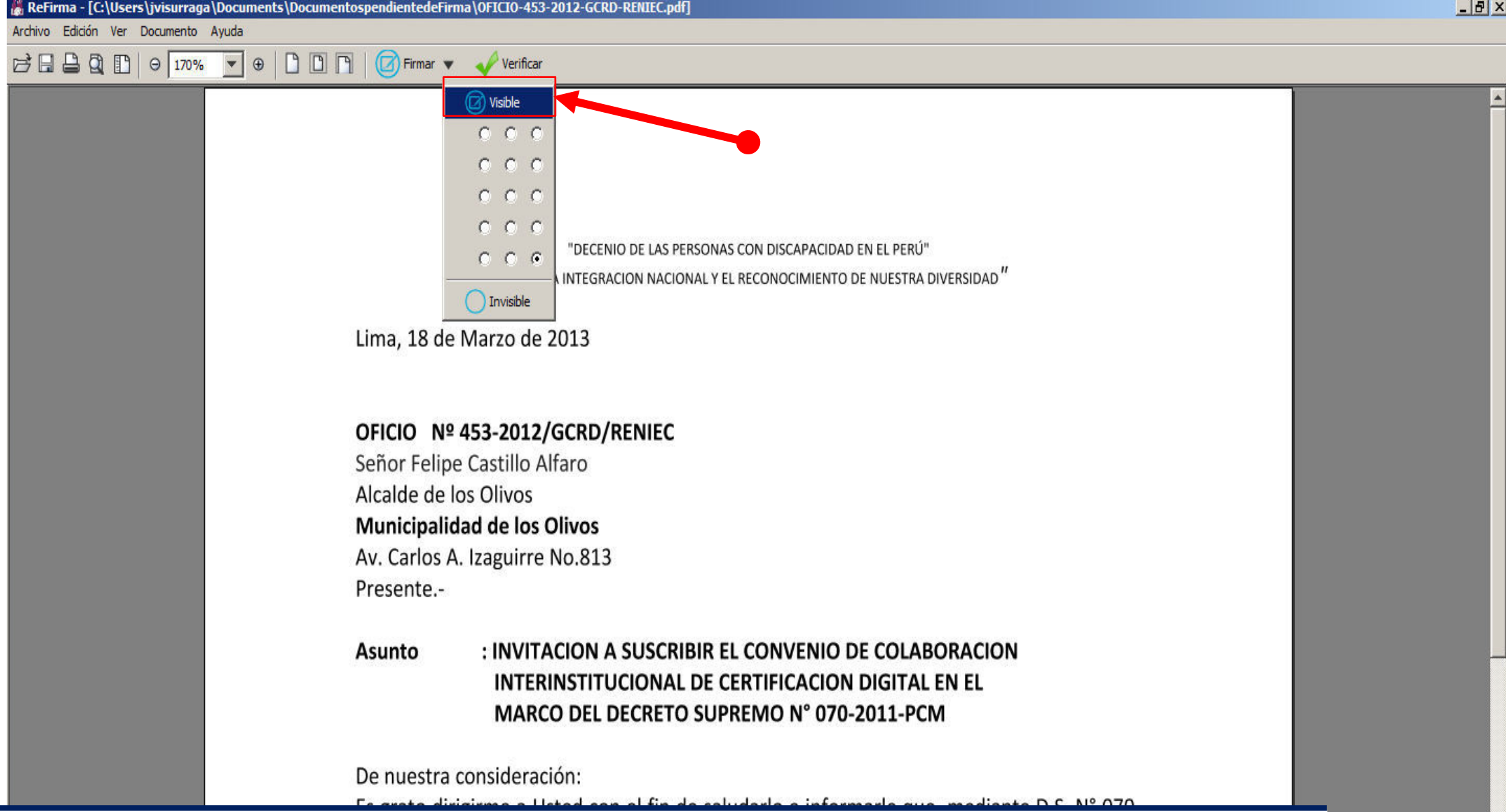
Seguidamente ubicamos el ícono desplegable en forma de flecha apuntando hacia abajo, el cual se encuentra al costado del ícono [Firmar] con el fin de determinar la ubicación de la imagen que representará la firma digital. Cabe mencionar que esta imagen no tiene valor legal si no que significa un elemento a fin de generar confianza en el usuario, ya que la firma digital no es visible; por tanto esta imagen tiene como objetivo confirmar al usuario que efectivamente se ha generado una firma digital.



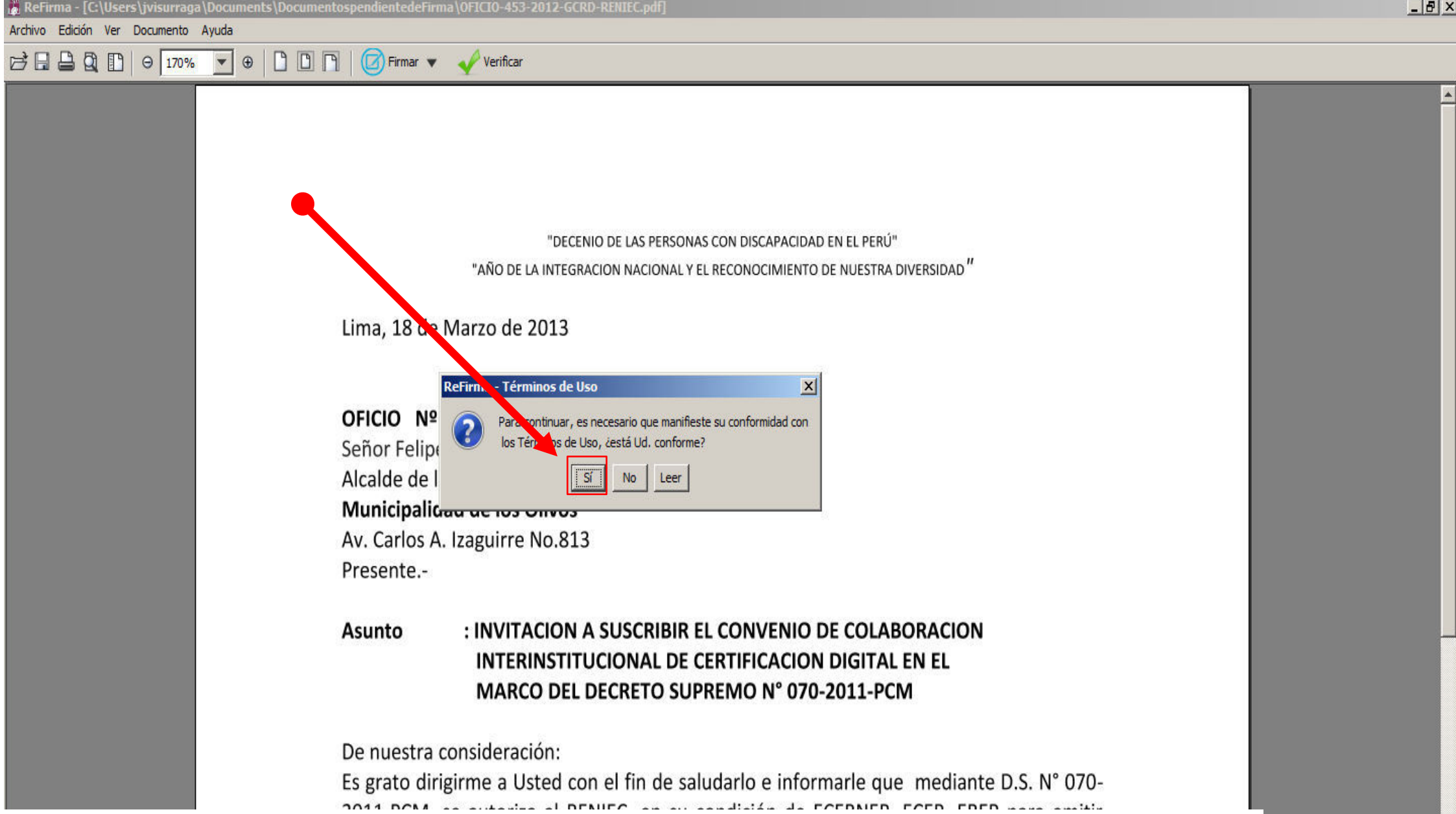
Damos click al desplegable y seleccionamos la posición donde deseamos que se ubique la imagen que representa la firma digital.



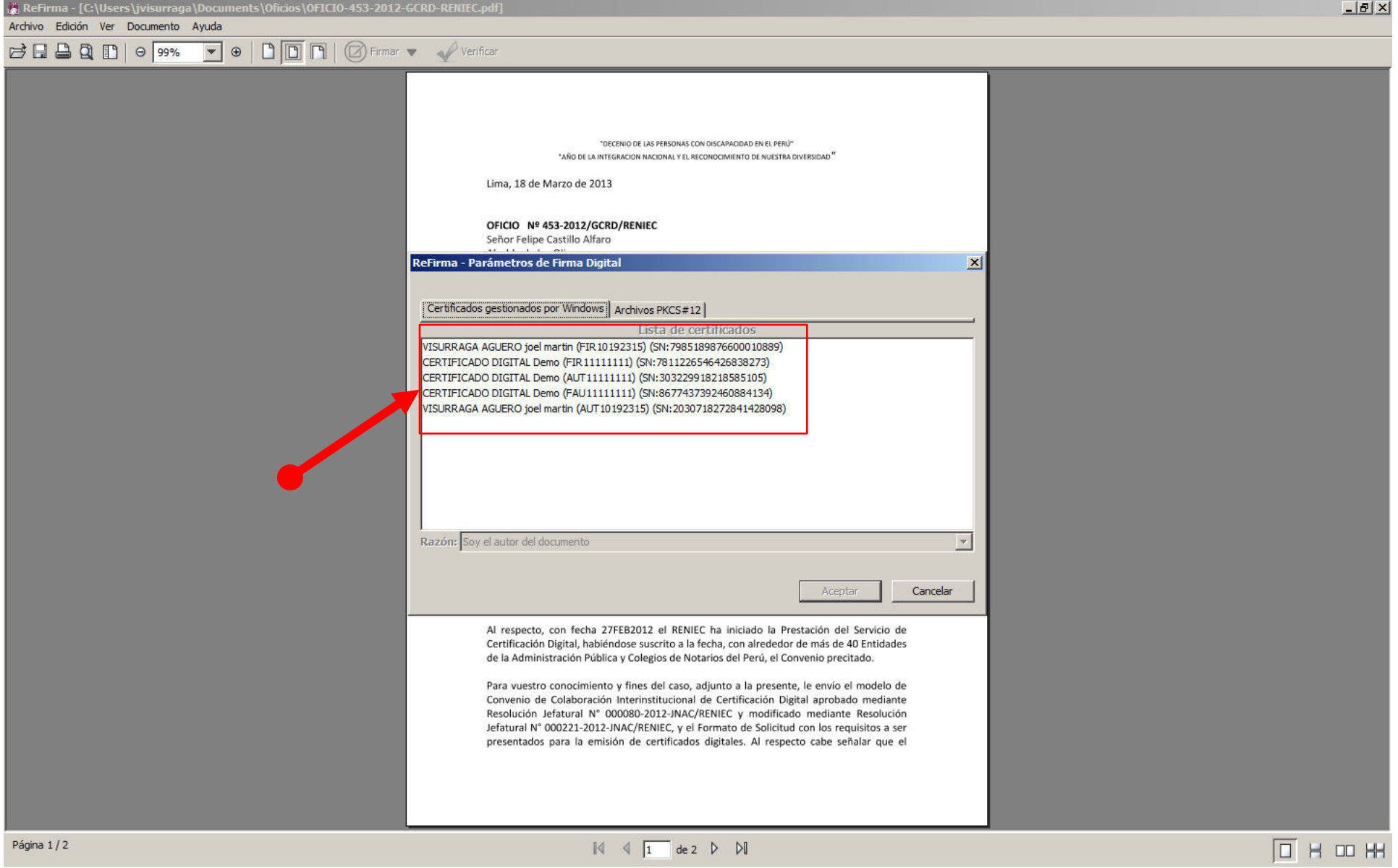
Para este caso específico, seleccionamos la ubicación inferior derecha.



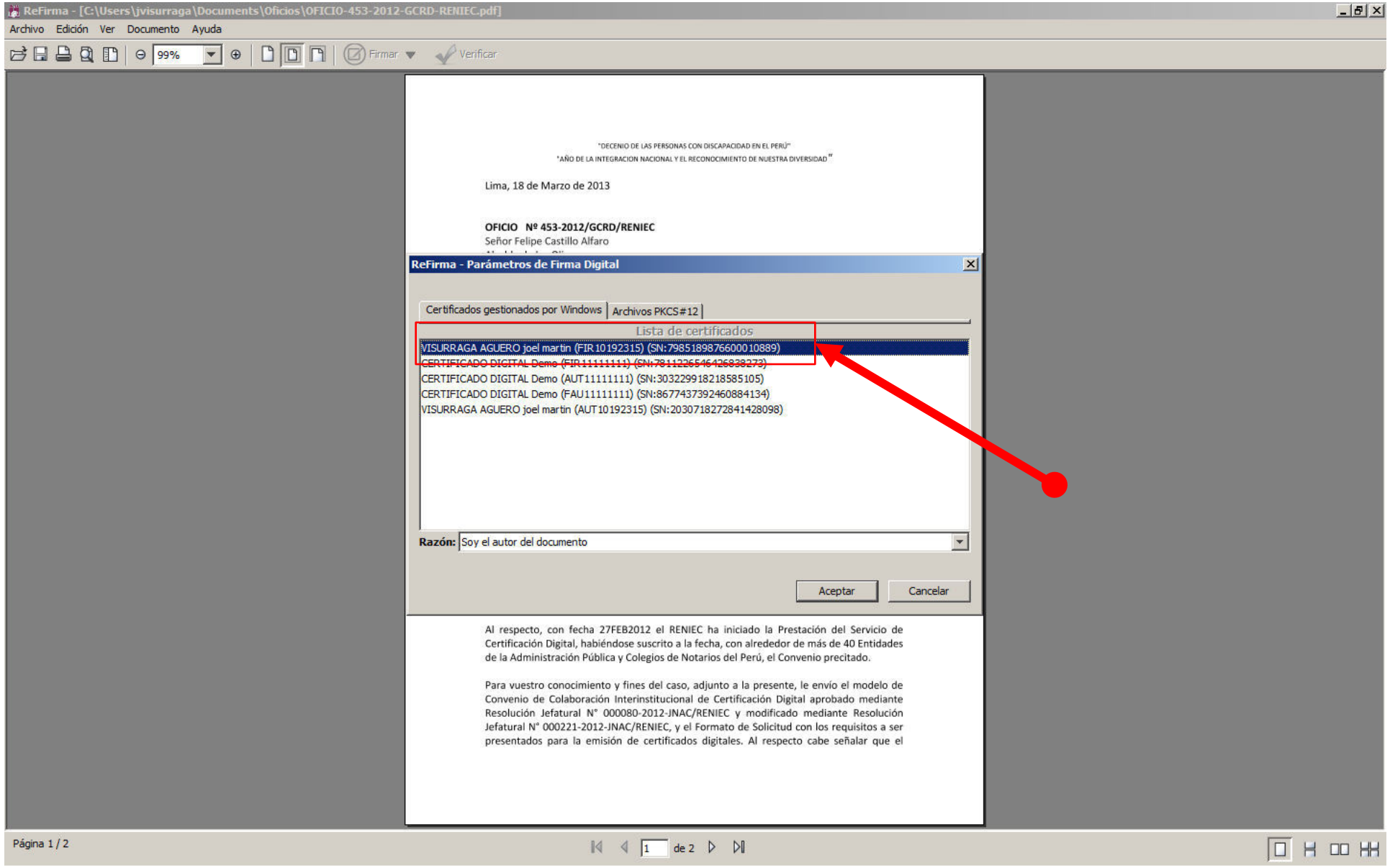
Luego damos click a la opción <Visible>.



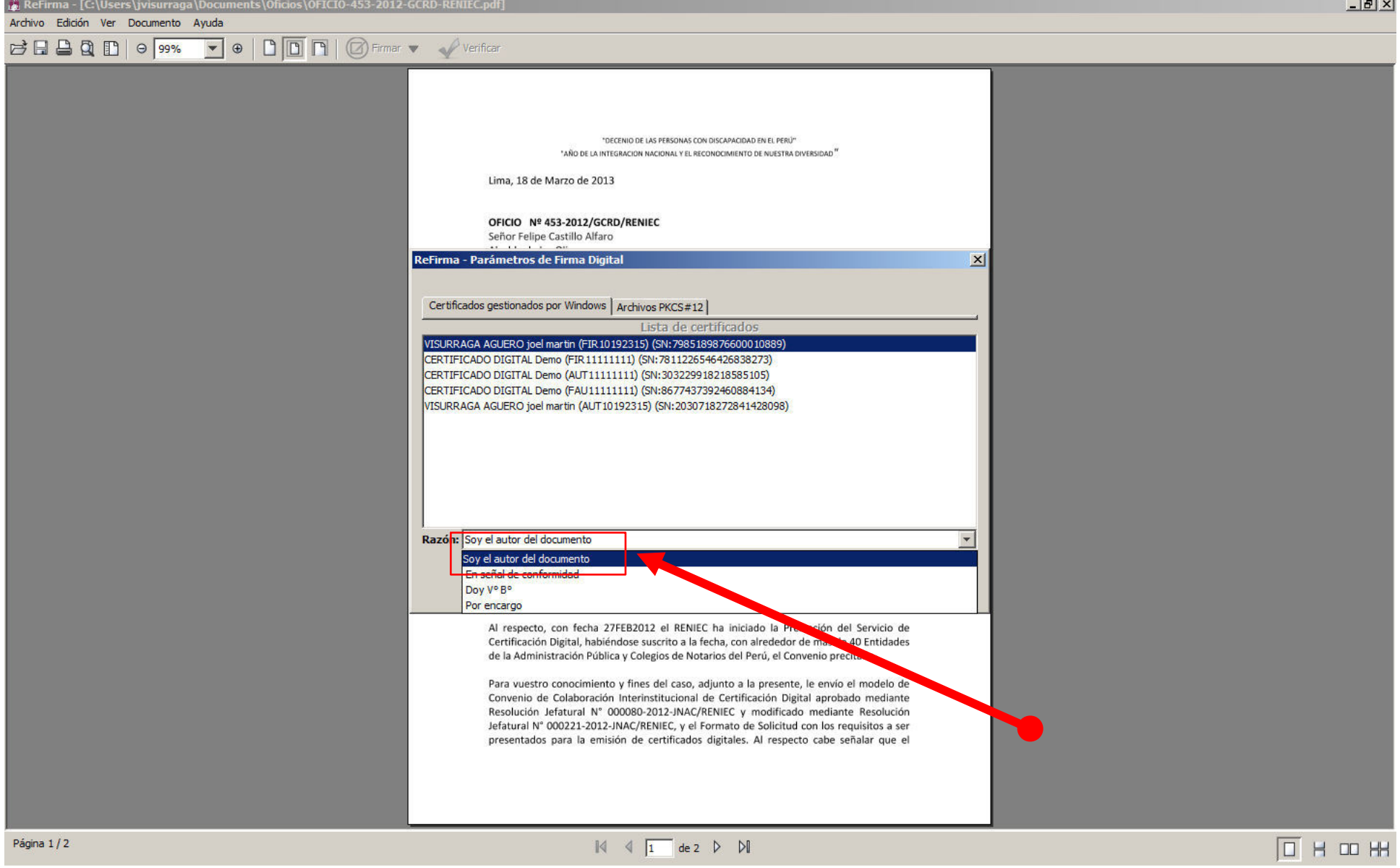
A continuación se muestra una ventana de diálogo solicitándo nuestra conformidad con los términos de uso del software de firma digital "ReFirma 1.1.0", al que respondemos dando click en el botón [Sí].



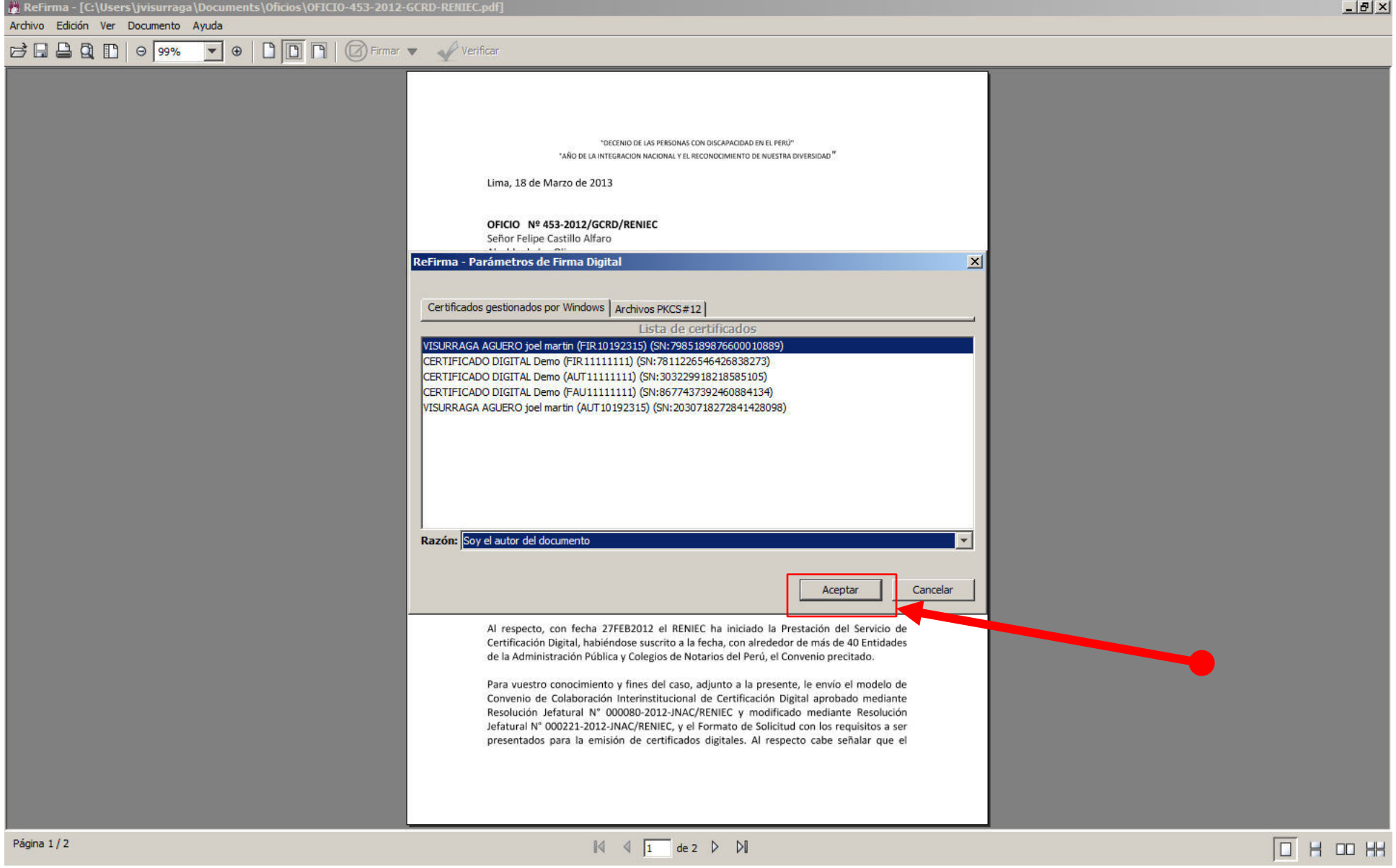
Transcurridos unos segundos se muestra la ventana "ReFirma: Parámetros de Firma Digital" en el cual se muestran los certificados digitales instalados.



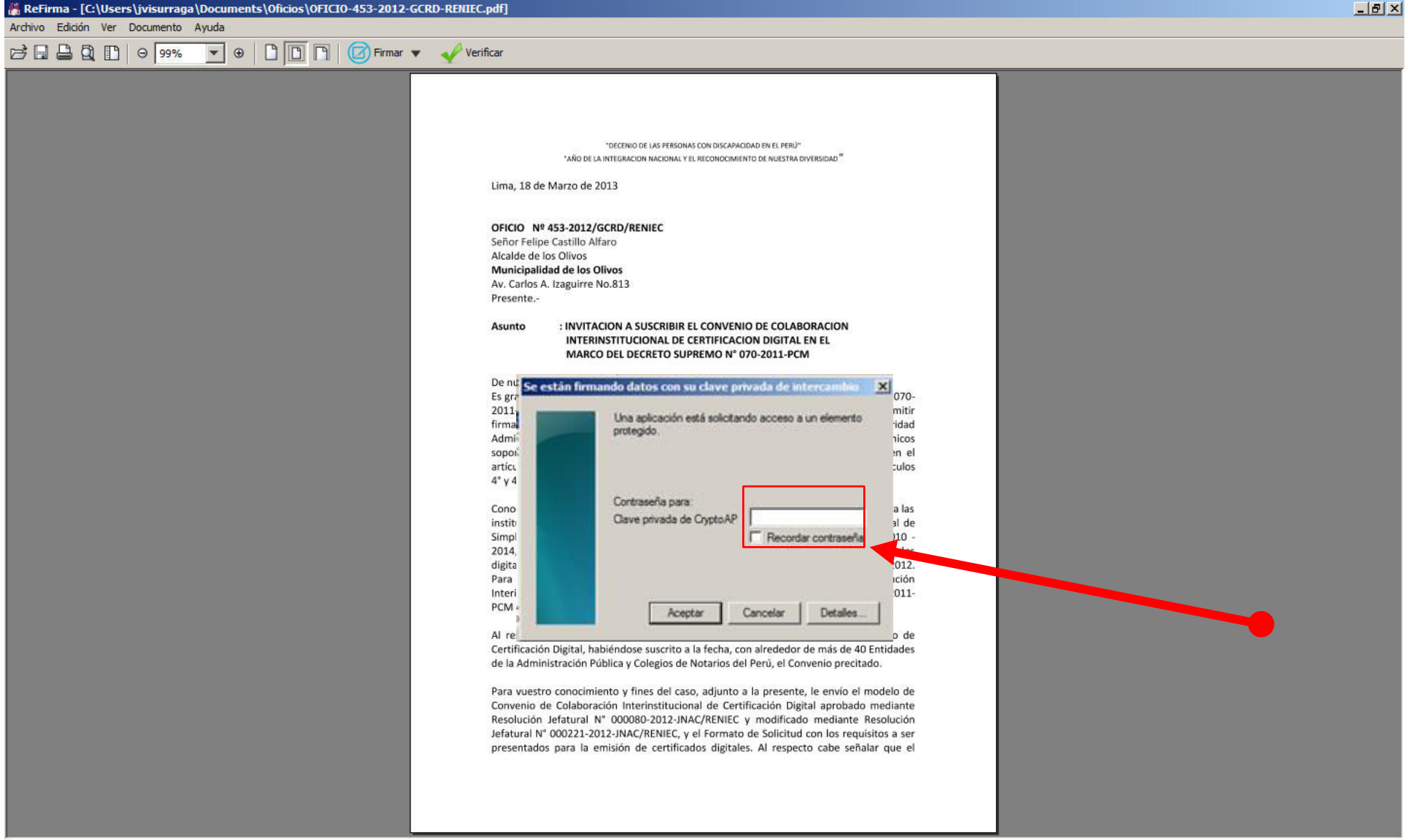
Luego seleccionamos el certificado digital con el que firmaremos el documento electrónico.



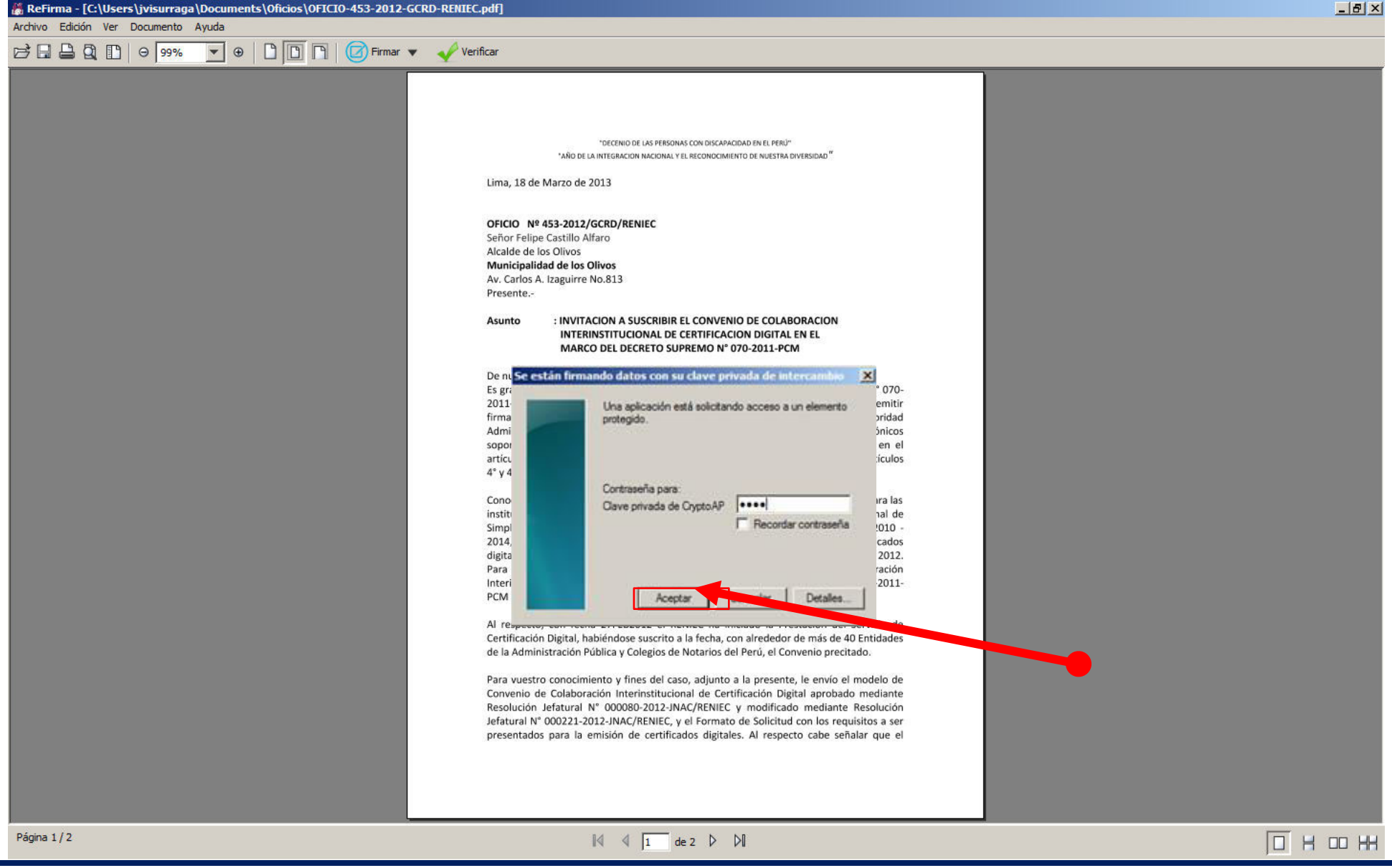
En la parte inferior encontraremos un desplegable donde podemos seleccionar la razón por la cual firmamos digitalmente el documento electrónico. Seleccionamos la razón respectiva.



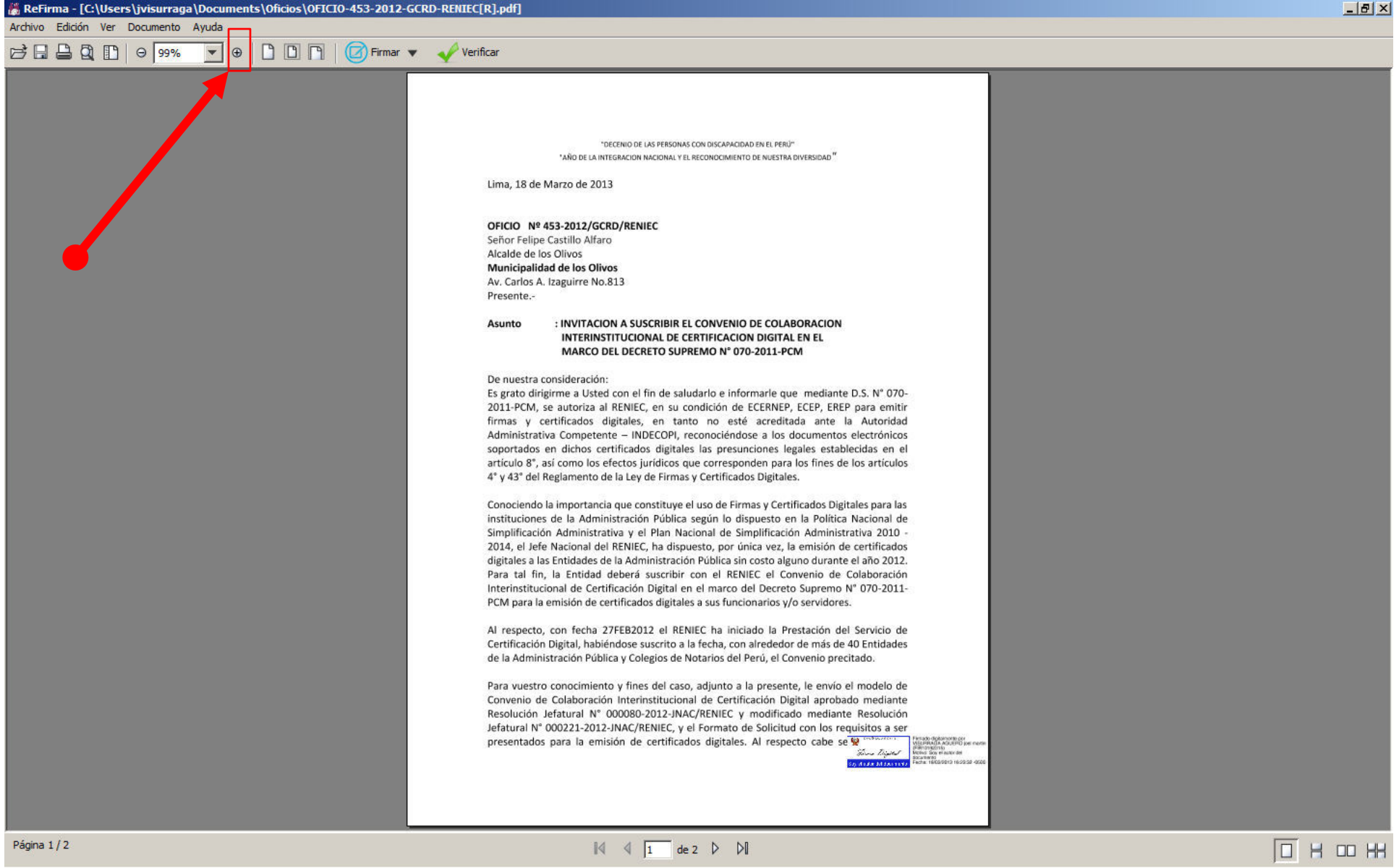
Luego damos click en el botón [Aceptar].



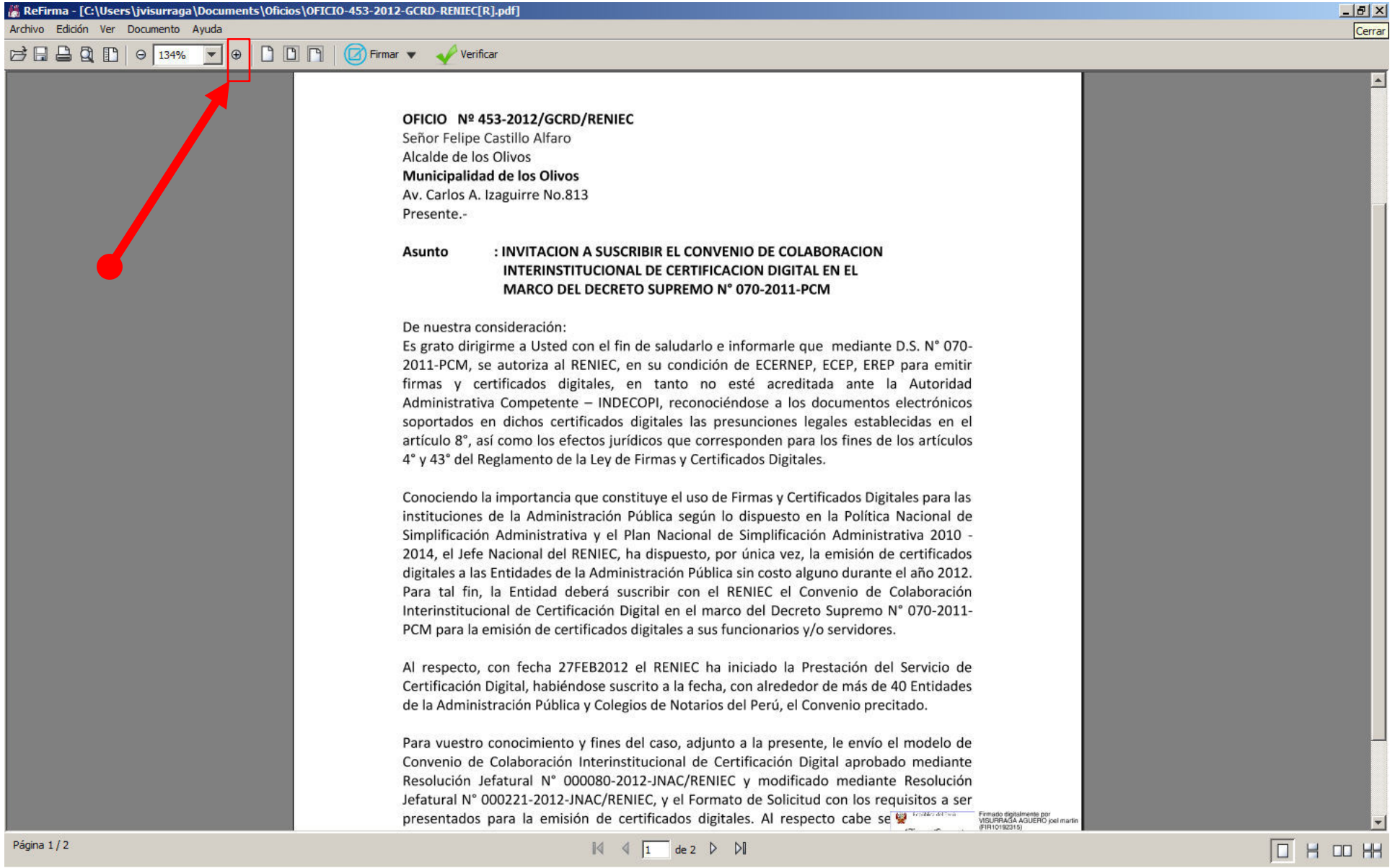
A continuación se nos solicitará la contraseña de acceso al certificado digital. Esta contraseña debe ser conocida sólo por el dueño del certificado digital. Es importante saber que por motivos de seguridad no es recomendable habilitar el check en la opción "Recordar contraseña"



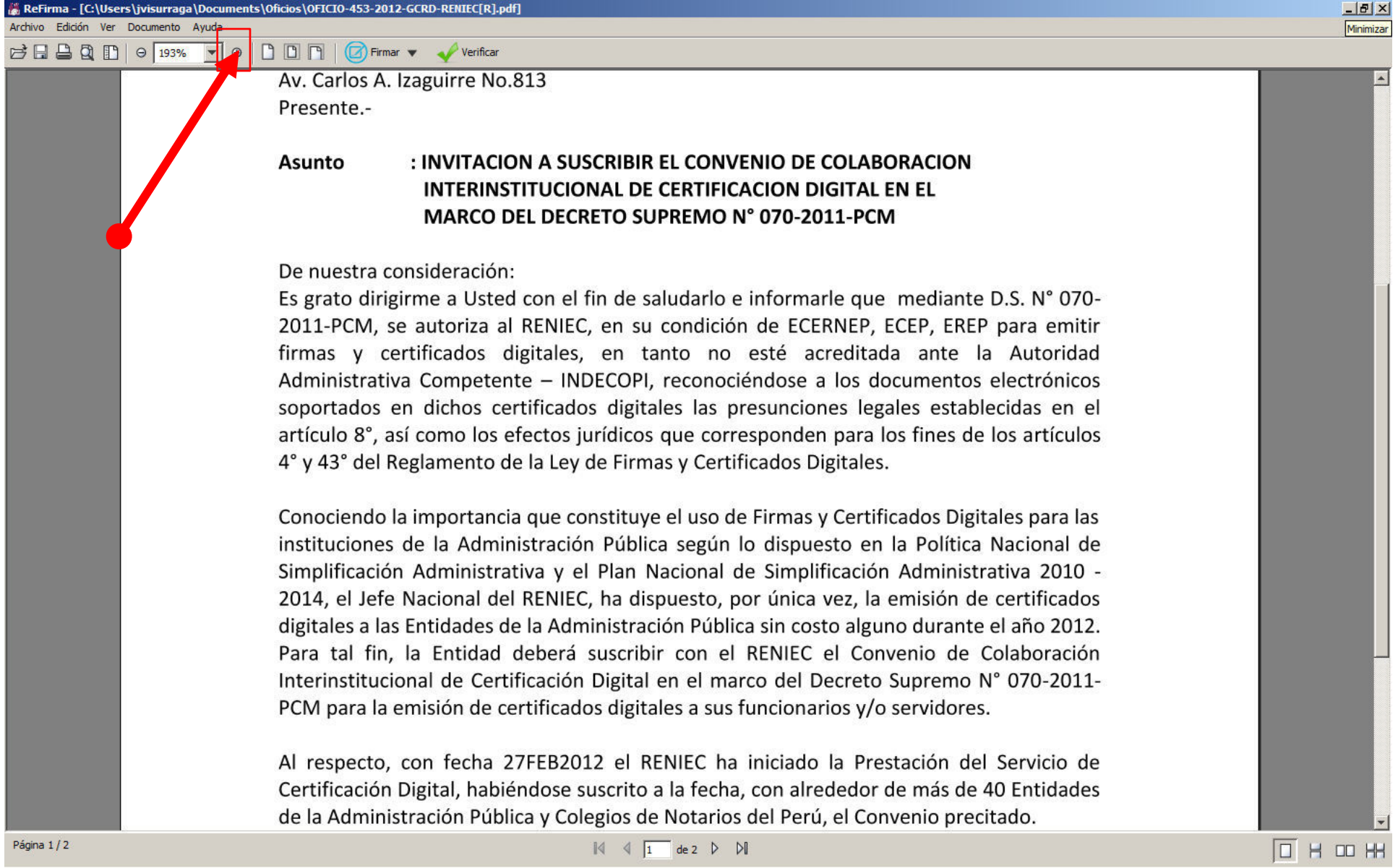
Finalmente damos click en la opción [Aceptar] y obtenemos un documento electrónico firmado digitalmente.



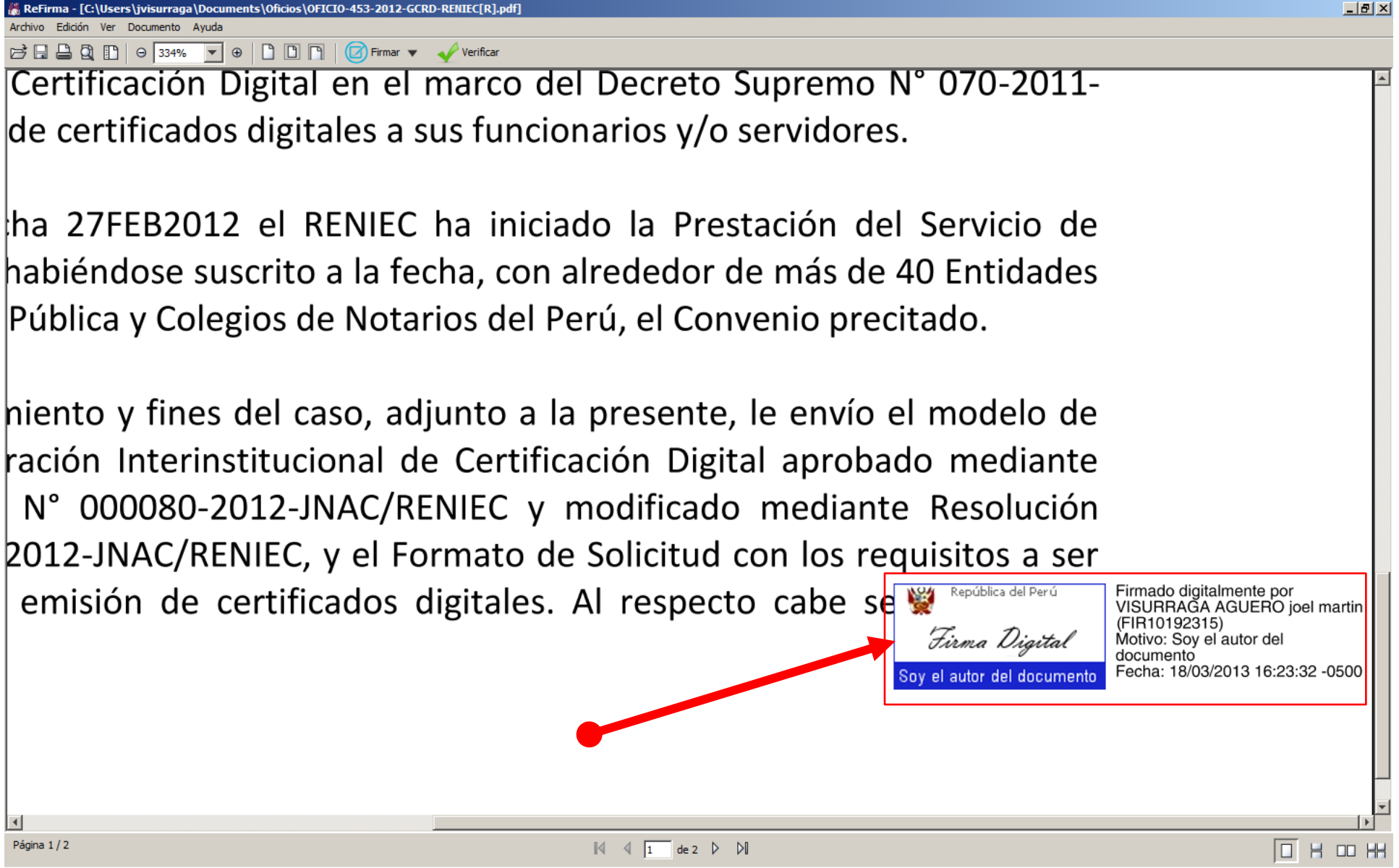
Podemos observar la imagen que representa la firma digital con mayor detalle maximizando el tamaño del documento con el botón [+] o [Acercar].



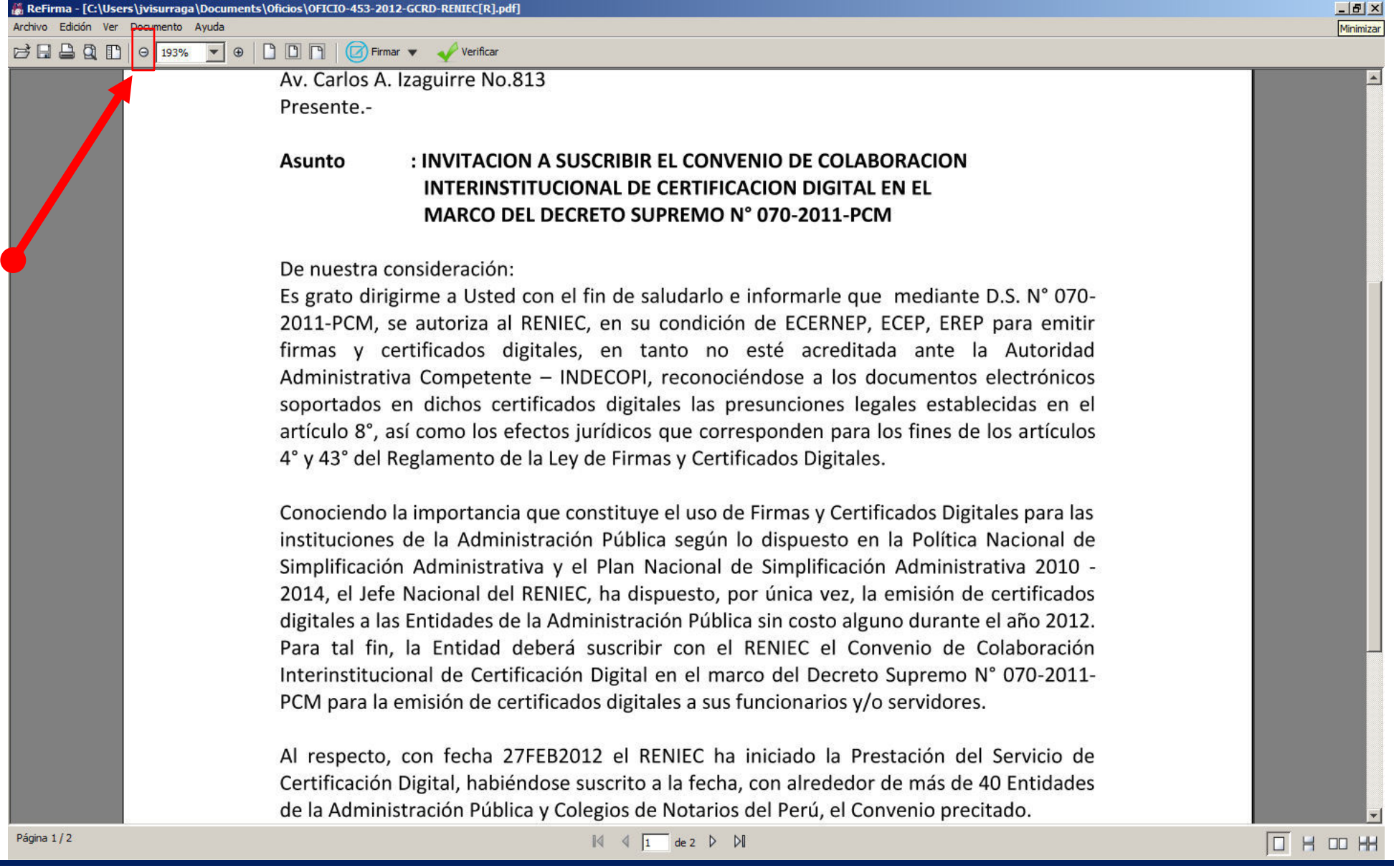
Podemos observar la imagen que representa la firma digital con mayor detalle maximizando el tamaño del documento con el botón [+] o [Acercar].



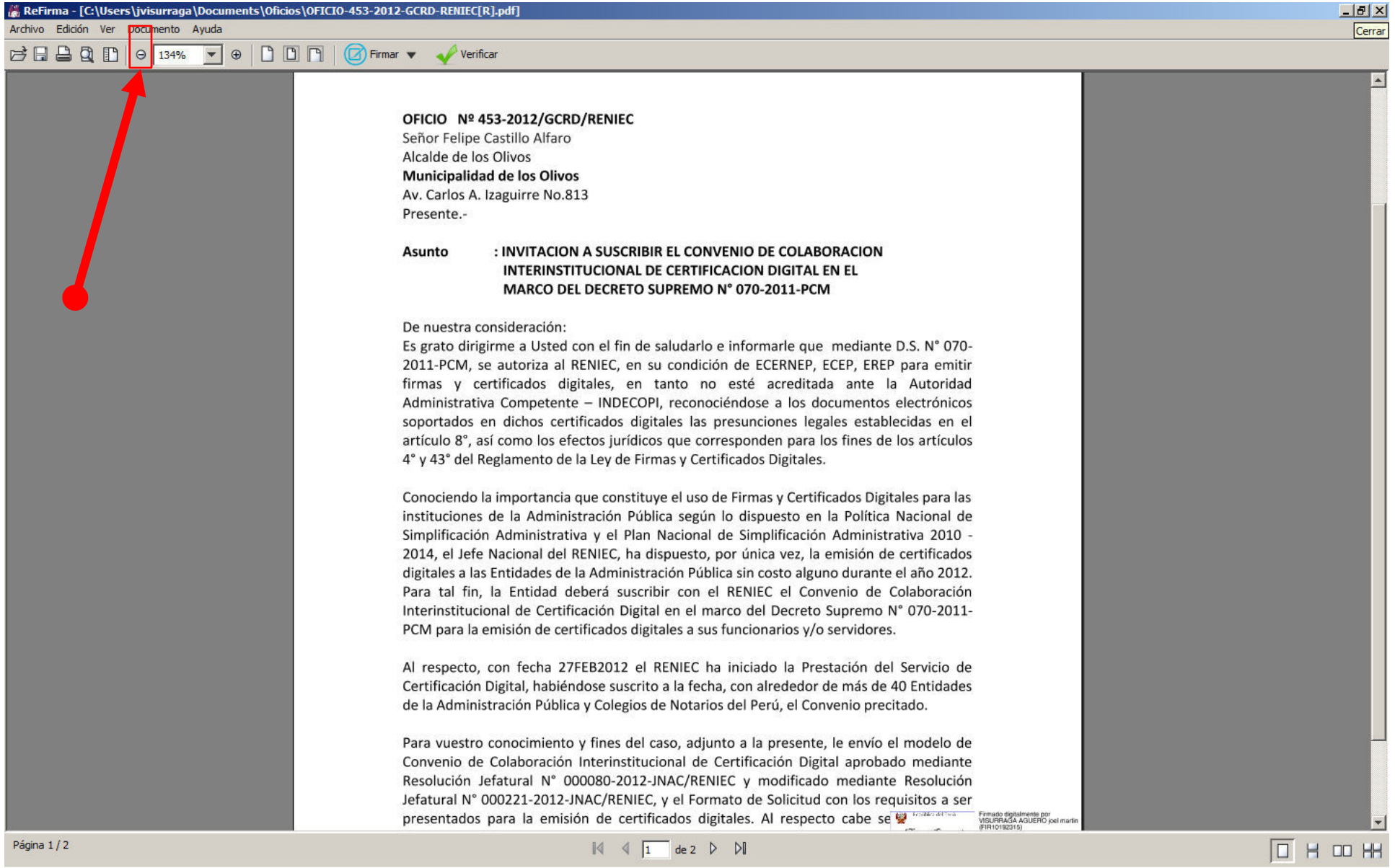
Podemos observar la imagen que representa la firma digital con mayor detalle maximizando el tamaño del documento con el botón [+] o [Acercar].



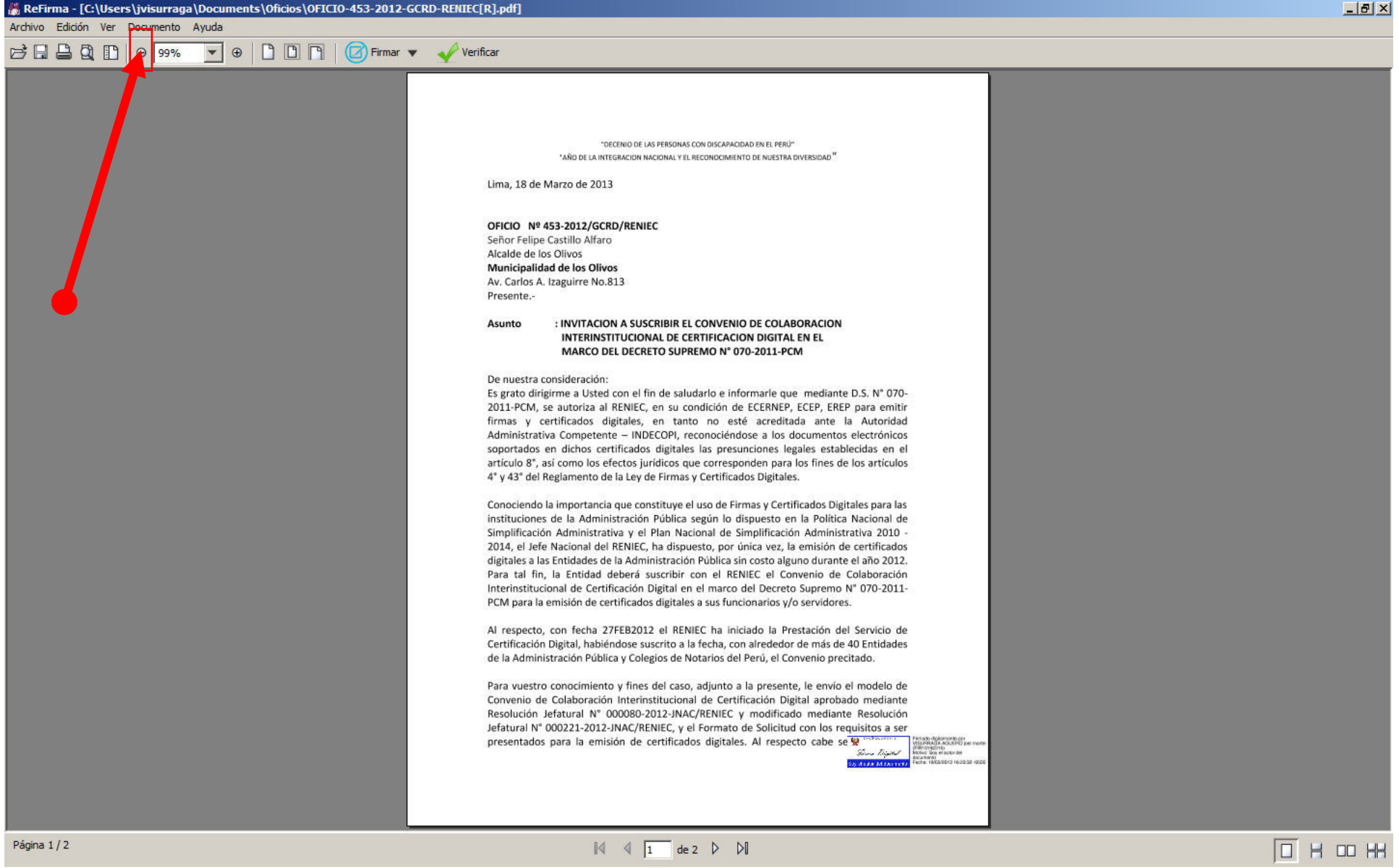
Podemos observar la imagen que representa la firma digital con mayor detalle maximizando el tamaño del documento con el botón [+] o [Acercar].



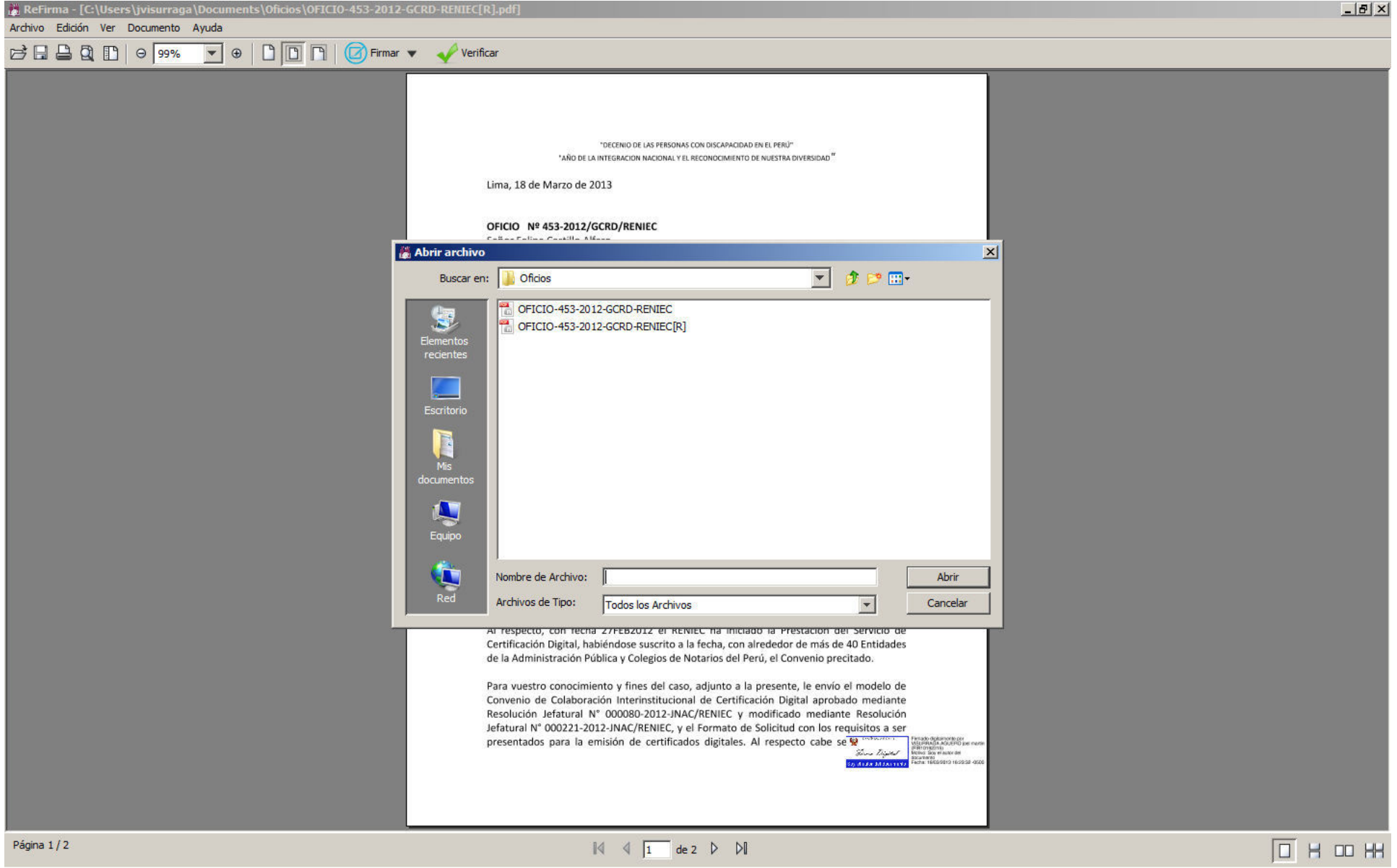
Utilizamos el botón [-] o [Alejar] para ver el documento completo.



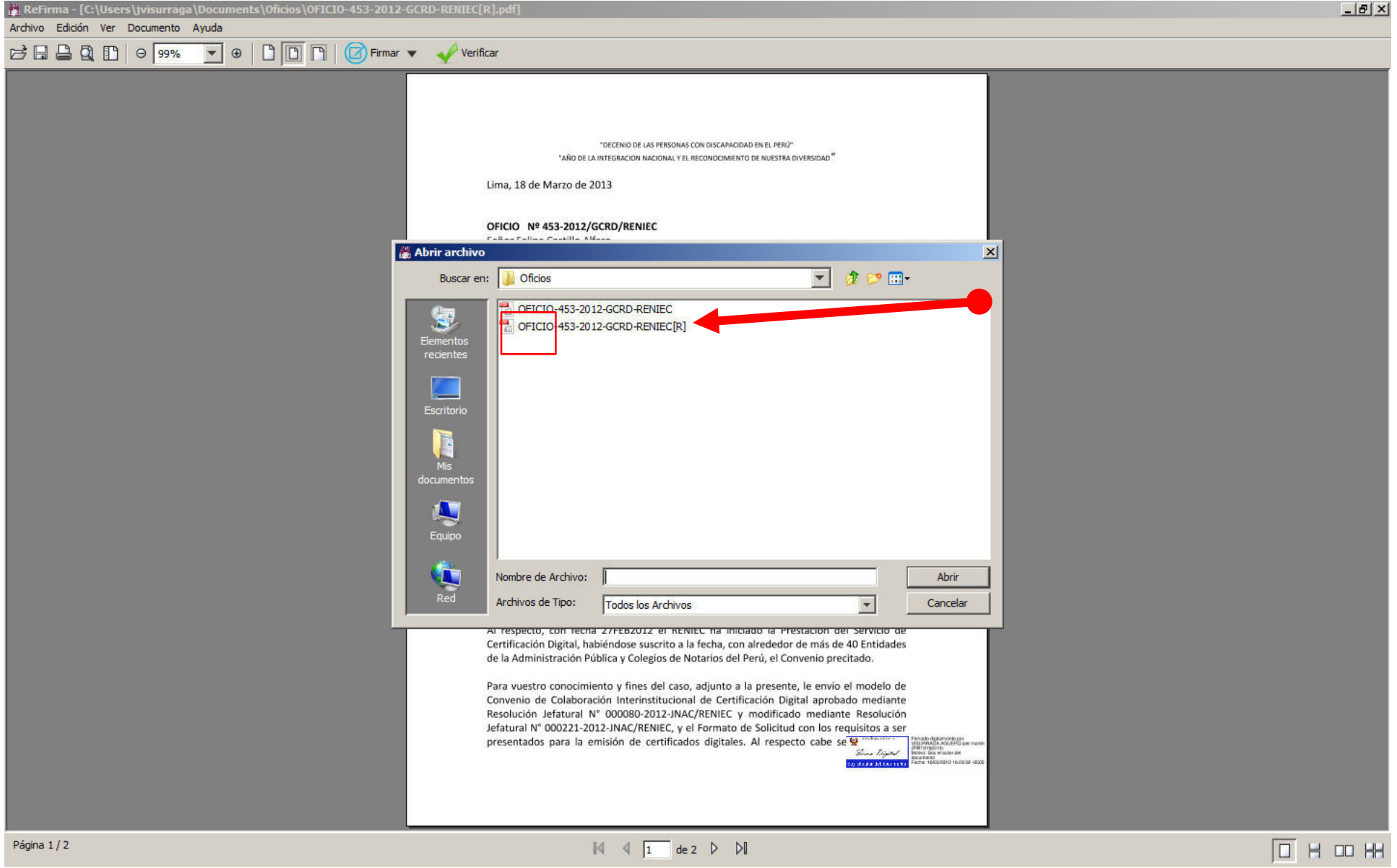
Utilizamos el botón [-] o [Alejar] para ver el documento completo.



Utilizamos el botón [-] o [Alejar] para ver el documento completo.



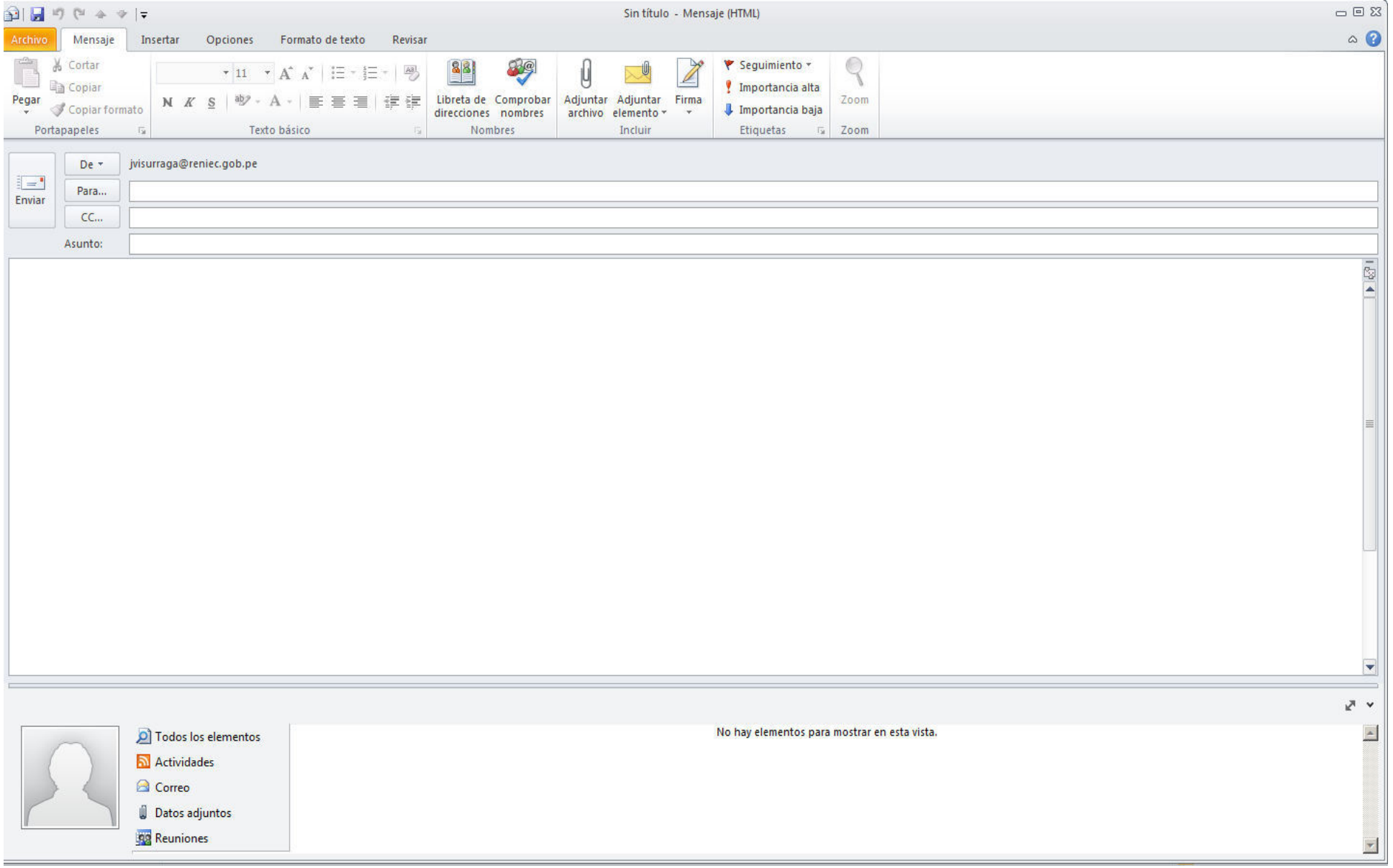
Utilizando la opción <Archivo> y la posterior subopción <Abrir>, podemos visualizar que se ha generado un segundo archivo.



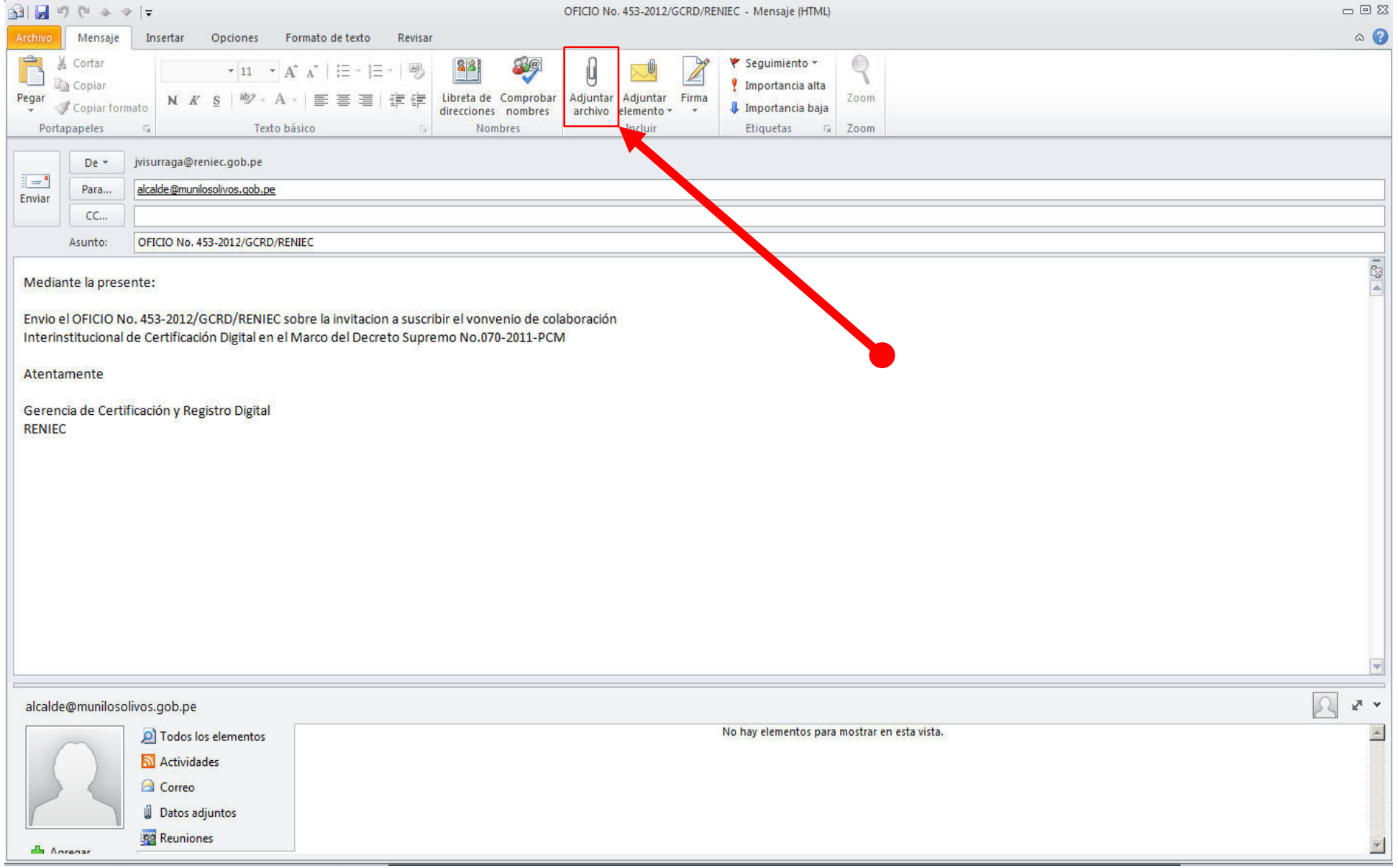
Podemos comprobar el que está firmado digitalmente porque tiene la letra [R] al lado derecho del nombre.

Paso 3

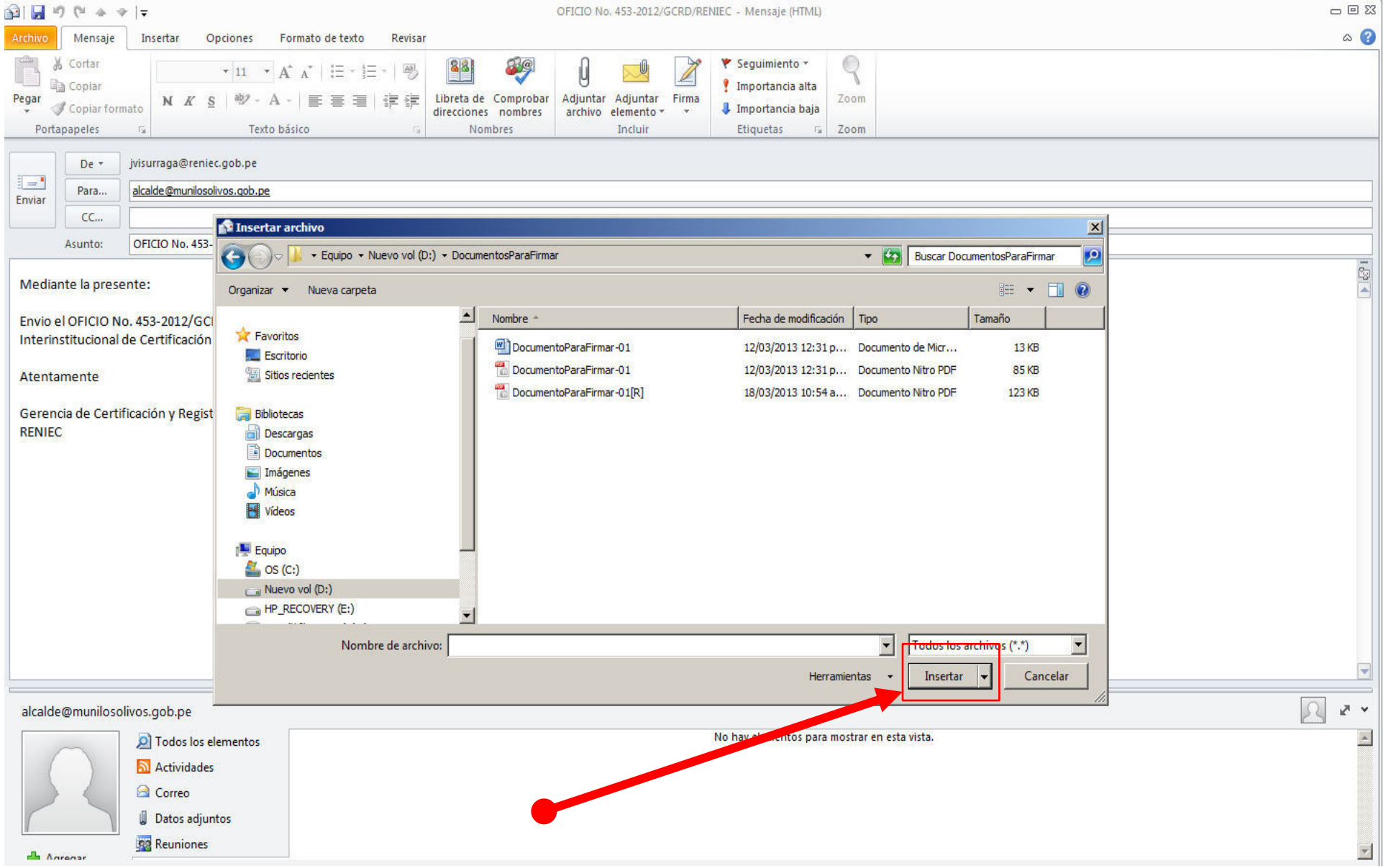
Envío del documento electrónico con firma digital vía correo electrónico



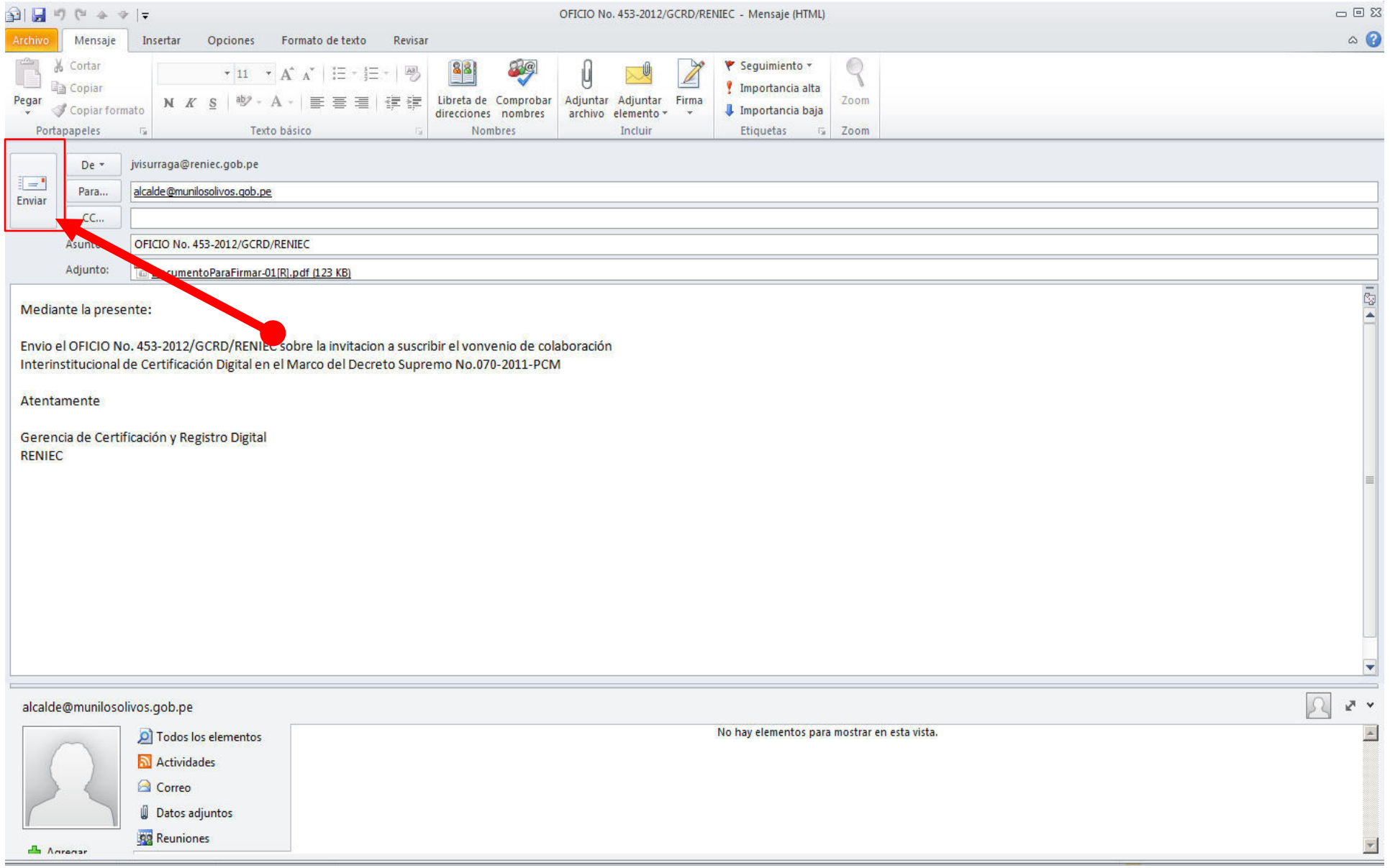
Enviaremos el documento electrónico que ya hemos firmado digitalmente "Oficio-453-2013-GV-EmpresaY[R].pdf" a la Empresa Y a través del correo electrónico.



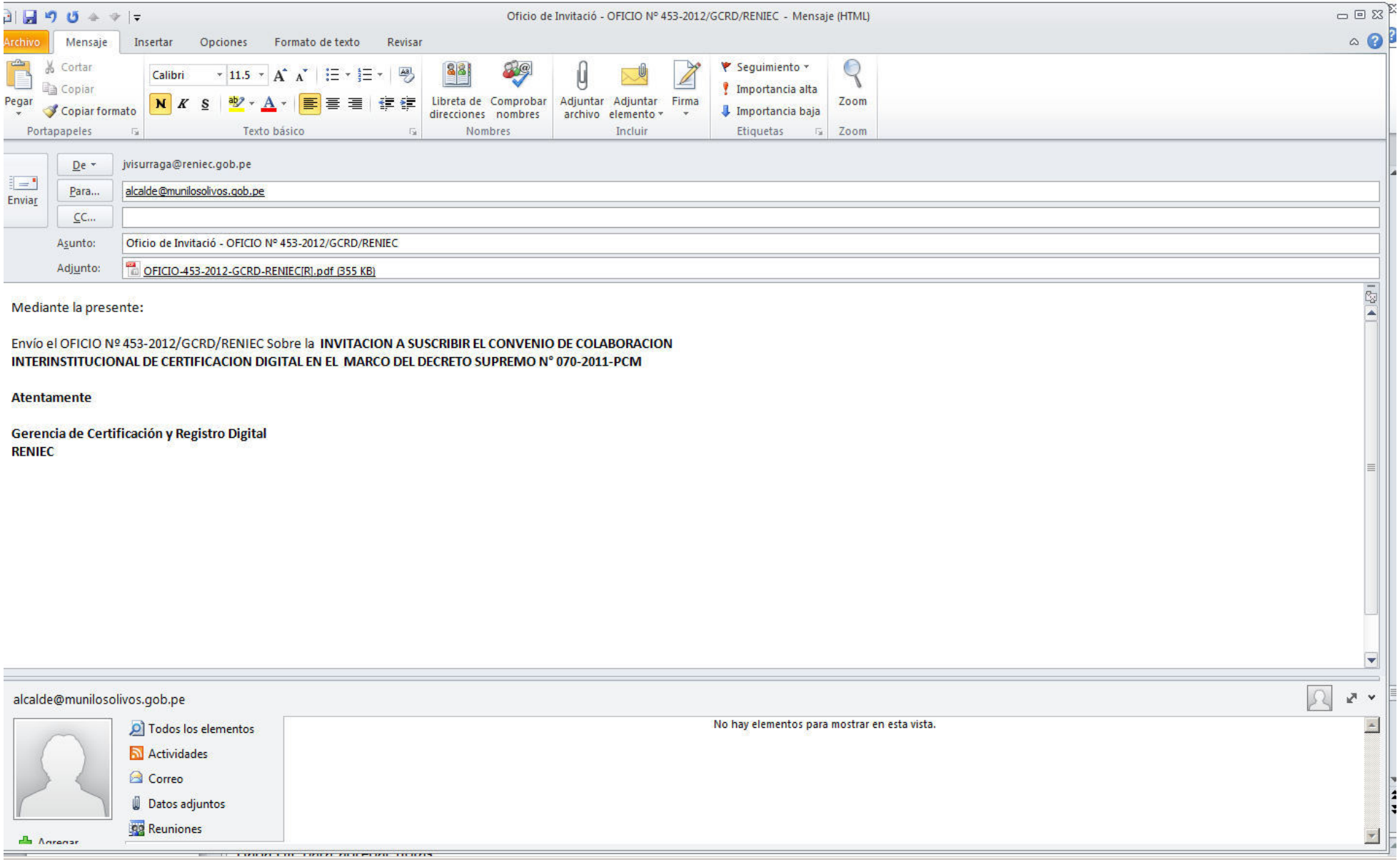
Para ello, redactamos el mensaje a enviar y luego hacemos click en el enlace [Adjuntar archivo].



Al mostrarse la ventana del explorador de Windows seleccionamos el archivo firmado digitalmente que deseamos enviar y damos click en la opción [Insertar].



Una vez que el mensaje de correo está redactado y el archivo se ha adjuntado, hacemos click en [Enviar].

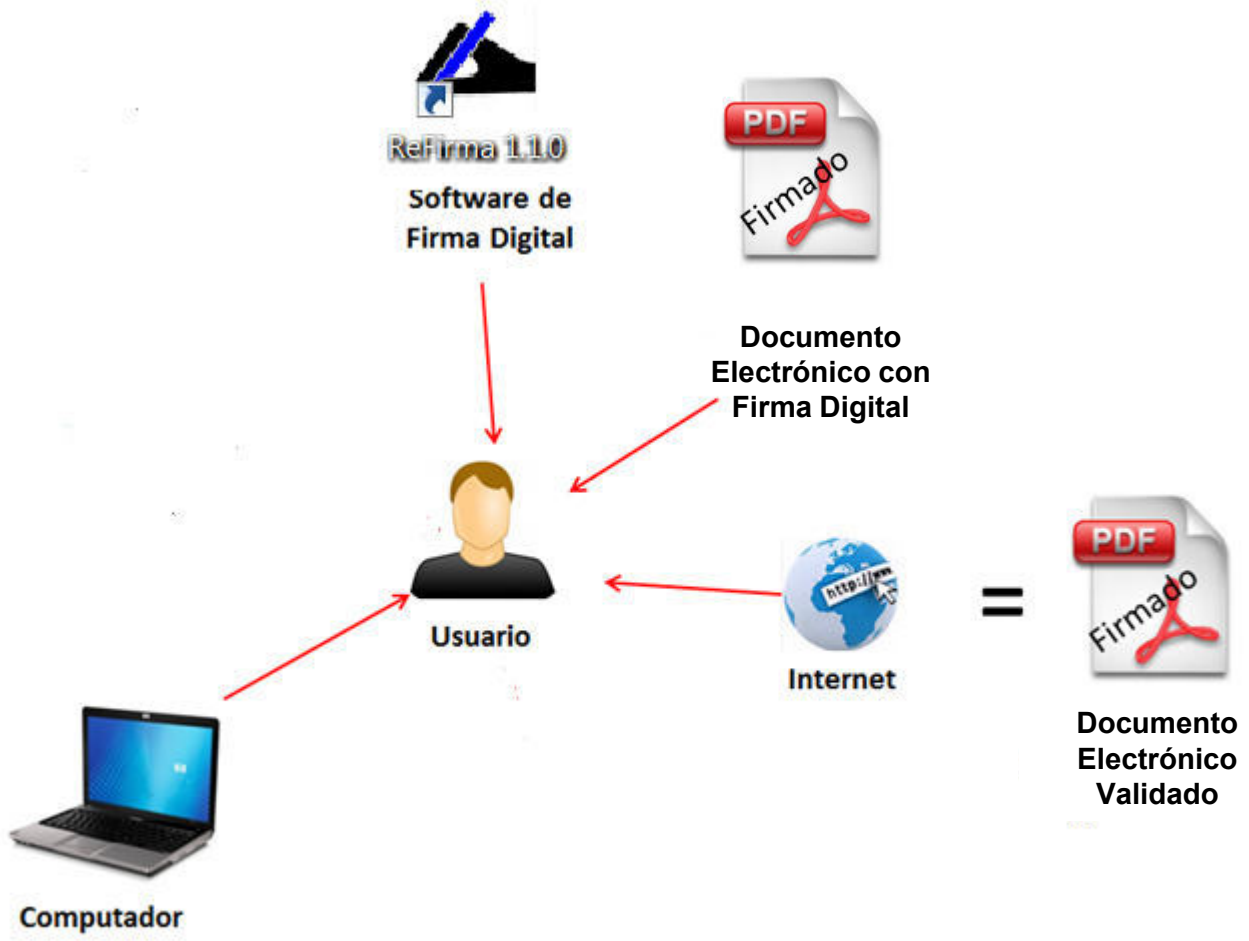


Es así cómo hemos enviado a través de correo electrónico un documento firmado digitalmente con seguridad y pleno valor legal.

Caso práctico

Validación de un documento electrónico con firma digital utilizando el software Refirma

Requerimientos para Validar un Documento Electrónico con Firma Digital

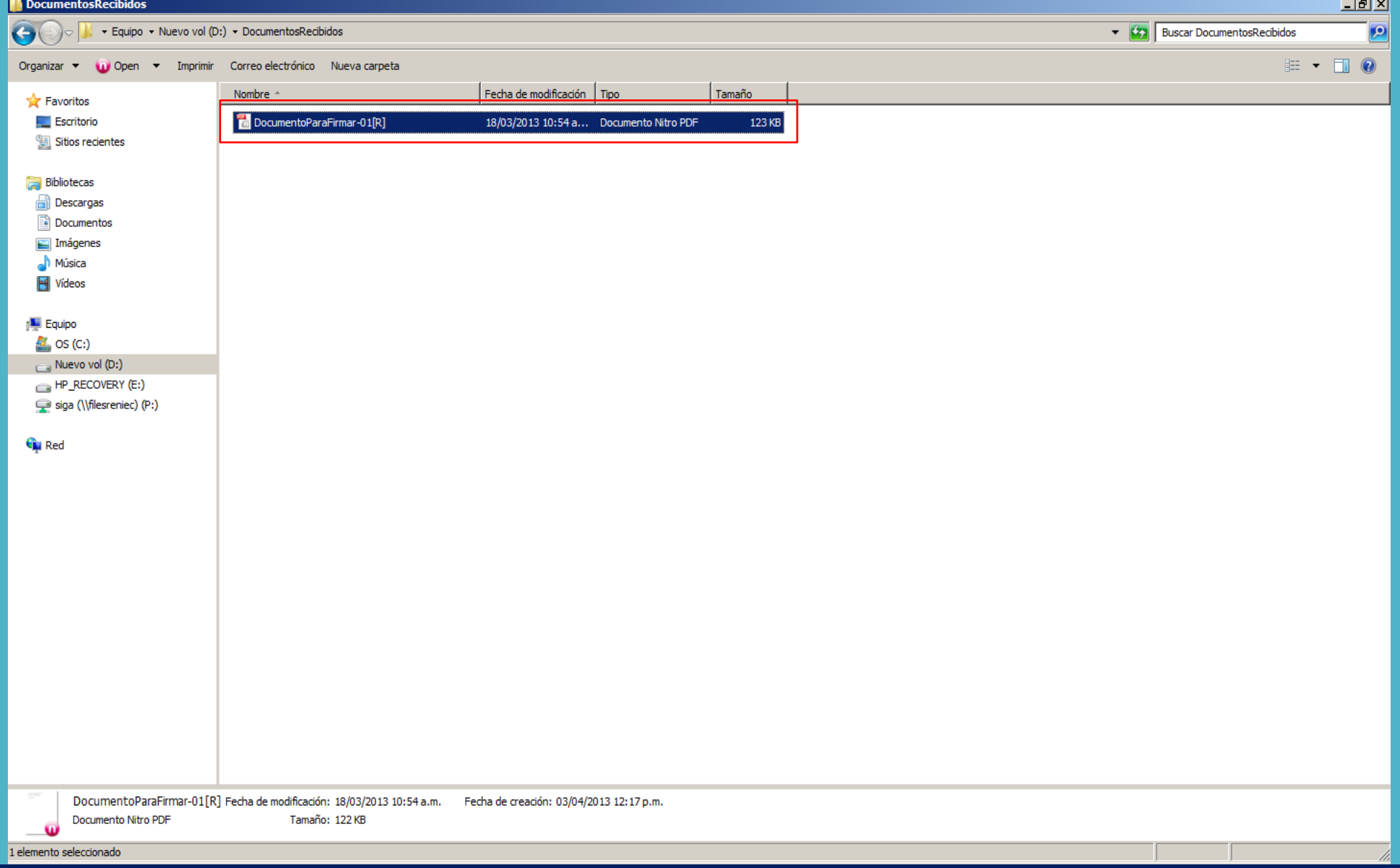


Empresa Y

A la Empresa Y ha llegado un Oficio de La Empresa X

Utilizando la opción de verificación del software ReFirma podemos comprobar que el documento electrónico con firma digital no ha sido modificado y consultar los datos del remitente (firmante).

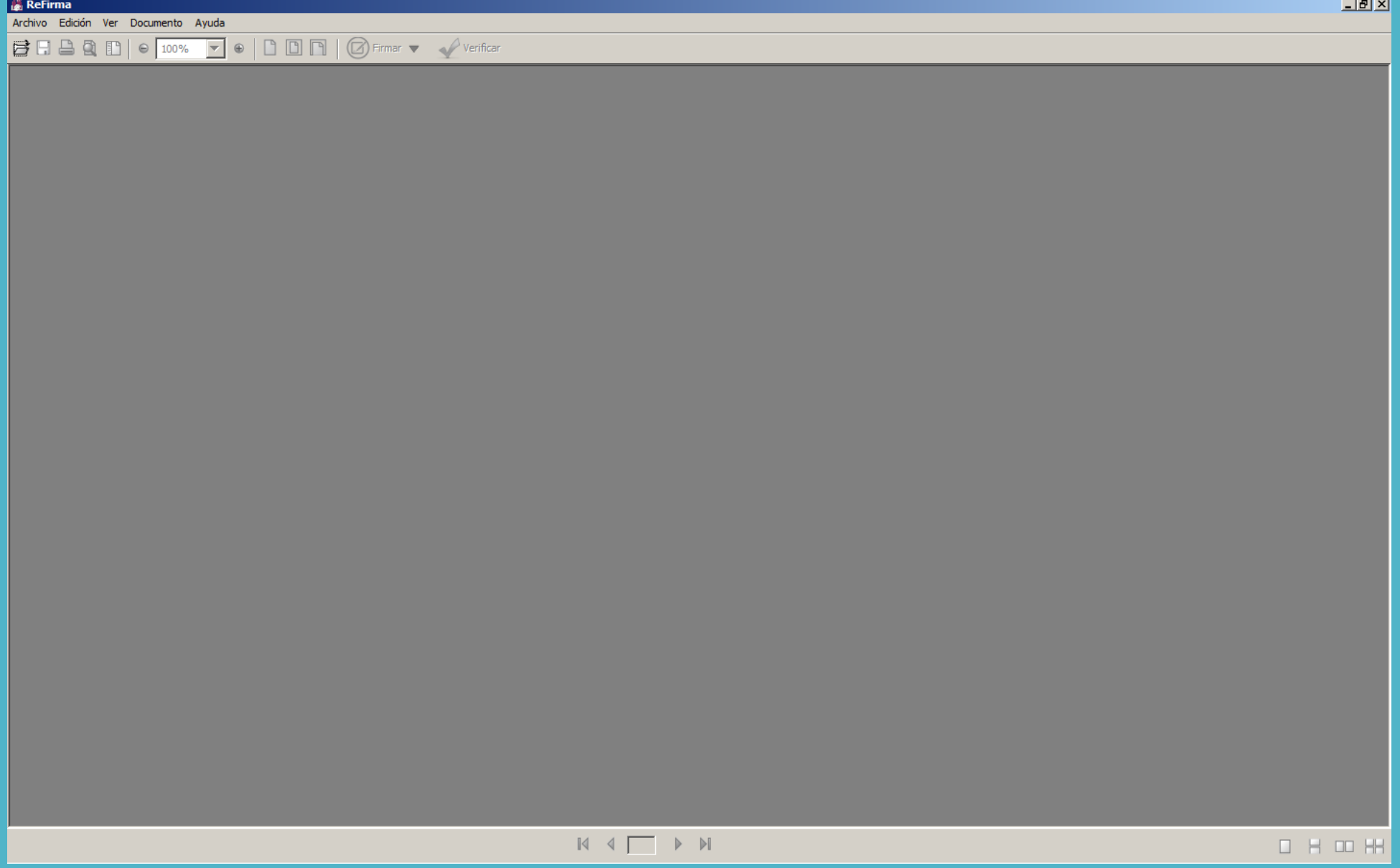
La Empresa X envió a la Empresa Y un documento firmado digitalmente. La municipalidad verificará que los documentos no han sido alterados, es decir que la firma digital es válida, a fin de poder usarlos con la misma seguridad, confianza y valor legal conforme usa los documentos firmados manuscritamente.



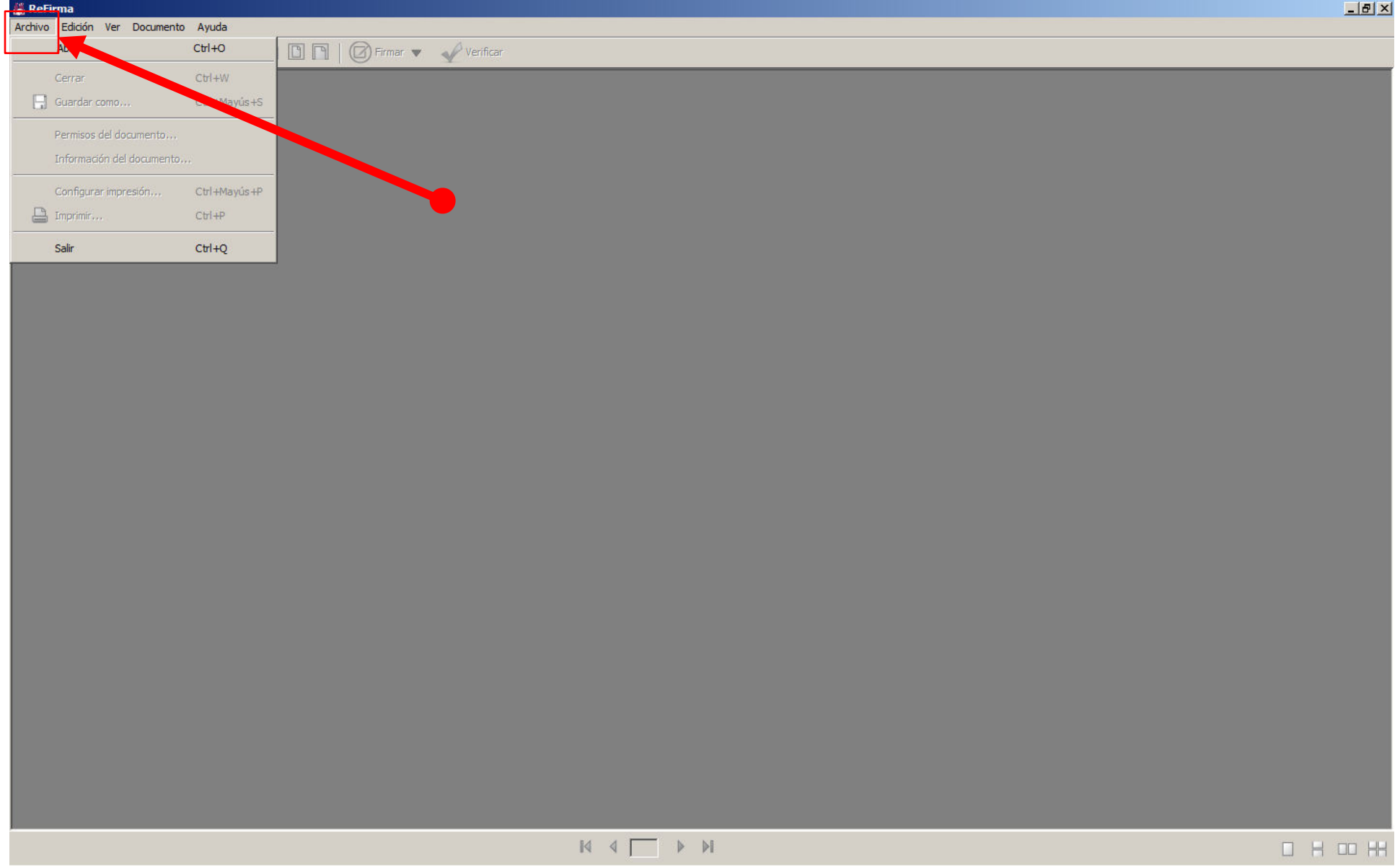
Para tal verificación, hemos tenido en primer lugar, que guardar el documento firmado digitalmente y que queremos verificar en nuestra PC.

Ubicamos el icono "ReFirma 1.1.0" en el escritorio del computador y damos doble click para ejecutar el software de Firma Digital ReFirma.

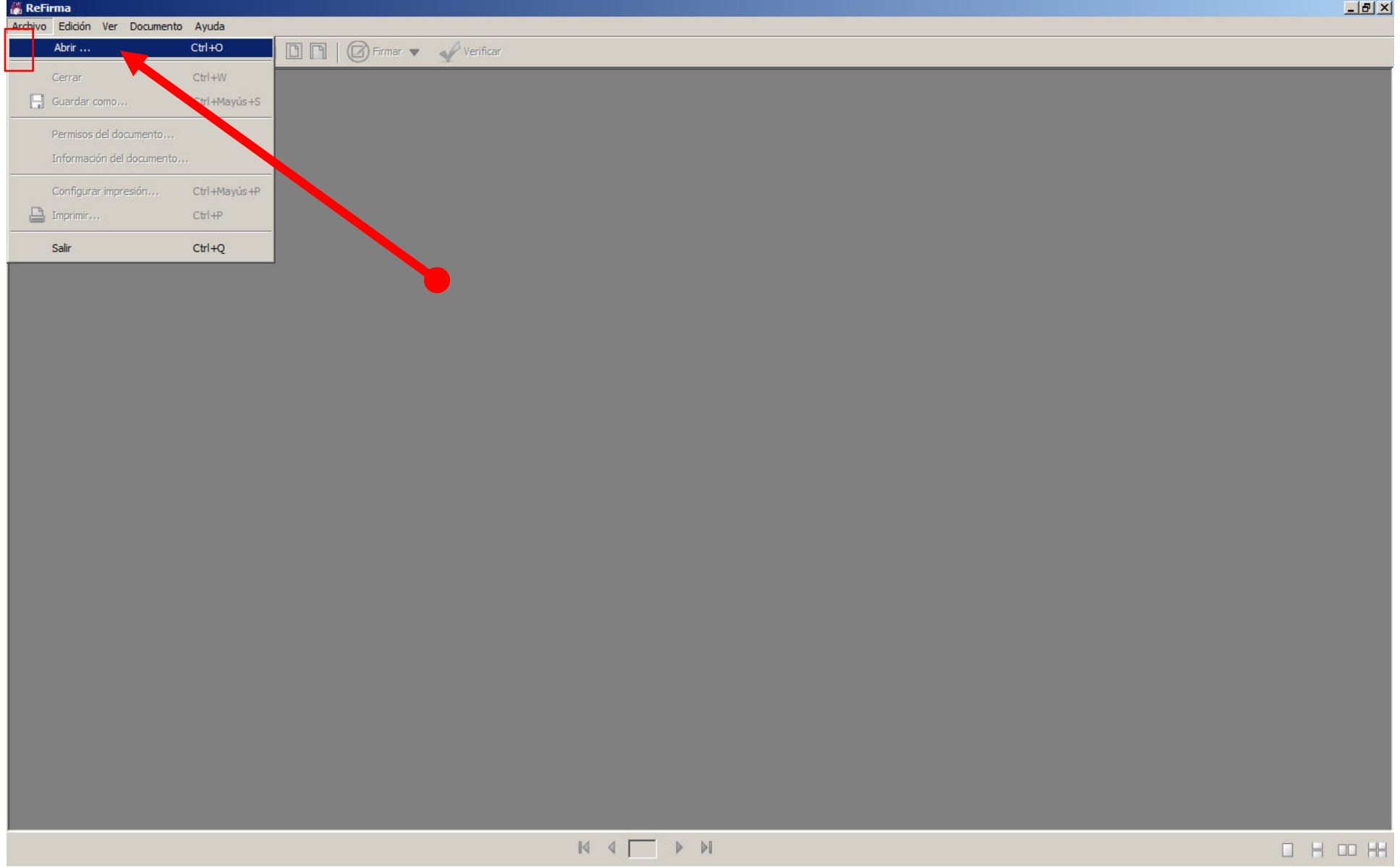
Ubicamos el icono "ReFirma 1.1.0" en el escritorio del computador y damos doble click para ejecutar el software de Firma Digital ReFirma.



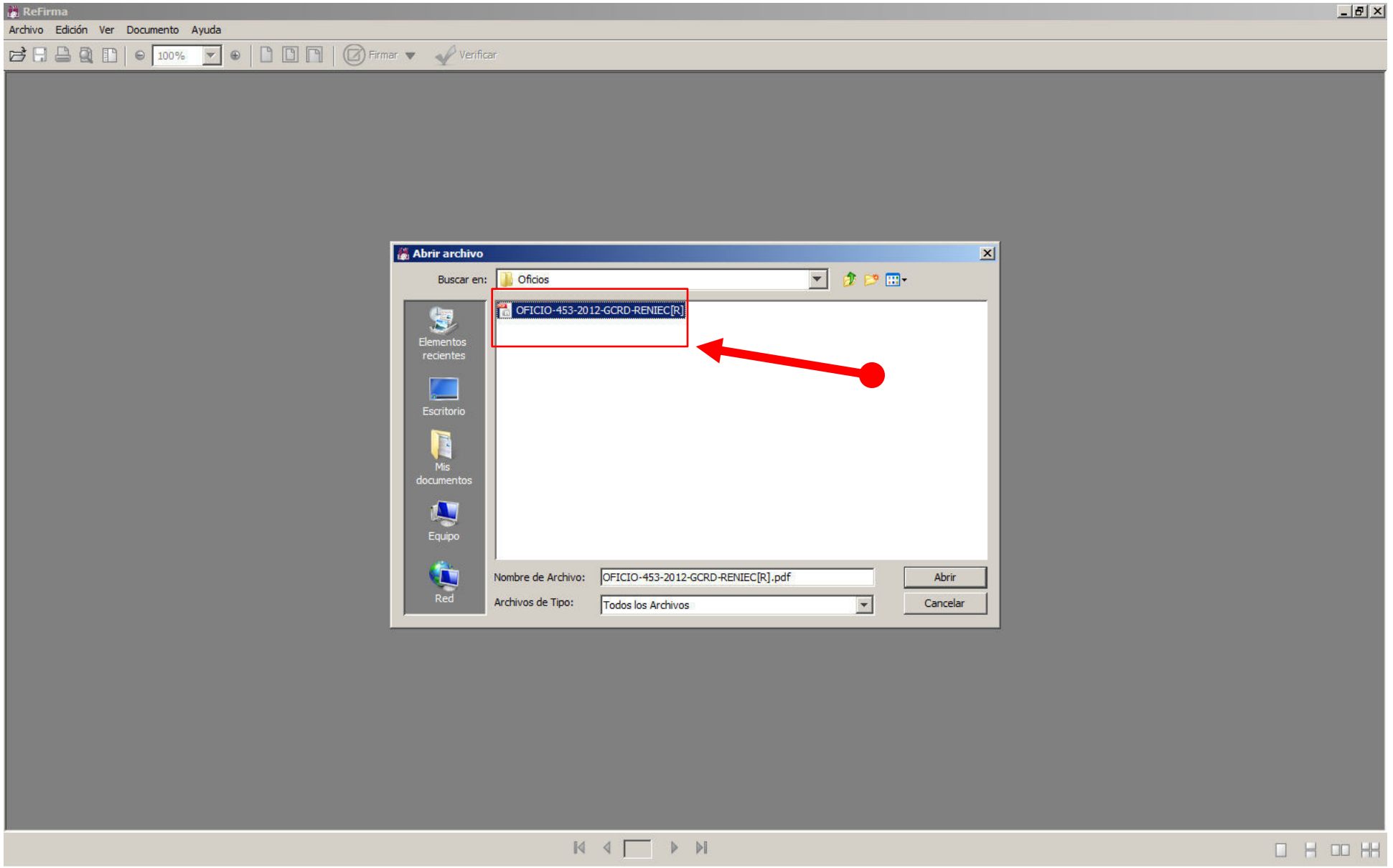
A continuación nos mostrara la ventana principal del software ReFirma



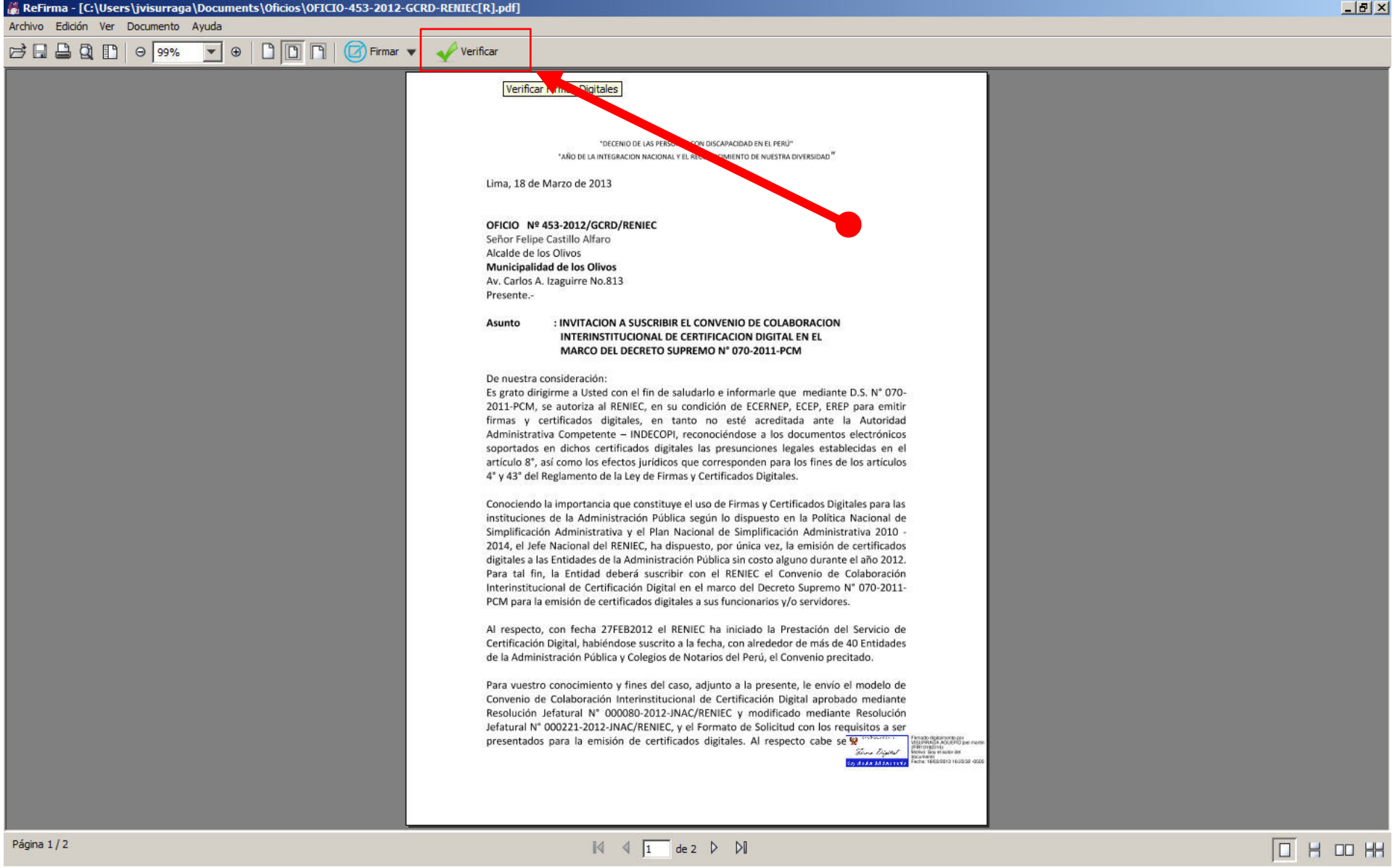
Ubicamos la opción <Archivo> en la barra del menú principal y damos click para desplegarse las subopciones.



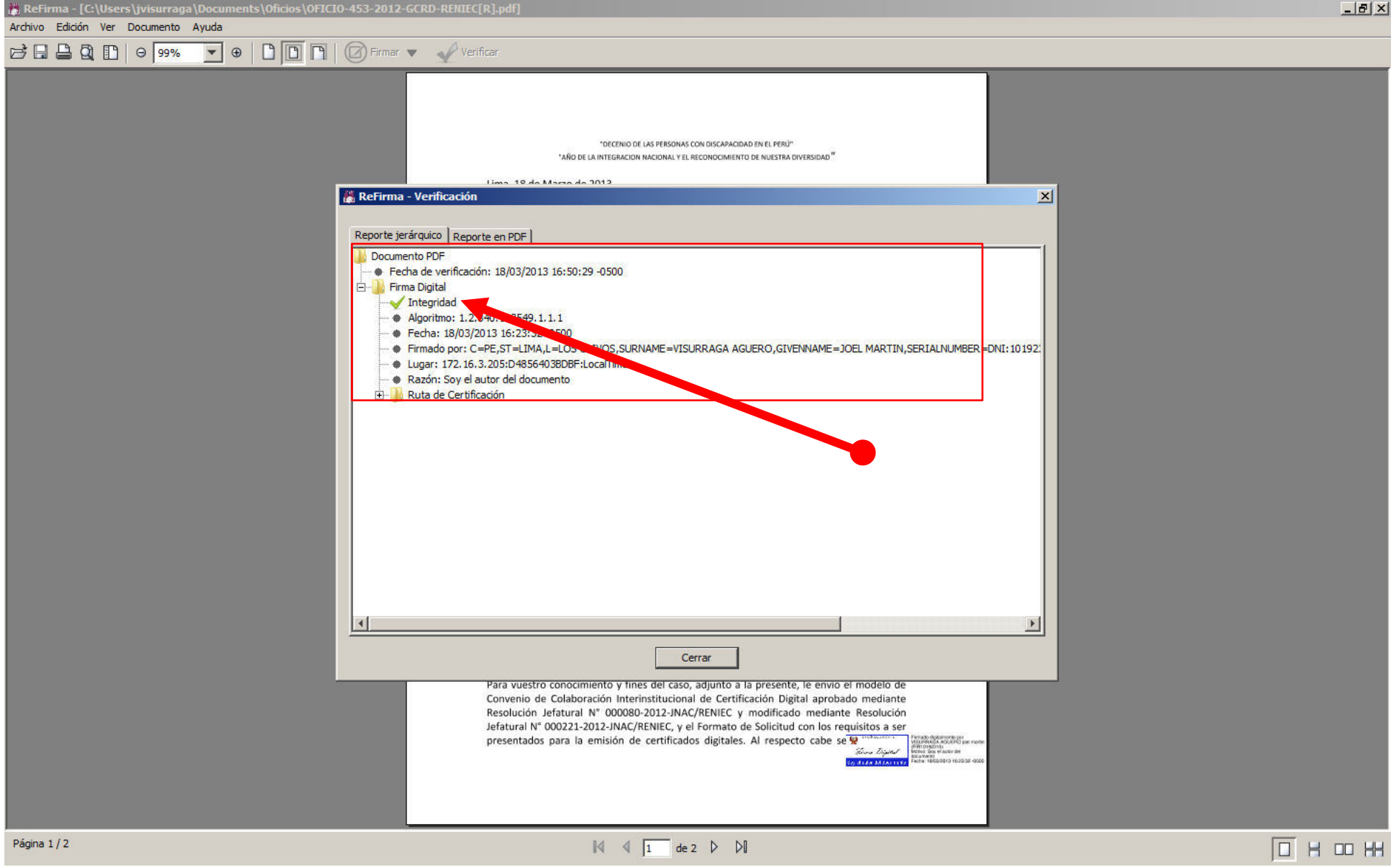
Ubicamos la sub-opción <Abrir> y le damos click.



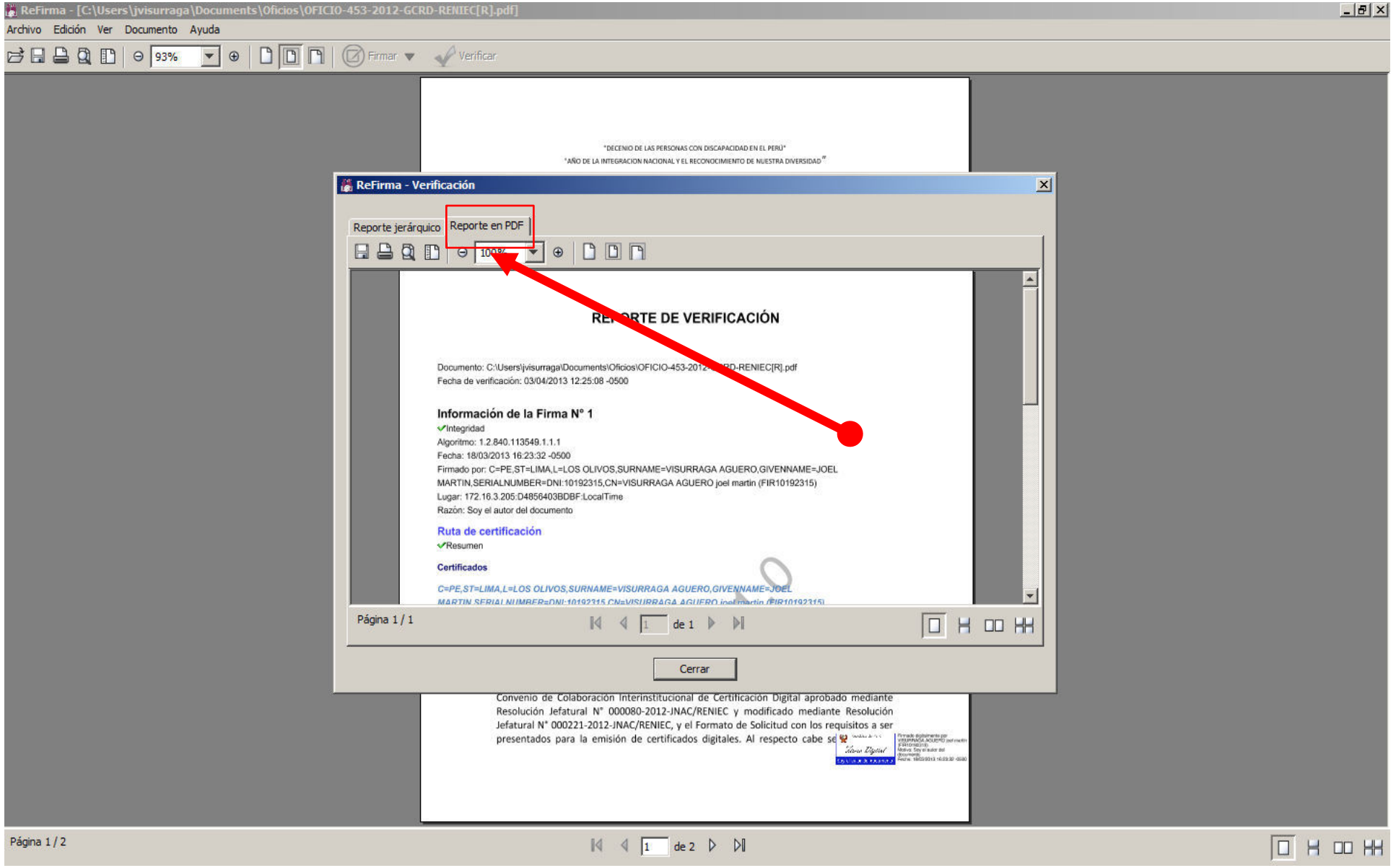
Al abrirse la ventana "Abrir archivo" ubicamos el documento firmado digitalmente que nos enviaron y que previamente hemos guardado en nuestra PC.



Damos click al ícono al ícono [Verificar] ubicado en la barra del menú principal.



Es así como se muestra la ventana "ReFirma - Verificación" que detalla que el documento es íntegro y cuyo contenido no ha sido alterado.



Asimismo eligiendo la opción [Reporte en PDF] podemos obtener ese mismo reporte en tal formato a fin de poder guardarlo o imprimirlo.

Firma Digital

Argentina

2023

Firma Digital

Manual para SAS de Ciudad Autónoma de Buenos Aires

Versión 2.0 - 03/2019

Inspección General de Justicia

Ministerio de Justicia y Derechos Humanos
Presidencia de la Nación

Introducción

¿Qué es?

La firma digital es una solución tecnológica que permite ***añadir*** a documentos digitales y mensajes de correo electrónico una ***huella o marca*** única, a través de ciertas operaciones matemáticas.
La firma digital permite al receptor del mensaje o documento:

- Identificar al firmante de forma fehaciente (***Autenticación)***
- Asegurar que el contenido no pudo ser modificado luego de la firma sin dejar evidencia de la alteración (***Integridad)***
- Tener garantías de que la firma se realizó bajo el control absoluto del firmante (***Exclusividad)***
- Demostrar el origen de la firma y la integridad del mensaje ante terceros, de modo que el firmante no pueda negar o repudiar su existencia o autoría (***No Repudio***)

Conforme la ~~Ley 25.506~~ que la firma manuscrita de los documentos en papel, ya
que posee las mismas características técnicas de seguridad que una firma en papel, e incluso mayores.

¿Para qué sirve?

Facilita el reemplazo de documentación en papel por su equivalente en formato digital. Ahorra costos, simplifica procedimientos y brinda seguridad en el intercambio de información.

Se utiliza principalmente para firmar documentos PDF y correos electrónicos, pero también permite firmar documentos de texto, plantillas, imágenes y virtualmente cualquier tipo de documento. Su tecnología está incorporada en transacciones electrónicas, formularios web y navegación en páginas seguras.

¿Cómo funciona?

La tecnología de firma digital se sostiene de dos pilares: un método que hace imposible la alteración de la firma y una infraestructura que permite certificar la identidad del firmante.

Clave Asimétrica

La Clave Asimétrica es un método de criptografía o codificación, en el que se generan dos números de gran longitud (usualmente más de 200 cifras) mediante una fórmula matemática compleja. Estos números, llamados “claves”, son distintos, pero están relacionados de modo tal que ***lo que se cifra o encripta con una clave sólo puede descifrarse con la otra***. A este par de claves se los conoce como ***Clave Pública*** y . La clave pública se distribuye y la clave privada la conserva el propietario, protegida por una o varias contraseñas que sólo él conoce. El par de claves funciona siempre en conjunto: No es posible cifrar y descifrar un documento con una misma clave.
Cuando se aplica la clave privada sobre un documento digital en su totalidad, este queda cifrado o encriptado. Es decir, se vuelve ilegible para cualquiera que no posea la clave pública con que descifrarlo. En firma digital, ya que no se busca encriptar el mensaje sino darle una marca de autenticación, la clave asimétrica se utiliza de forma indirecta, no sobre el documento, sino sobre un resumen del mismo, denominado hash.

Hash

El hash (también conocido como digesto o huella digital), es un resumen único que identifica a un documento digital. Se puede aplicar a cualquier tipo de documento, incluso a una cadena de texto. Se obtiene al aplicar una fórmula matemática llamada ***“función unidireccional de resumen”***, o función hash. El resultado suele expresarse en números y letras minúsculas de la “a” a la “f” (sistema hexadecimal). Un ejemplo de hash podría ser:
165d5f1615a80bf0e106df3954c5a73439f659cf02d6c2eb760c21076fb17043

- Es un ***resumen***, porque sin importar el tamaño del documento, la función devuelve un hash de la misma longitud.
- Es ***unidireccional***, porque no es posible convertir el hash nuevamente en el documento original, ni conocer el contenido del documento a partir del hash.
- Al ser una ***función matemática***, aplicarla sobre un ***mismo documento*** mensaje devuelve .
- Es estadísticamente ***imposible*** encontrar dos documentos distintos que posean el mismo hash.
- Dos documentos pueden parecer a ***simple vista*** idénticos, pero poseer distinto hash. Aunque parezcan idénticos, si el hash difiere, ***no pueden*** considerarse el mismo documento digital.

Firma

Existe una gran variedad de aplicaciones para firmar digitalmente, pero en esencia todas funcionan del mismo modo:

1. Al momento de firmar, la aplicación calcula el hash del documento.
2. Luego utiliza la clave privada para cifrar ese hash (es en ese momento cuando solicita la contraseña con la que el usuario protegió su clave privada)
3. Finalmente, el hash cifrado se incorpora, junto con otros datos (fecha y hora de firma, datos del firmante, etc), como anexo del documento, obteniendo así un documento firmado digitalmente.

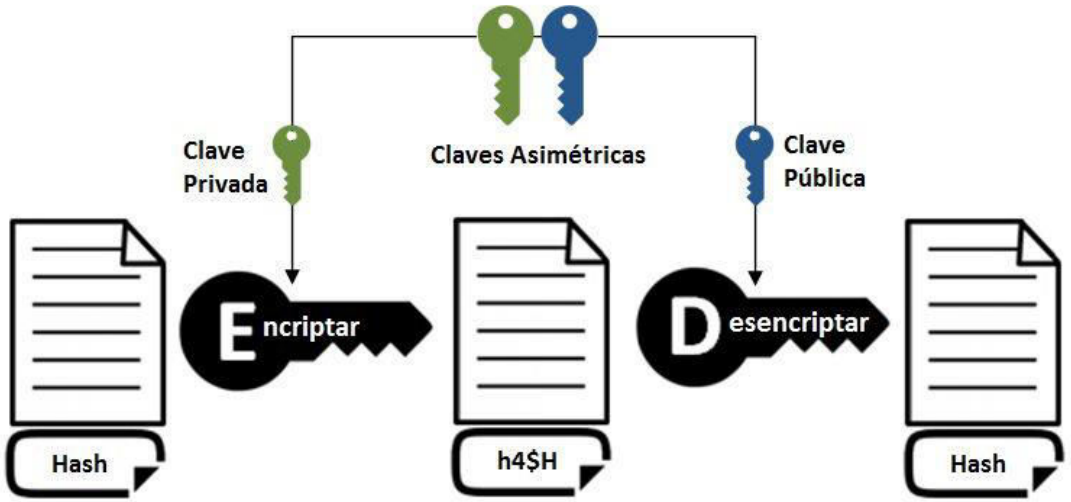
Autenticación

Cualquiera receptor del documento que posea la clave pública puede autenticarlo. Para ello solo debe:

1. Calcular el hash del documento.
2. Descifrar el hash contenido en la firma digital.
3. Compararlos.

Sí los hash coinciden, el receptor puede confirmar dos cosas:

- El contenido del documento no fue alterado luego de la firma,
- la clave privada con que se firmó coincide con la clave pública.



Certificado Digital

Para que el procedimiento de firma y autenticación sea confiable, necesitamos la seguridad de que esa clave pública efectivamente pertenece al firmante. Por eso, el segundo elemento que sostiene el sistema de firma digital es la "Infraestructura de Clave Pública" (PKI, en inglés), que regula cómo se emiten y distribuyen las claves. Para esto, utilizan documentos llamados Certificados de Clave Pública, o según nuestra normativa, Certificados Digitales. Un ***Certificado Digital*** es simplemente un documento firmado digitalmente por una autoridad, en el cual se atestigua que una clave pública pertenece a un determinado individuo o entidad. En general, contiene datos de identidad de la persona, su clave pública y el nombre de la autoridad que emitió el certificado. Todos los datos de identidad son previamente validados por esta autoridad, y el certificado se puede autenticar de la misma forma que cualquier otro documento con firma digital.

La Infraestructura de Clave Pública es el conjunto de procedimientos, políticas y roles normados que definen cómo se generan y organizan esos certificados. Si el certificado es auténtico y confiamos en la autoridad emisora, podemos asegurar la identidad del firmante. En nuestro país, esta regulación se conoce como ***Infraestructura de Firma Digital de la República Argentina (IFDRA)***.

¿Quién la regula?

La ***Autoridad de Aplicación*** establecida en la Ley N° 25.506 de Firma Digital. Actualmente el rol lo desempeña la ***GOBIERNO DE MODERNIZACIÓN*** (SGM) de la JEFATURA DE GABINETE DE MINISTROS. Actúa como , otorgando, denegando o revocando las licencias de los Certificadores Licenciados.

La ***Autoridad Certificante Raíz*** (AC-RAÍZ), operada por el Ente Licenciante, es el primer nivel de jerarquía en la IFDRA. Emite certificados digitales a las Autoridades Certificantes de segundo nivel, una vez aprobados los requisitos de licenciamiento.

Los ***Certificadores Licenciados*** son entidades públicas o privadas que se encuentran habilitados por el Ente Licenciante para emitir certificados digitales a personas. Estos operan cada ***Autoridad Certificante*** de .
Cada Certificador Licenciado delega en ***Autoridades de Registro*** las funciones de validación de identidad y otros datos de los suscriptores de certificados.

¿Cómo la obtengo?

Firma Digital Token: Requiere un dispositivo físico donde se almacena el certificado. Puede verificar los _____ un Certificado de Firma Digital Token, y dirigirse ante cualquier Autoridad de Registro con alguno de los Certificadores Licenciados.

Firma Digital Cloud: Permite firmar a través de una plataforma online. Puede consultar características, requisitos y forma de obtenerla en la Plataforma de Firma Digital Remota (PFDR)

Validación de Firma

Cómo Reconocer una Firma Digital

La firma digital es un pequeño bloque de información que suele anexarse o “incrustarse” al documento firmado. No es directamente visible en el documento, pero la mayoría de las aplicaciones que trabajan con documentos permiten distinguir cuales están firmados y ver los detalles de la firma. Muchos documentos poseen además un ***sello*** o en el texto, que indica datos del firmante o emula la firma manuscrita. Este sello puede ayudarnos a distinguir un documento firmado, pero el sello y la firma digital ***no son lo mismo***. Un documento firmado digitalmente puede carecer de sello, y puede existir un documento sellado sin firma digital.

Diferencia entre Firma Electrónica y Firma Digital

La ley define a la firma electrónica como “*al conjunto de datos electrónicos integrados, ligados o asociados de manera lógica a otros datos electrónicos, utilizado por el signatario como su medio de identificación, que carezca de alguno de los requisitos legales para ser considerada firma digital*”. Entonces, para poder ser considerada firma electrónica, el procedimiento debe al menos poseer las propiedades de Autenticación e Integridad, y por ende No Repudio. La diferencia entre una Firma Digital y una Firma Electrónica es que la primera se realiza con un Certificado Válido. Los ejemplos más comunes de firma electrónica son:

- Las firmas realizadas con certificados que ***no fueron emitidos por un Certificador Licenciado***, incluyendo
  - certificados emitidos por autoridad certificante ***extranjera*** (salvo las que cumplan los requisitos del art. 16 ley 25.506),
  - certificados emitidos por un ente nacional, privado o público ***sin licencia***,
  - certificados generados ***por el propio firmante*** mediante alguna aplicación informática.
- La firma realizada con certificado válido (emitido por un Certificador Licenciado) pero ***expirado o revocado*** antes de firmar.
- Las firmas de documentos generados mediante las plataformas de ***Trámites a Distancia*** (TAD) y GDE, salvo los casos en que al firmar se haya utilizado un ***Token*** o .

Conforme la ley, la firma electrónica tiene valor legal, pero no tiene el mismo valor de prueba que la firma digital. Si alguien niega o desconoce una firma digital, esa persona tiene que probar que la firma es falsa. En cambio, si alguien niega o desconoce una firma electrónica, es la otra parte quién debe que probar que la firma es auténtica. Si la Firma Digital es comparable a la Firma Certificada en papel, la Firma Electrónica lo es a la Firma Simple. Cuando una norma u organismo exija firma digital, no es suficiente la firma electrónica.

Jerarquía de Certificados

Tal como se menciona en el apartado de Certificados Digitales una Autoridad Certificante. ¿Pero cómo puedo saber si esa firma es realmente de la autoridad? Por este motivo es que también existen certificados digitales de estas autoridades, los cuales son firmados a su vez por una entidad de mayor jerarquía. Se genera así una "***cadena de confianza***" en la que con sólo adquirir el certificado de la autoridad máxima de manera segura, podremos validar sucesivamente los certificados de menor jerarquía. Conforme la Infraestructura de Firma Digital Argentina, existen dos niveles de autoridad:

1° - Autoridad Certificante Raíz - AC-RAÍZ

Es la autoridad operada por el Ente Licenciante, y por lo tanto, la de mayor jerarquía. Sus certificados son básicos para poder validar cualquier firma digital, y se conocen como Certificados Raíz. Los certificados raíz están firmados por la propia autoridad.

- Certificado AC-RAIZ RA 2007

  Certificado AC-RAIZ RA V2

2° - Certificadores Licenciados

Son todos aquellos que el Ente Licenciante habilitó a emitir certificados digitales para personas. Se consideran Autoridades Certificantes de segundo nivel, y sus certificados se conocen como Certificados Intermedios. Cada uno de estos certificados es necesario para validar las firmas de todas aquellas personas que hayan adquirido la firma digital con ellos.

- Certificado Autoridad Certificante ONTI

  Certificado Autoridad Certificante AFIP

- Certificado Autoridad Certificante Modernización PFDR

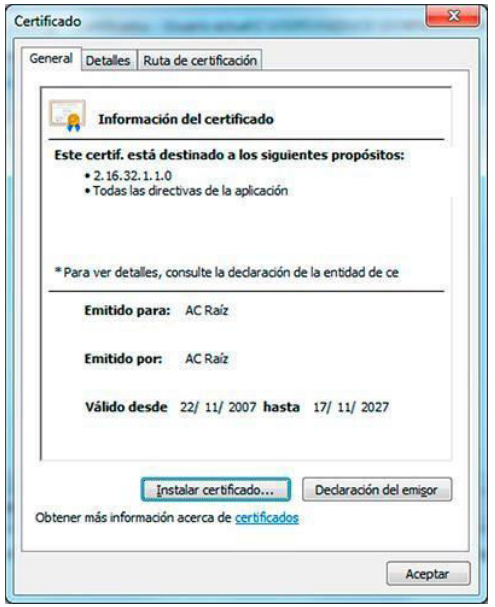
Se enumeran aquí los principales certificados utilizados en la Administración Pública Nacional. En caso de necesitar validar otros documentos, el listado completo de Certificadores Licenciados se encuentra en la página de Firma Digital Argentina: https://www.acraiz.gob.ar/Home/CertificadoresLicenciados

Aún en aquellos casos en que el emisor de un certificado no fuera una autoridad reconocida, es posible adquirir los certificados intermedios del emisor e instalarlos. Eso permitirá validar los documentos firmados con certificados provistos por ese emisor. Esto no es recomendable salvo que se confíe plenamente en la idoneidad del emisor, y aún en estos casos, debe tenerse en cuenta que la firma de dicho documento puede no ser reconocida por terceros, ya que se considera firma electrónica

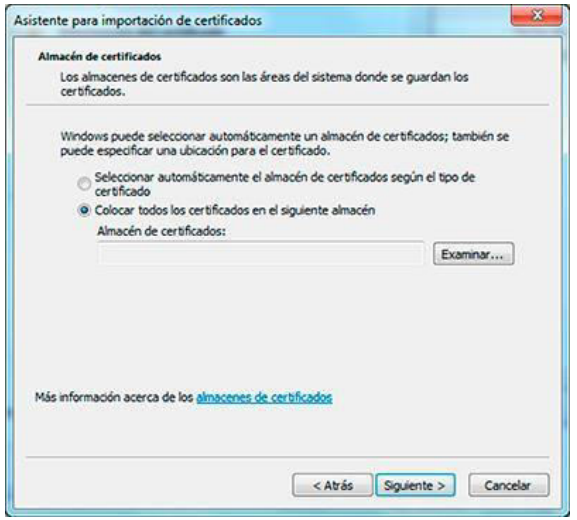
Instalación de Certificados AC

Como paso previo a realizar la verificación de una firma digital, el equipo o dispositivo debe tener correctamente instalados los certificados raíz e intermedios. ***Nota****Para instalar el certificado AC se recomienda haber iniciado una sesión con un usuario con permisos de administrador en su PC.*

1. Descargar el archivo de certificado.
2. Una vez finalizada la descarga, abrir el archivo haciendo doble clic.
    a. Si apareciera una advertencia de seguridad, seleccionar “Abrir”
3. En la ventana de información, hacer click en “Instalar certificado”.

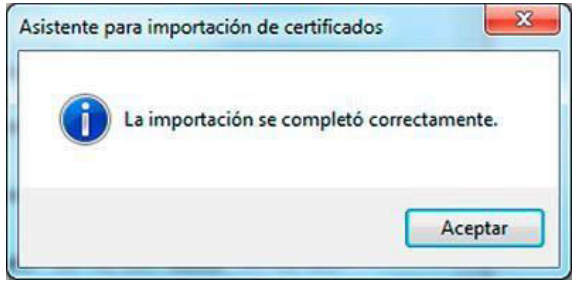


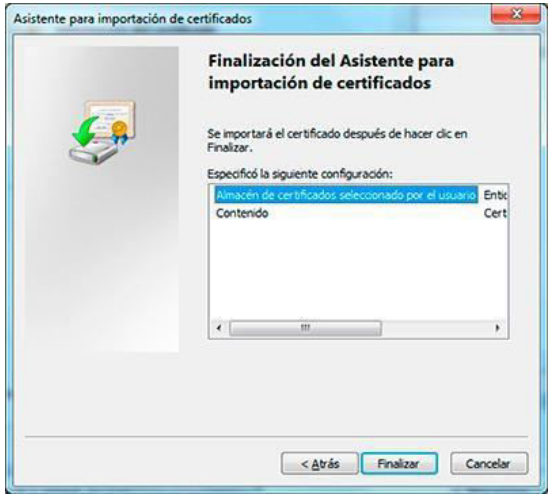
4. Una vez abierto el Asistente para importación de certificados, hacer click en “Siguiente”.
5. Seleccionar la opción “Colocar todos los certificados en el siguiente almacén” y hacer clic en “Examinar”.
6. Seleccionar el almacén de certificados que corresponda con el nivel:



a. Sí es un Certificado Raíz, seleccionar la carpeta “Entidades de certificación raíz de confianza”
b. Sí es un Certificado Intermedio, seleccionar la carpeta “Entidades de certificación intermedias”

7. Hacer click en “Siguiente” y luego “Finalizar”.
8. Si el certificado se importó con éxito, debería aparecer la ventana final indicándolo.





Todos los certificados instalados pueden consultarse ingresando desde Windows al Panel de Control>Opciones de Internet>Contenido>Certificados. Además de los certificados instalados manualmente, se verán todos los que el sistema operativo instala de manera predeterminada.

Vigencia de los Certificados

Cuando una autoridad de certificación emite un certificado digital, lo hace por un periodo máximo de validez que oscila entre uno y cinco años (los certificados intermedios y raíz también la tienen, pero períodos más amplios). El objetivo de este periodo de caducidad es obligar a la renovación del certificado para adaptarlo a los cambios tecnológicos. Así se disminuye el riesgo de que el certificado quede comprometido por un avance tecnológico. La fecha de caducidad o expiración viene indicada en el propio certificado digital. Sin embargo, existen otras situaciones que pueden invalidar el certificado digital aún cuando no ha expirado, de manera inesperada:

- El usuario del certificado cree que su clave privada o el token con el certificado se extravió o fue robado.
- Desaparece la condición por la que el certificado fue expedido. Por ejemplo, el cambio de apoderado de una entidad jurídica. El certificado contiene información errónea o información que ha cambiado. Por ejemplo, una errata en los apellidos.
- Una orden judicial, etc.

Por tanto, debe existir algún mecanismo para comprobar la validez de un certificado antes de su caducidad. Los principales mecanismos para verificar esto son las ***CRL (Certificate Revocation List)*** y . Una CRL es una lista de certificados que la autoridad emisora decretó que ya no son válidos, y en los que no debe confiar ningún sistema de usuario. Un OCSP consulta ese listado y devuelve el estado de revocación de un certificado.
El vencimiento o revocación de un certificado ***no invalida todas*** las firmas realizadas con el mismo, sino tan solo aquellas que fueron realizadas en un momento posterior a su fecha y hora de caducidad/revocación.
En caso de necesitar revocar un certificado, deberá consultar a la Autoridad de Registro que se lo emitió. Adicionalmente puede consultar los procedimientos de revocación para Firma Token (con Clave Privada

Verificación

Existen muchas aplicaciones que permiten verificar la firma digital. En este instructivo se explica como hacerlo para documentos en formato PDF, mediante el software gratuito Xolido Sign
DC). Debido a ciertas limitaciones del software de Adobe, ***recomendamos la utilización de Xolido***.
Condición previa, deberá haberse descargado e instalado el software elegido desde la página oficial.

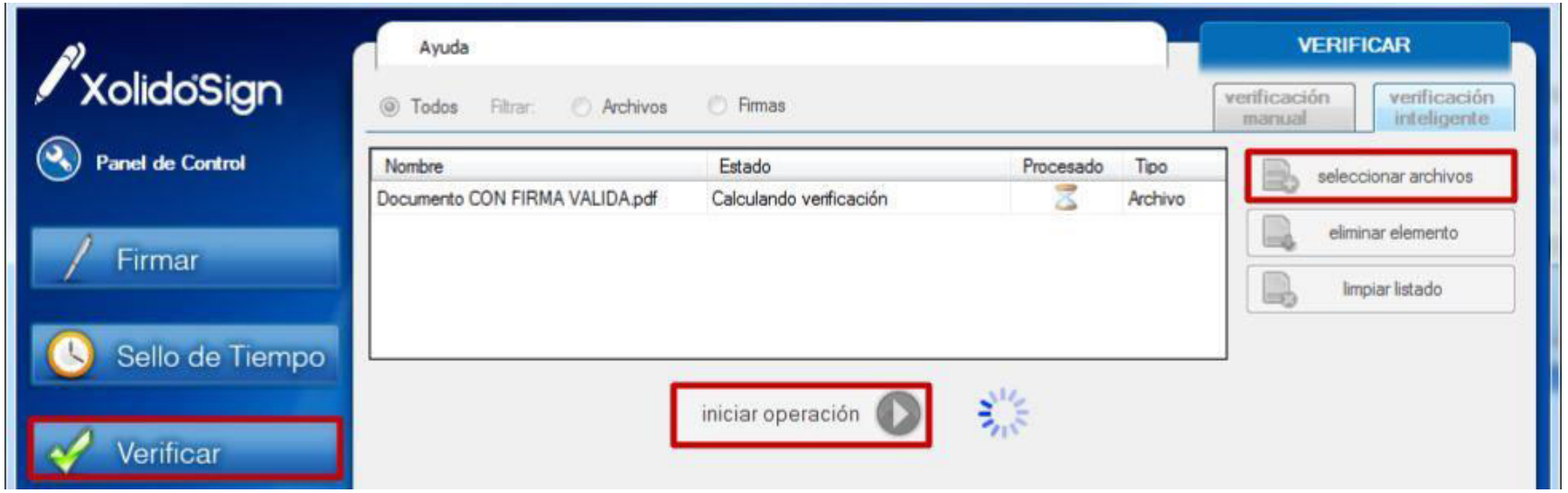
Importante:*Si la red donde se encuentra el equipo utiliza un servidor proxy o una configuración especial para acceder a Internet, deberá contactar a su administrador de red o asegurarse que el software elegido posee acceso. Esto permite al software realizar verificaciones sobre la hora de firma y estado de revocación del certificado.*

A. En el caso de Xólido, debe ingresar al menú Opciones Globales>Opciones Avanzadas>Configuración de Proxy, y seleccionar “usar configuración establecida en Internet Explorer” (los usuarios avanzados pueden optar por configurar manualmente el proxy)
B. En el caso de Adobe, la configuración por defecto utiliza la configuración de Internet Explorer. En caso de necesitar personalizarla, debe ingresar al menú Edición>Preferencias>Internet.

Xolido Sign

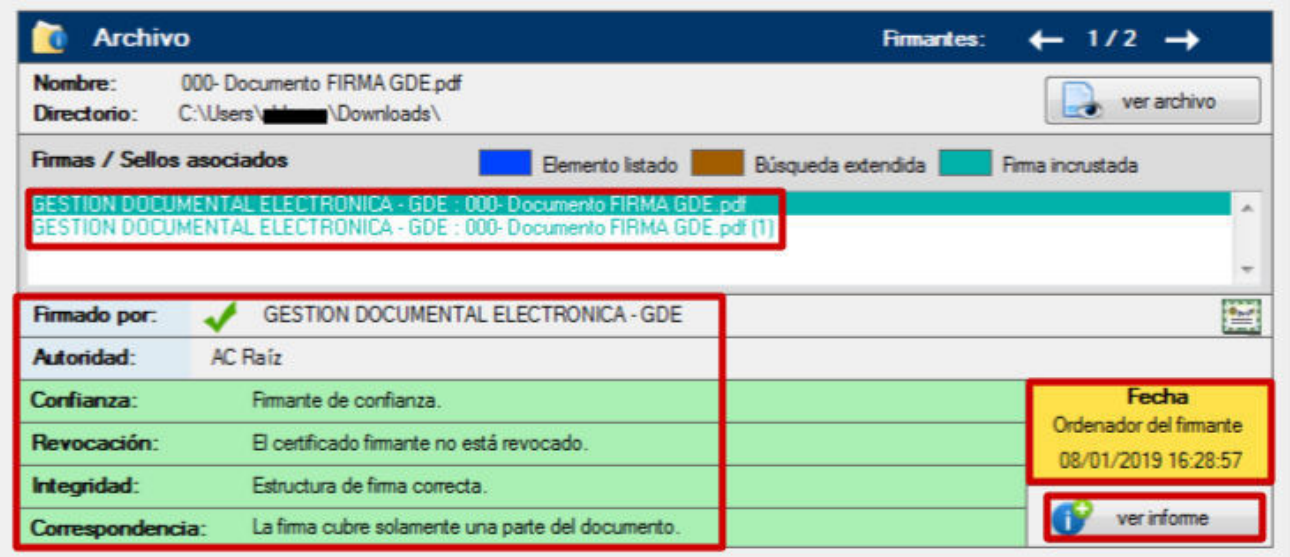
Xolido Sign es una aplicación especialmente diseñada para trabajar con firmas digitales. Sirve tanto para firmar como para verificar firmas en varios tipos de archivo. En este instructivo se detallará únicamente el procedimiento de verificación de firma en documentos PDF. Para mayor información, puede consultar en Manual de Usuario al que puede accederse desde la aplicación.

1. Abrir el programa e ingresar en la opción Verificar. Se utilizará la modalidad de “verificación inteligente” (opción por defecto).
2. Hacer click en “seleccionar archivos” y elegir el documento cuya firma desea verificar (verificar de a un documento por vez)
3. Finalmente, presionar “Iniciar operación”.



Si informa que “no ha podido procesar la información asociada”, ese archivo carece de firma digital.

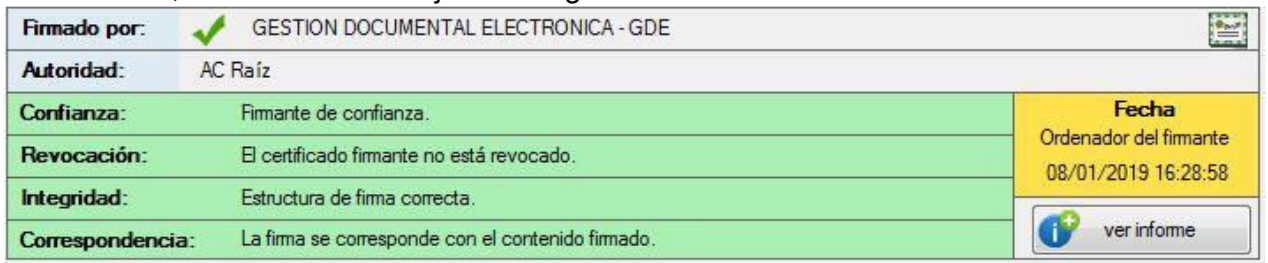
4. Una vez procesado el archivo, se abrirá un panel inferior que contiene toda la información de las firmas verificadas.
   También permite desplegar un análisis más detallado presionando el botón "***Ver informe***".



Firmas / Sellos asociados: Lista todas firmas que se hayan realizado sobre el documento. Las firmas deben seleccionarse una por una a fin de ver detalles y validez de cada una de ellas.
Firmado por: Indica el nombre del firmante de la firma seleccionada.
Autoridad: Indica qué autoridad emitió el certificado raíz (ver apartado
Confianza:
confianza completa (los certificados intermedios y certificado raíz deben estar instalados).
Revocación: Verifica si el certificado de firma fue revocado por la autoridad certificante. Informa también si pudo comprobarse o no el estado de revocación.
Integridad: Informa si el proceso de firma se realizó correctamente.
Correspondencia: Informa si el documento coincide con el firmado, o fue modificado con posterioridad a la firma.
Momento de la Firma: Indica fecha y hora de la firma, así como de dónde procede este dato.

Respuestas Usuales

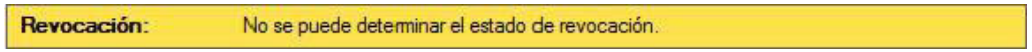
Idealmente, la verificación arrojará los siguientes resultados:



Esto indica que es una firma pasó satisfactoriamente todas las revisiones. Sin embargo también pueden obtenerse los siguientes resultados:

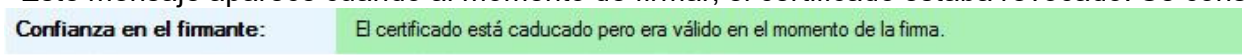
Este mensaje aparece cuando existen múltiples firmas en un documento. Cada firma añade un “anexo” al documento, y cada nueva firma se realiza sobre la anterior, por lo que solo la última de las firmas se realiza sobre el documento final completo.

Todos los certificados de firma digital deben se emitidos por Certificadores Licenciados, y en consecuencia, como Autoridad siempre debe figurar “AC Raíz” o “AC Raíz de la República Argentina”. Caso contrario, se considera *Firma Electrónica*.



El estado de revocación debería poder consultarse para cualquier certificado emitido por Autoridad Certificante. Este mensaje suele aparecer cuando el software no puede acceder a internet (ver apartado verificación y el certificador no posee un método de verificación del estado de revocación.

Este mensaje aparece cuando al momento de firmar, el certificado estaba revocado. Se considera *Firma Electrónica*.

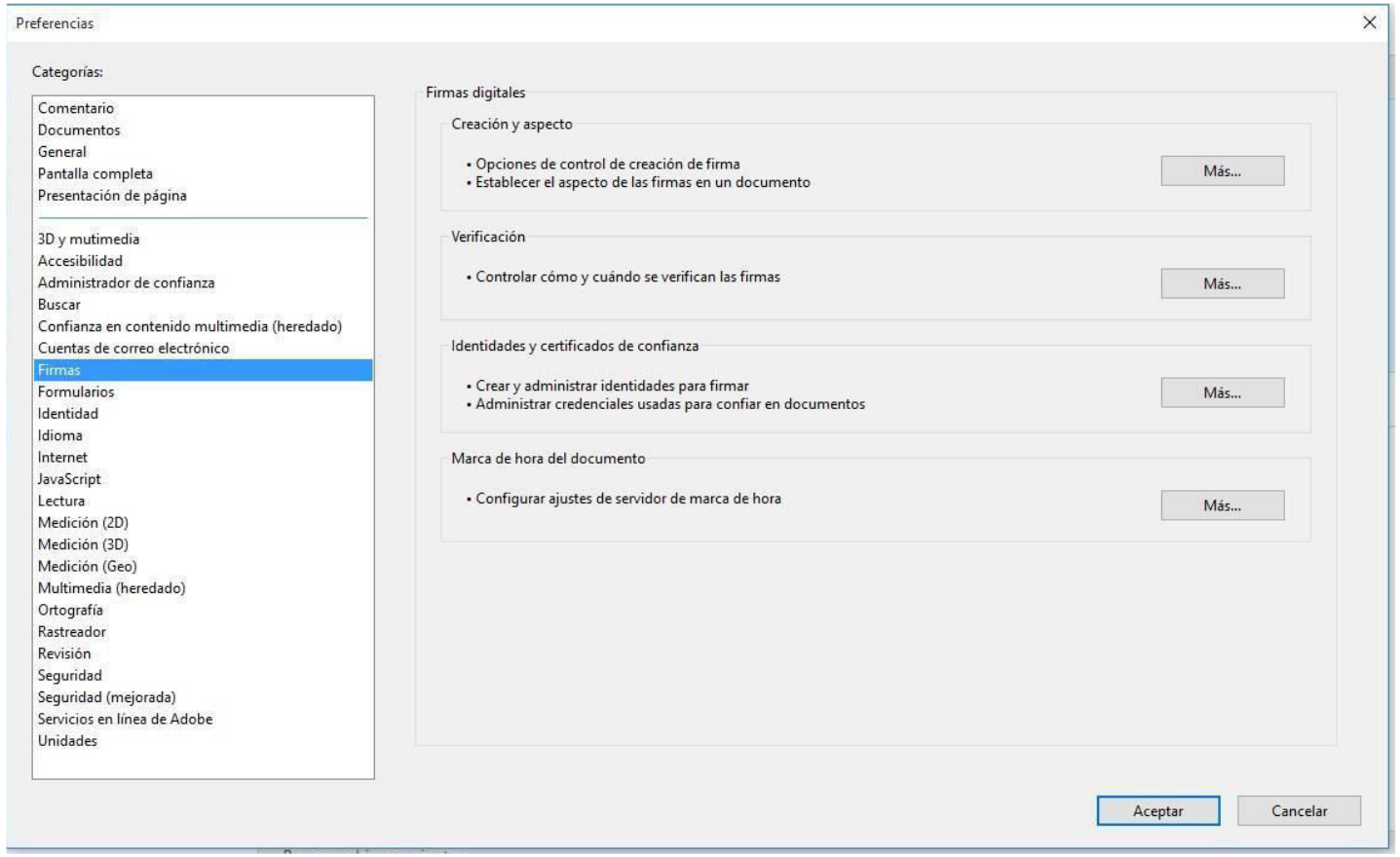


Cuando un certificado haya expirado o sido revocado, pero era válido al momento de la firma, la verificación inicial saldrá correcta. Ingresando al informe detallado, puede verse el estado actual de vigencia y revocación. Para asistencia sobre el informe detallado y otros mensajes de advertencia y error, consulte el manual de usuario de Xolido Sign.

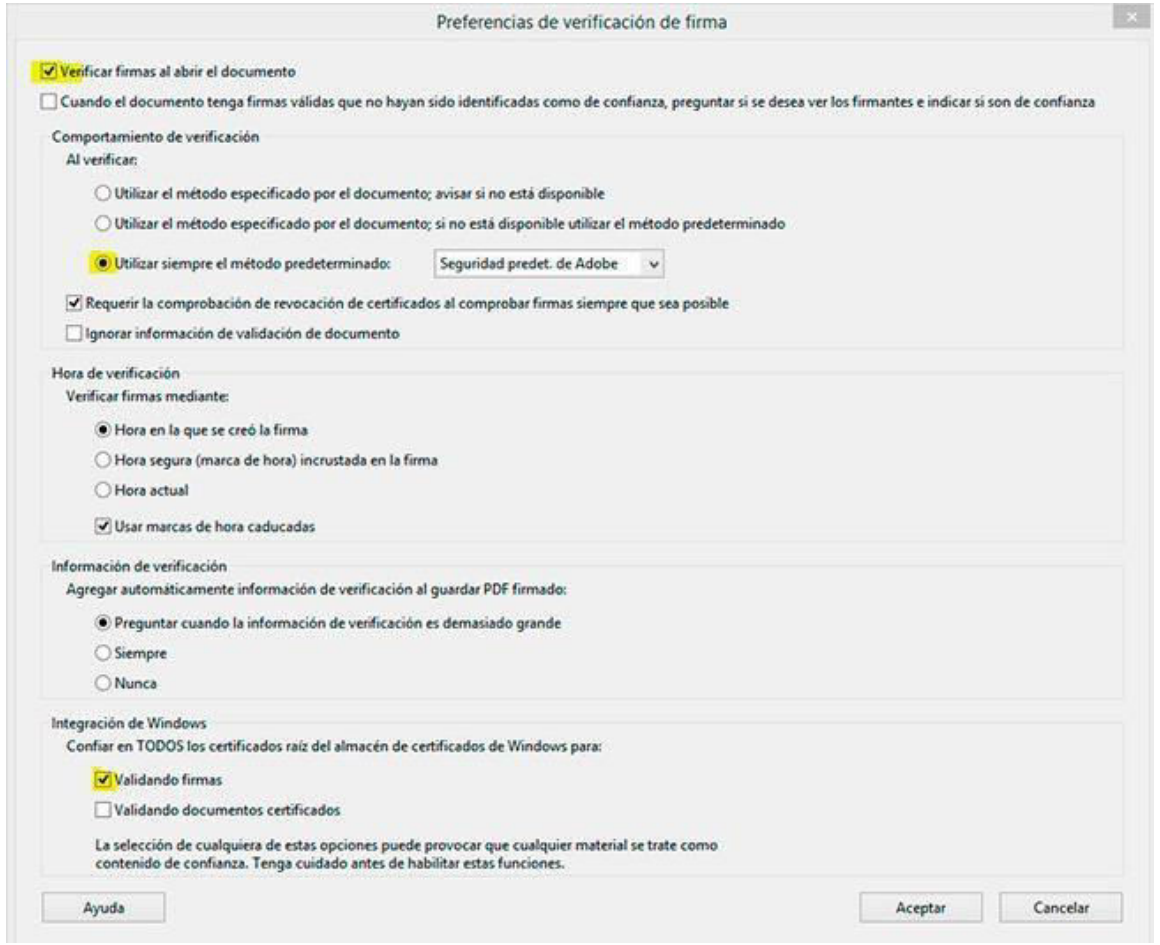
Adobe

Configuración

1. Ingresar al menú Edición > Preferencias, y allí, al apartado Firmas.
2. Desplegar las opciones de Verificación, presionando el botón Más.

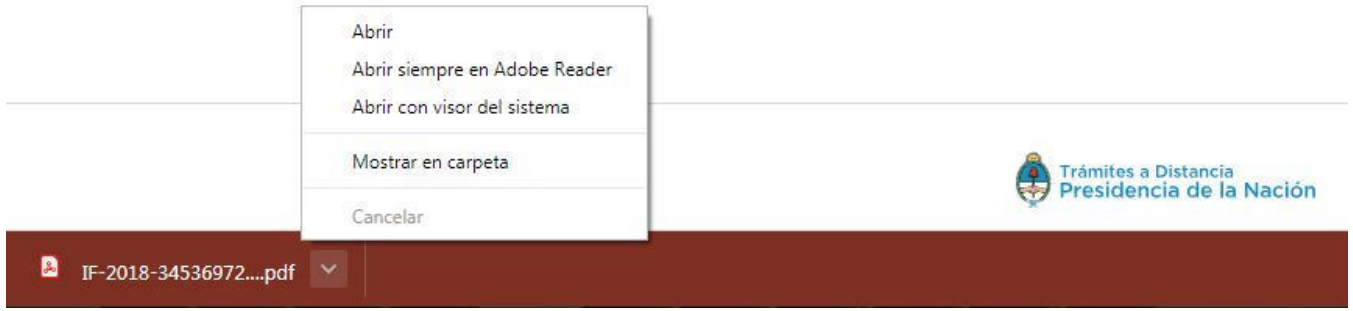


3. Tildar la opción “Verificar firmas al abrir el documento”.
4. En “Comportamiento de verificación”, seleccionar la opción “Utilizar siempre el método predeterminado, y allí, la opción “Seguridad predeterminada de Adobe”
5. En “Integración con Windows”, tildar la opción “Validando firmas”.

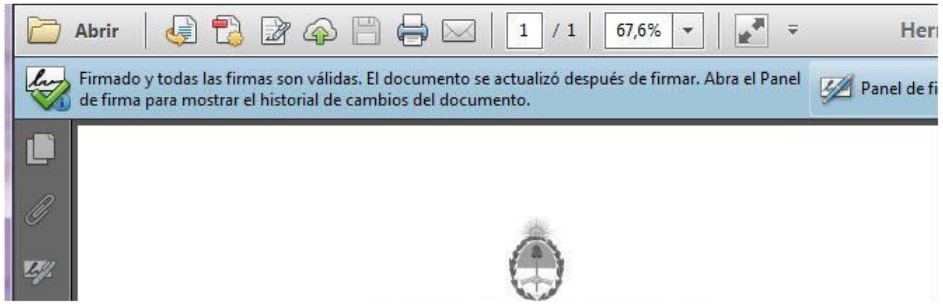


Verificación

1. Abrir el documento a validar mediante Adobe Reader.
    a. Si el documento fue descargado de la Web, y por defecto se abre con el visor del navegador Chrome, abrirlo desde el Explorador de Windows, o al descargar, presionar la flecha que se encuentra a la derecha del icono de documento descargado, y seleccionar la opción “Abrir con visor del sistema”.



2. Al abrir el documento, en la parte superior, bajo la barra de herramientas, aparecerá el mensaje de comprobación de firmas.

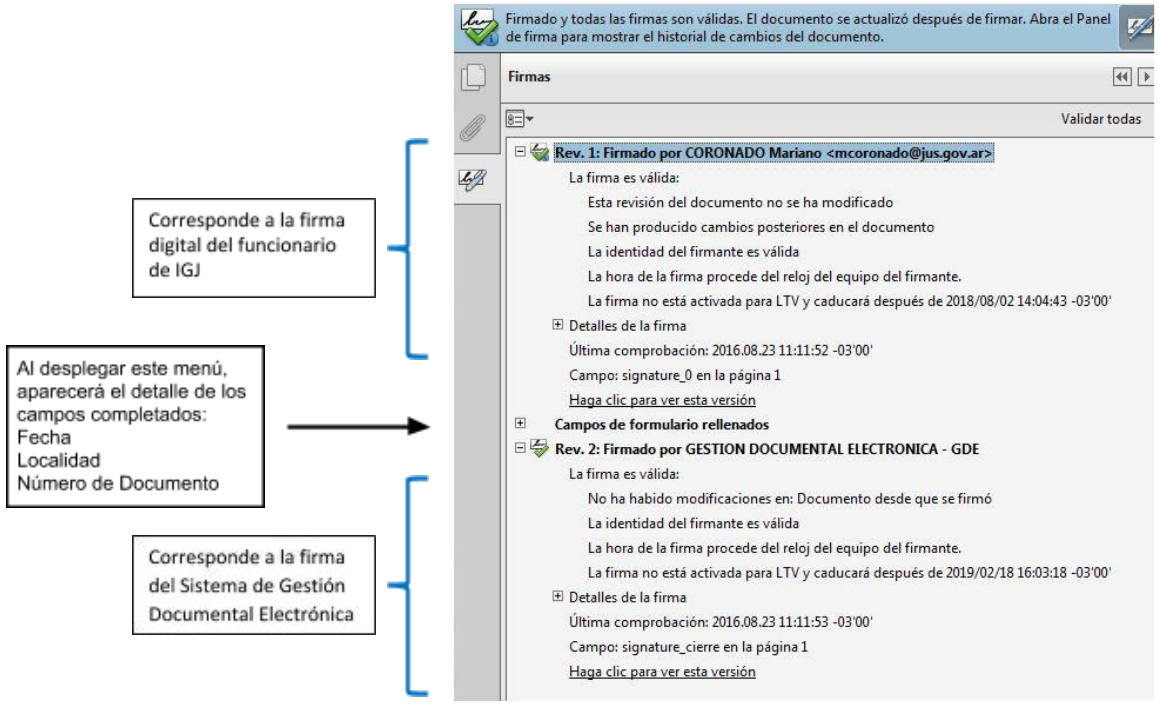


Idealmente, aparecerá el mensaje en la imagen superior. La tilde verde indica que las firmas son válidas. El mensaje “El documento se actualizó después de firmar”, aparece siempre en los documentos firmados a través de las plataformas TAD/GDE (Trámites a Distancia - Gestión Documental Electrónica). Esto sucede porque luego de la firma del agente de la APN, el sistema incorpora el número de documento, fecha y localidad, y realiza una segunda firma para “sellar” el documento.

Puede abrir el panel de firma, presionando el icono correspondiente en la barra lateral izquierda, para comprobar datos adicionales de la firma.

Panel de Firma

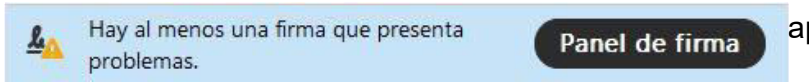
Este panel proporciona información acerca de la integridad, veracidad del documento firmado, así como información acerca del firmante, razón, fecha y hora de la firma.



Para conocer características adicionales del panel de firma, consulte el manual de adobe al respecto:
https://helpx.adobe.com/es/acrobat/using/validating-digital-signatures.html

Otros Mensajes de Firma

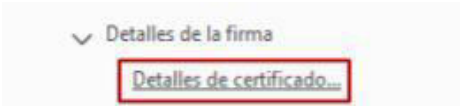
Si al abrir el documento, el panel superior de firmas no presenta la tilde verde que confirma la validez de la firma digital utilizada, hay que verificar los motivos.En caso que

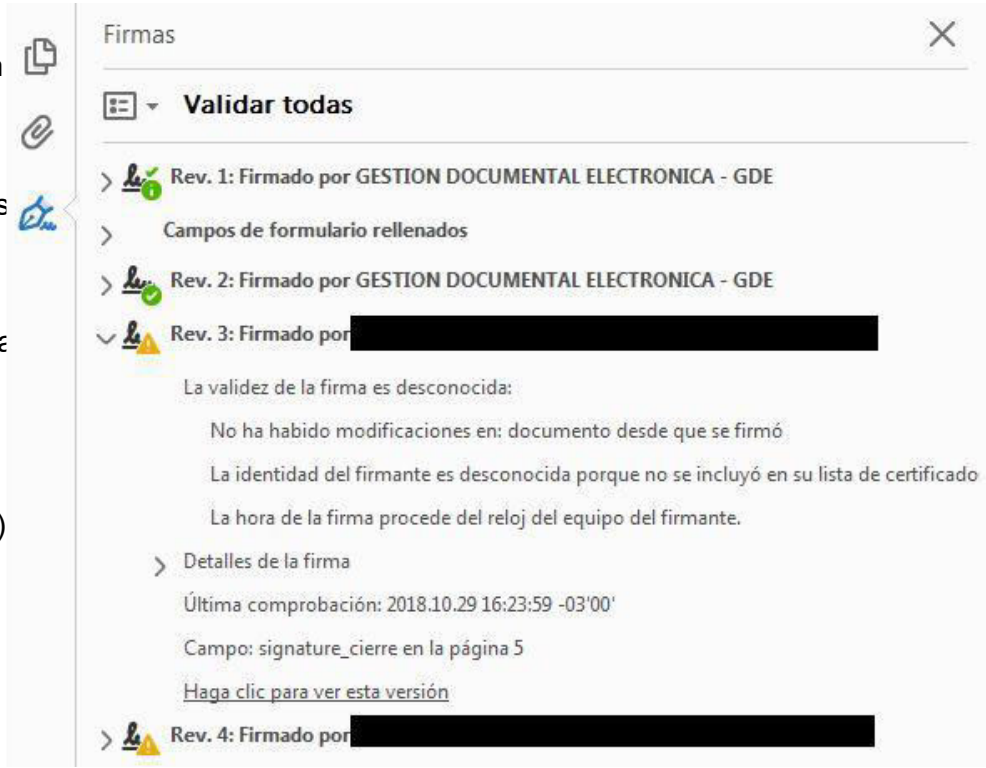


aparezca:

1. Desplegar el panel de firmas para ver los detalles de las mismas.

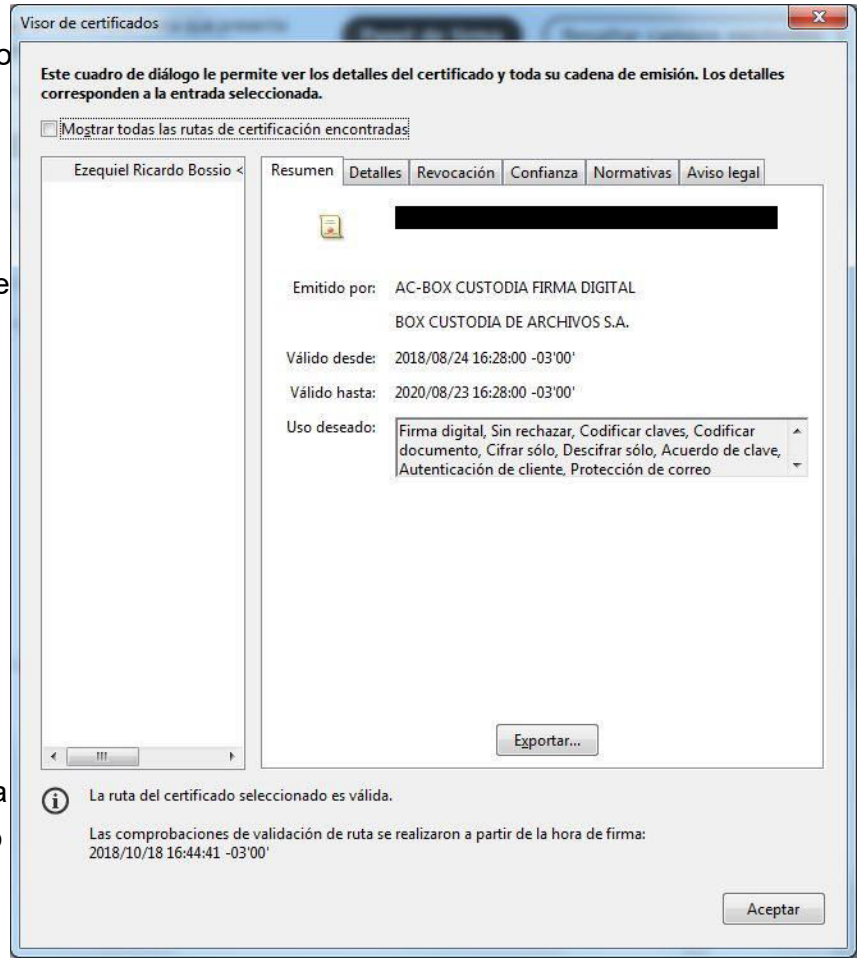
2. Allí, desplegar los datos de las firmas que presenten inconvenientes.
   Sí aparece el mensaje “La validez de la firma es desconocida” y debajo “La identidad del firmante es desconocida porque no se incluyó en su lista de certificados” esto puede deberse a:
   a. El Certificado Intermedio correspondiente a la Autoridad Certificante del firmante no fue correctamente instalado.
   b. La Autoridad Certificante no es un Certificador Licenciado. (es Firma Electrónica)
   c. El certificado fue generado por el mismo firmante. (es Firma Electrónica)





3. A fin de comprobar esto, desplegar la sección “Detalles de la firma, y allí, presionar “Detalles de Certificado”

Una ver abierto el Visor de certificados, deberá comprobar qué entidad aparece en el campo “Emitido por”, y verificar el listado completo de Certificadores Licenciados.
Si es un Certificador Licenciado (caso A), descargar el correspondiente certificado y realizar los pasos de la sección Instalación de Certificados AC.
En caso contrario, no se trata de una Firma Digital válida. Puede haber sido emitida por un certificador extranjero o local No Licenciado (caso B) o, si el emisor del certificado coincide con la identidad de la persona (tachada en la captura), de un certificado generado por el mismo firmante (caso C).



No Comprueba Revocación

En aquellos casos en que aparezca un problema con la firma, y al desplegar el panel un mensaje que indica:

La firma es válida, pero no se ha podido comprobar la revocación de la identidad de los firmantes

deberán utilizar Xolido para validar la firma. Esto sucede generalmente con certificados vencidos, ya que Adobe no valida los mismos ni su estado de revocación cuando vencieron, por lo que no es posible determinar a simple vista si el certificado era válido al momento de la firma.

Firma Inválida

Una o más firmas del documento pueden presentar este problema. Los motivos para esto pueden ser varios, entre ellos:

- El documento fue modificado (fueron añadidas o quitadas páginas, se adjuntaron documentos, se modificó el texto o apariencia del documento en cualquier forma) luego de la firma.
- El documento fue firmado como versión final, luego de lo cual no permite añadir firmas ni ninguna otra operación sin invalidar las firmas anteriores.
- Ocurrió un error durante el proceso de firmado.

Al margen del motivo, no es posible corregir o reparar el documento que presenta este problema. El mismo se considera como carente de firma, digital o electrónica.

Sin Firma

Cuando el mensaje superior de firma no aparezca y tampoco exista el botón para desplegar el panel de firma, el documento PDF no está firmado. Es posible que se esté visualizando la versión del documento previa a la firma o por otros motivos la haya eliminado. Deberá rastrearse el documento correctamente firmado.

Para mayor detalle sobre las características de la Firma Digital en PDF, puede consultar el manual de Adobe (en inglés):

https://www.adobe.com/devnet-docs/acrobatetk/tools/DigSig/Acrobat_DigitalSignatures_in_PDF.pdf

Links Útiles

- ***Ministerio de Producción - Firma Digital***
- ***Secretaría de Modernización Administrativa - Firma Digital***

  Plataforma de Firma Digital Remota (PFDR)

  - ***Preguntas Frecuentes***

    _____

  - ***Firmador***
- ***Autoridad de Aplicación (AC-RAÍZ)***

  IGJ - Firma Digital

Normativa

- Ley 25.506 - Ley de Firma Digital

  Decreto 2.628/2002 - Reglamentación de la Ley de Firma Digital
- Decreto 561/2016 - Sistema de Gestión Documental Electrónica

  Decreto 892/2017 - Autoridad Certificante MODERNIZACIÓN-PFDR (Plataforma de Firma Digital Remota)
- Resolución MM 399E/2016 - Políticas únicas de Licenciamiento y Certificación

  INFOLEG - Normativa Compilada sobre Firma Digital (apartado 1.4)

Seguridad en Informática - Prácticos

Docente: Carlos Cagnani

*Este documento fue realizado en concepto de capacitación en Formación Profesional y dictada para el **Sindicato CePETel** a contar del mes de mayo del año 2023.*

Comandos

Comandos de Windows

- Systeminfo
- ping
- tracert/traceroute
- netstat
- ipconfig/ifconfig
- Route
- Nslookup (ejemplo cambiando DNS)
- `net use && net share`

Windows Comandos

Cambio de DNS

- netsh interface ipv4 show dnsserver
- netsh interface ipv4 set dns “Ethernet" static 8.8.8.8. primary
- netsh interface ipv4 set dns “Ethernet" static 208.67.222.222. primary
- netsh interface ipv4 set dns “Ethernet" source=dhcp
- nslookup

Comandos Windows

Usuarios

- whoami /User /FO LIST && net user %username%
- net users && net localgroup

Firewall

- netsh advfirewall show allprofiles
- netsh advfirewall show currentprofile

Interface

- netsh interface show interface
- netsh interface ipv4 show addresses name=ethernet
- netsh interface set interface “Network_adapter_name” admin=enable
- netsh interface ipv4 set address "Ethernet" static 192.168.1.10 255.255.255.0 192.168.1.1
- netsh interface ipv4 set address name="Ethernet" source=static address=192.168.1.10 mask=255.255.255.0 gateway=192.168.1.1
- netsh interface ipv4 set address name="Ethernet" source=dhcp

Recycle Bin

Host Name: MSEDGEWIN10
IE Version: 11.379.17763.0

IP show

Administrator: Command Prompt

```
C:\Windows\system32>ipconfig

Windows IP Configuration


Ethernet adapter Ethernet:

   Connection-specific DNS Suffix  . : fibertel.com.ar
   Link-local IPv6 Address . . . . . : fe80::7c79:ce46:3514:bd64%7
   IPv4 Address. . . . . . . . . . . : 192.168.0.160
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.0.1

C:\Windows\system32>
```

Re-arm (Windows XP only). Note that no error is given in the case no rearms are left.

rundll32.exe syssetup,SetupOobeBnk

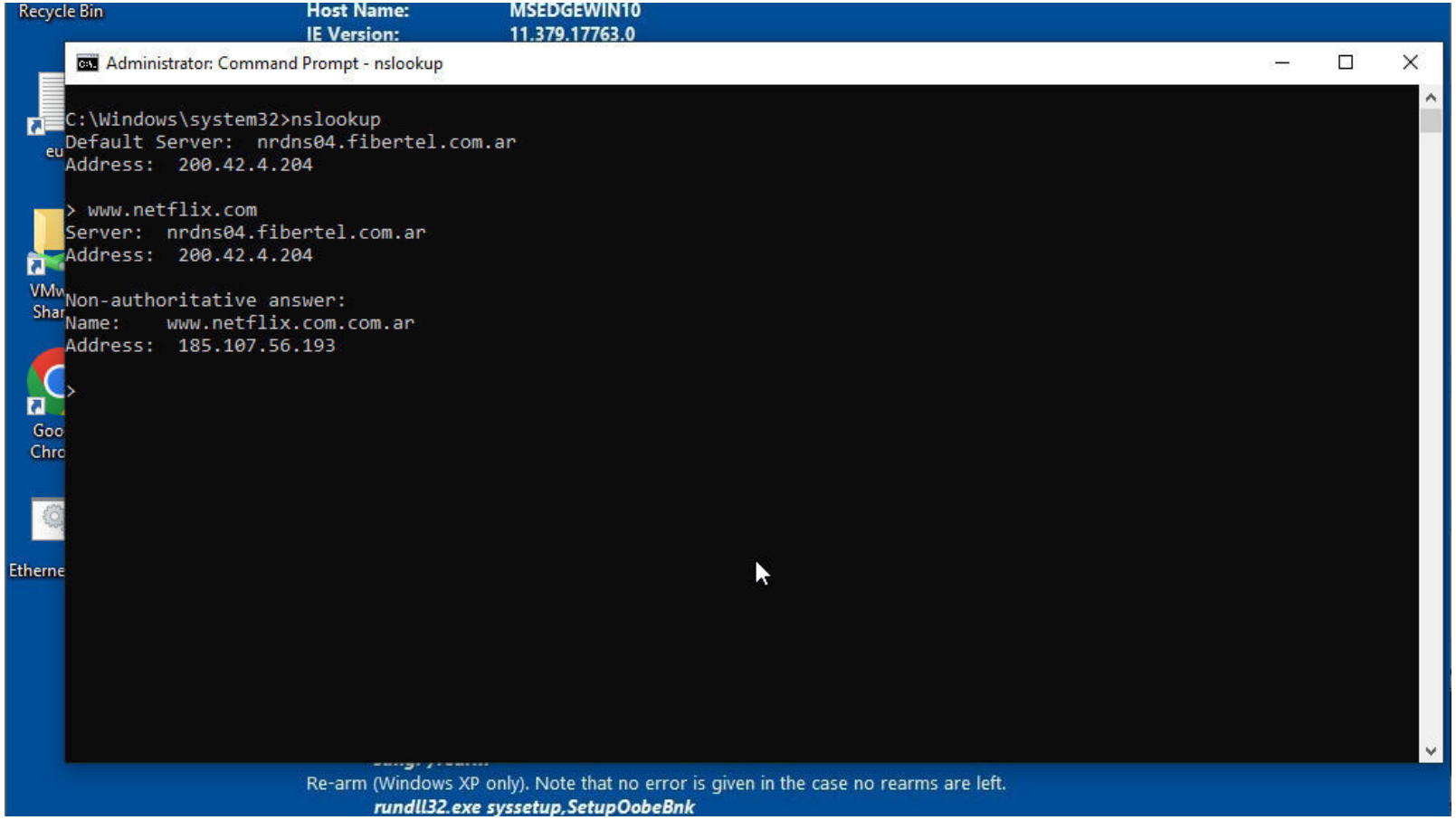
IE Version: 11.379.17763.0

DNS Show

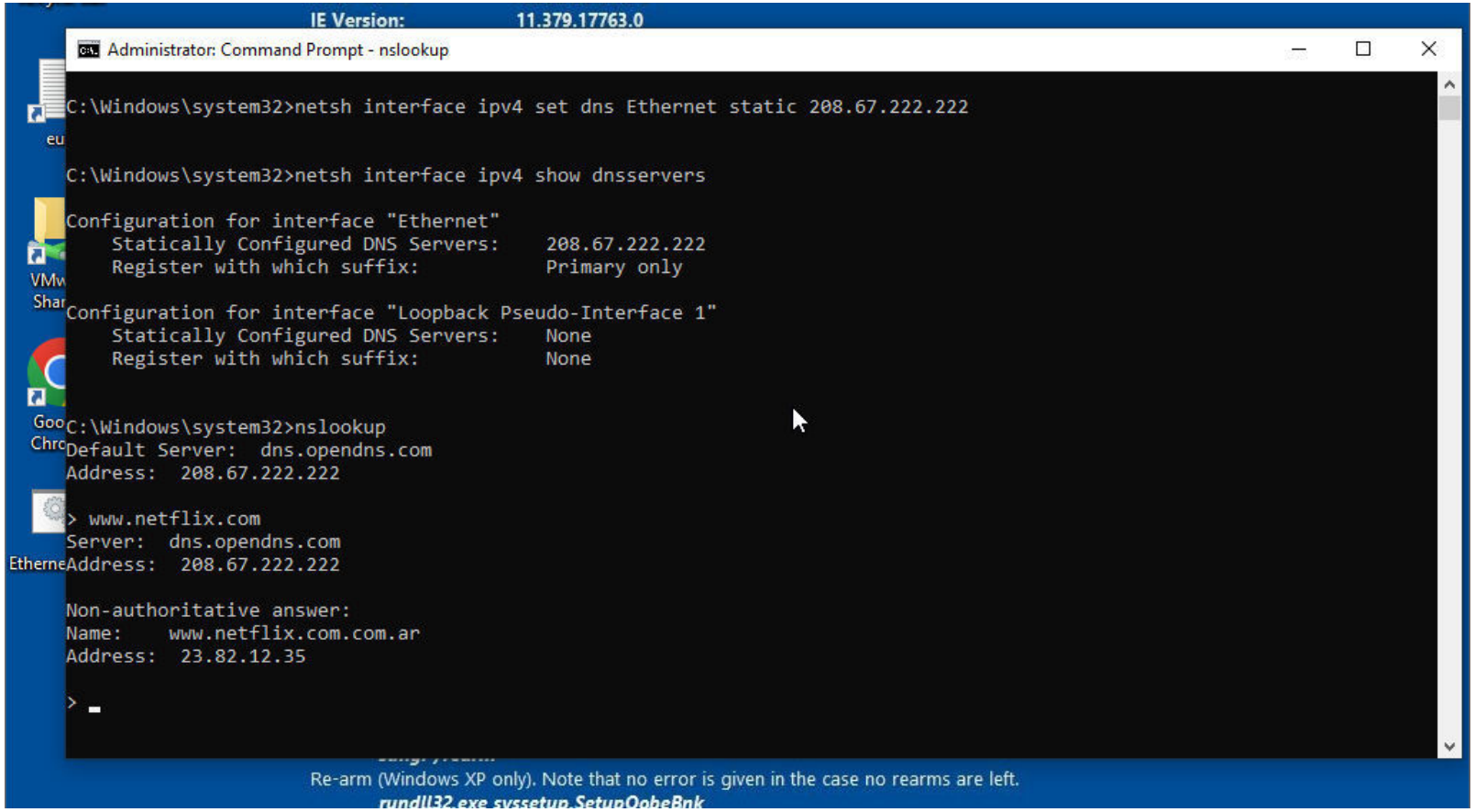
```
C:\Windows\system32>
C:\Windows\system32>
C:\Windows\system32>
C:\Windows\system32>
C:\Windows\system32>
C:\Windows\system32>
C:\Windows\system32>
C:\Windows\system32>
C:\Windows\system32>
C:\Windows\system32>
C:\Windows\system32>
C:\Windows\system32>
C:\Windows\system32>
C:\Windows\system32>
C:\Windows\system32>
C:\Windows\system32>
C:\Windows\system32>
C:\Windows\system32>netsh interface ipv4 show dnsservers

Configuration for interface "Ethernet"
    DNS servers configured through DHCP:  200.42.4.204
                                          200.49.130.51
    Register with which suffix:           Primary only

Configuration for interface "Loopback Pseudo-Interface 1"
    Statically Configured DNS Servers:    None
    Register with which suffix:           None


C:\Windows\system32>
```

Re-arm (Windows XP only). Note that no error is given in the case no rearms are left.

rundll32.exe syssetup,SetupOobeBnk



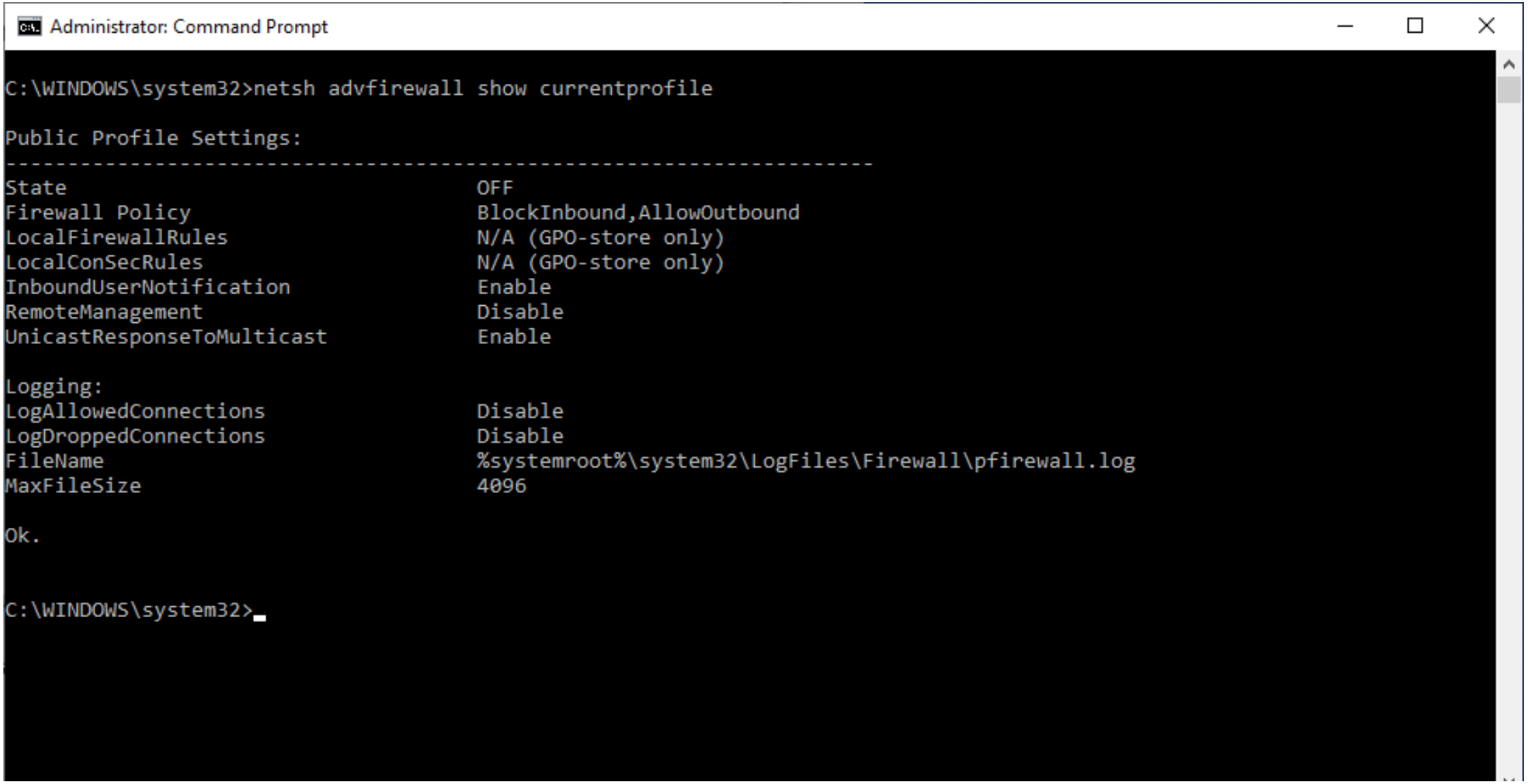
NSLOOKUP resolución default

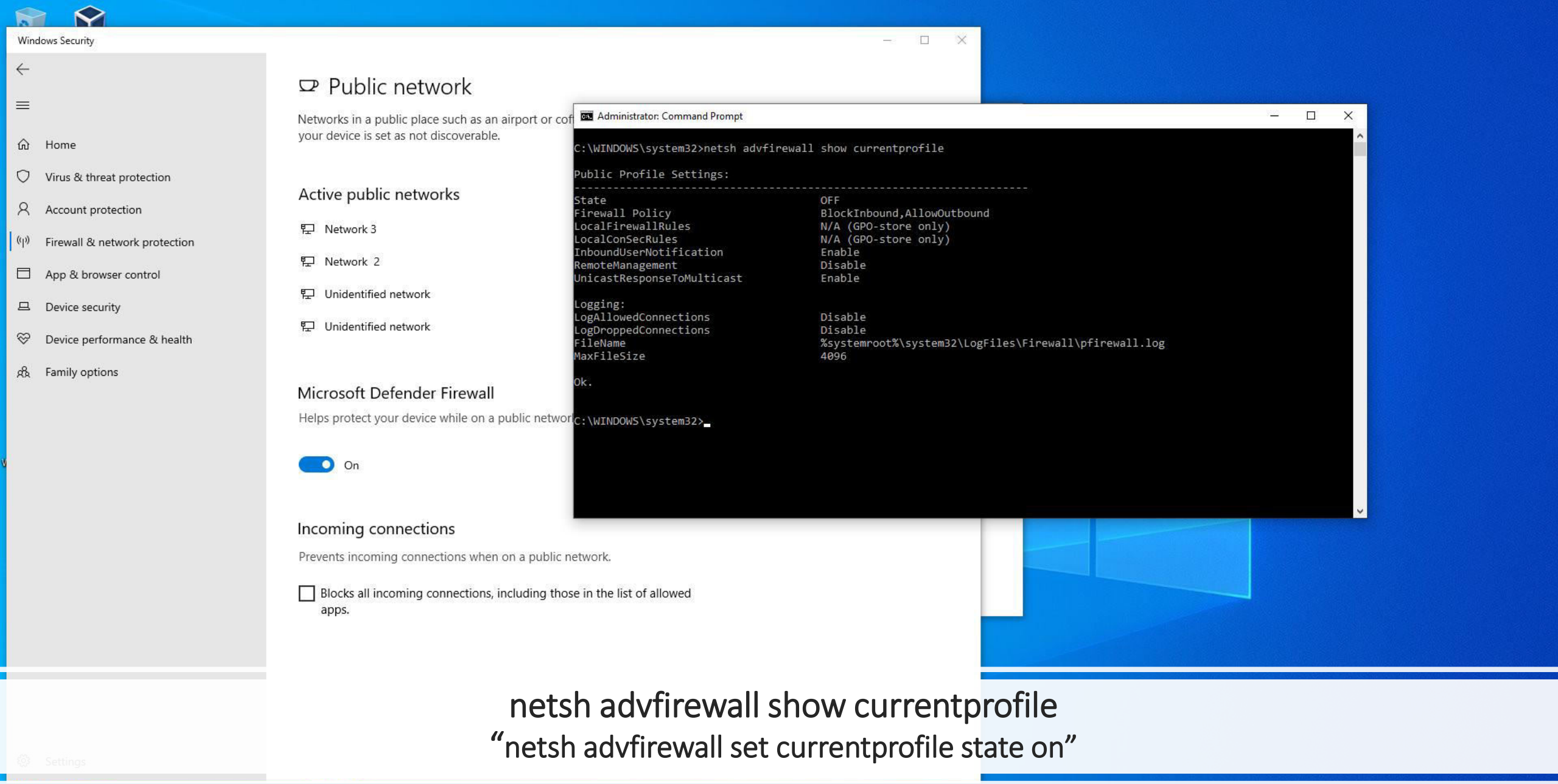


NSLOOKUP Resolución otro DNS

Firewall de Windows

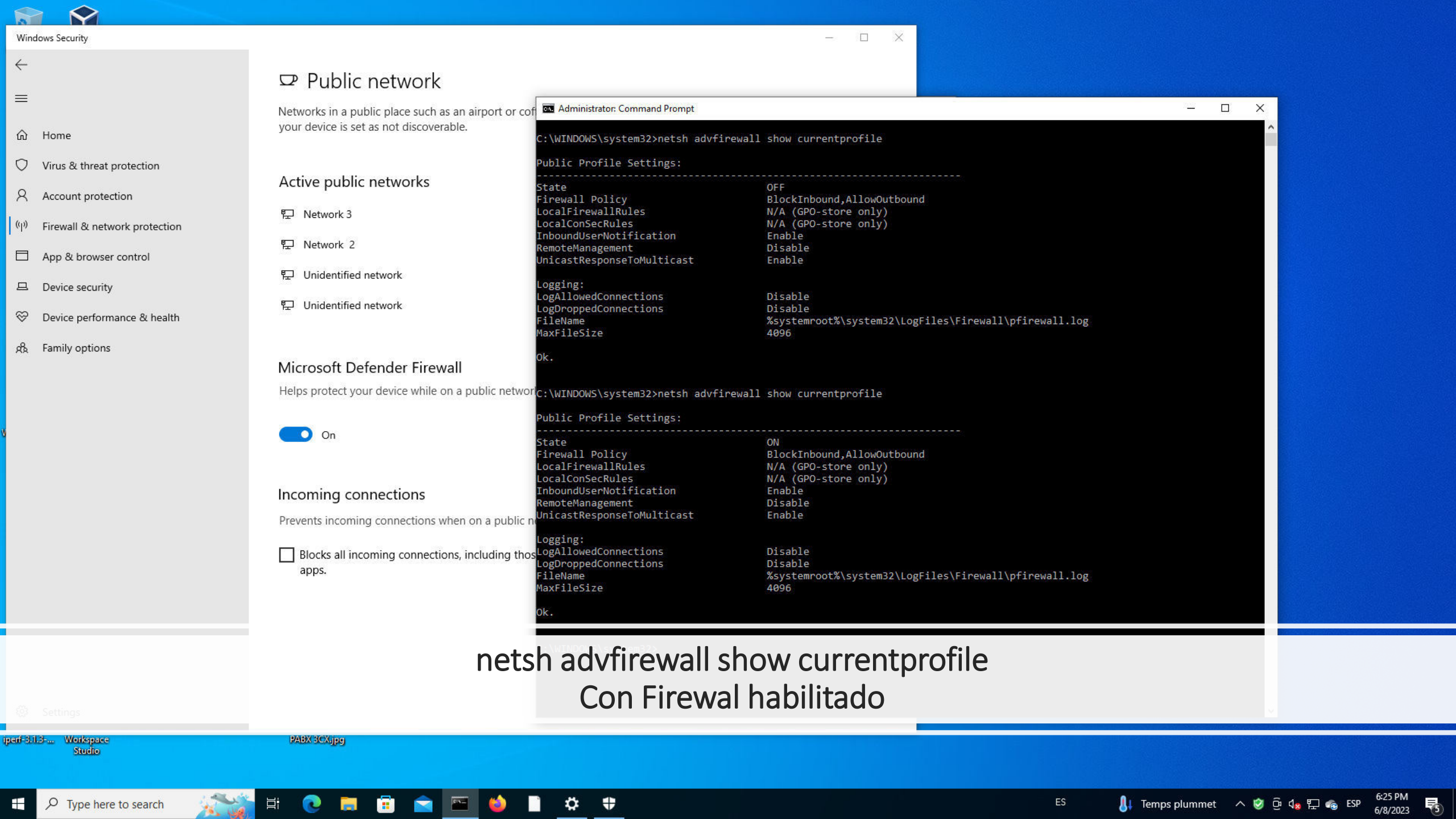
netsh advfirewall show currentprofile





netsh advfirewall show currentprofile

“netsh advfirewall set currentprofile state on”


Windows Security
Public network
Networks in a public place such as an airport or cof
your device is set as not discoverable.
Home
Virus & threat protection
Account protection
Firewall & network protection
App & browser control
Device security
Device performance & health
Family options
Active public networks
Network 3
Network 2
Unidentified network
Unidentified network
Microsoft Defender Firewall
Helps protect your device while on a public networ
On
Incoming connections
Prevents incoming connections when on a public n
Blocks all incoming connections, including thos
apps.
Settings
Administrator: Command Prompt
C:\WINDOWS\system32>netsh advfirewall show currentprofile
Public Profile Settings:
State OFF
Firewall Policy BlockInbound,AllowOutbound
LocalFirewallRules N/A (GPO-store only)
LocalConSecRules N/A (GPO-store only)
InboundUserNotification Enable
RemoteManagement Disable
UnicastResponseToMulticast Enable
Logging:
LogAllowedConnections Disable
LogDroppedConnections Disable
FileName %systemroot%\system32\LogFiles\Firewall\pfirewall.log
MaxFileSize 4096
Ok.
C:\WINDOWS\system32>netsh advfirewall show currentprofile
Public Profile Settings:
State ON
Firewall Policy BlockInbound,AllowOutbound
LocalFirewallRules N/A (GPO-store only)
LocalConSecRules N/A (GPO-store only)
InboundUserNotification Enable
RemoteManagement Disable
UnicastResponseToMulticast Enable
Logging:
LogAllowedConnections Disable
LogDroppedConnections Disable
FileName %systemroot%\system32\LogFiles\Firewall\pfirewall.log
MaxFileSize 4096
Ok.
netsh advfirewall show currentprofile
Con Firewal habilitado
iperf-3.1.3-...
Workspace Studio
PABX 3CX.jpg
Type here to search
ES
Temps plummet
ESP
6:25 PM
6/8/2023

Firewall Windows Netsh

The following examples show how to open ports, block ports, and allow programs through Windows Firewall.

Add an inbound Firewall rule to open port 80:

- netsh advfirewall firewall add rule name="allow80" dir=in protocol=tcp localport=80 action="allow"

Disable the above rule:

- netsh advfirewall firewall set rule name="allow80" new enable=no

Allow port 80 to IP Address 192.168.1.10 only:

- netsh advfirewall firewall add rule name="allow80" dir=in protocol=tcp localport=80 remoteip="192.168.1.10" action=allow

Block port 80 from IP Address 192.168.1.10:

- netsh advfirewall firewall add rule name="block80" dir=in protocol=tcp localport=80 remoteip="192.168.1.10" action=block

Firewall Windows Netsh

The following examples show how to open ports, block ports, and allow programs through Windows Firewall.

Allow a program through the Firewall:

- netsh advfirewall firewall add rule name="netcat" dir=in program="C:\program files (x86)\nmap\ncat.exe" action=allow

List all Firewall rules:

- netsh advfirewall firewall show rule all

List all inbound rules:

- netsh advfirewall firewall show rule all dir=in

Display all the settings for inbound rules called netcat:

- netsh advfirewall firewall show rule name="netcat" verbose

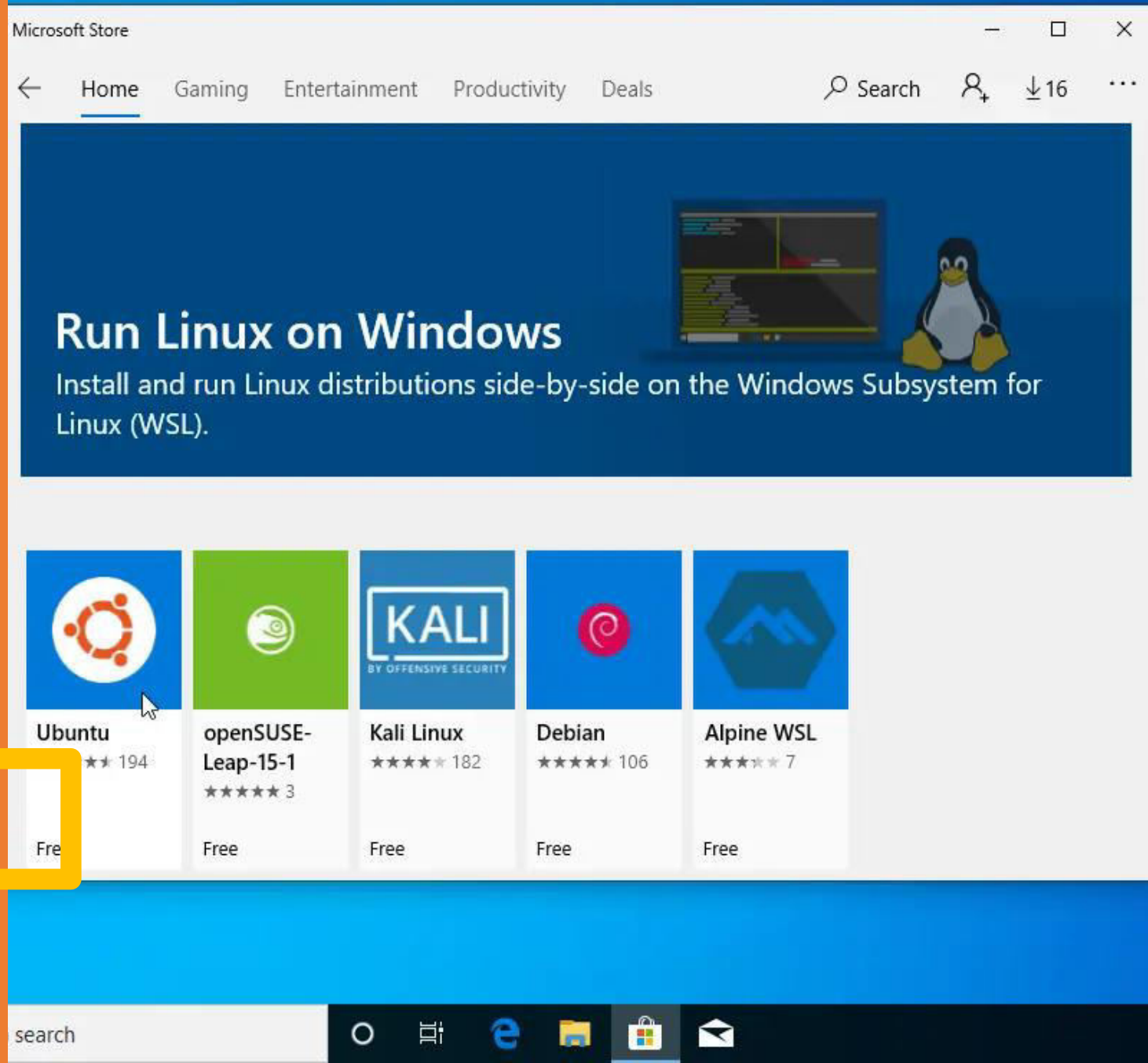
Window PowerShell

- Get-command
- Get-comman –type all
- Get-command –type cmdlet
- Get-command –type function
- Get-command *dns*
- Get-command restart*
- Get-Command –ModuleNetTCPIP
- Get-Command -ParameterName ComputerName
- Get-Command install*
- Get-Command –nown *service

Linux Distribuciones o versiones

- 1 Ubuntu
- 2 Debian
- 3 CentOS Linux
- 4 CentOS Stream
- 5 Red Hat Enterprise Linux (RHEL)
- 6 Gentoo
- 7 Fedora
- 8 OpenSUSE
- 9 Scientific Linux
- 10 CloudLinux

Ubuntu en Windows



Ubuntu en Windows

- Ubuntu en Windows es una aplicación de Windows 10 que se ejecuta en el Subsistema de Windows para Linux (WSL), que es una capa de compatibilidad de aplicaciones para ejecutar sistemas operativos Linux de forma nativa en Microsoft Windows.

Ubuntu en Windows

La instalación de Ubuntu en Windows 10 implica un proceso de dos pasos:

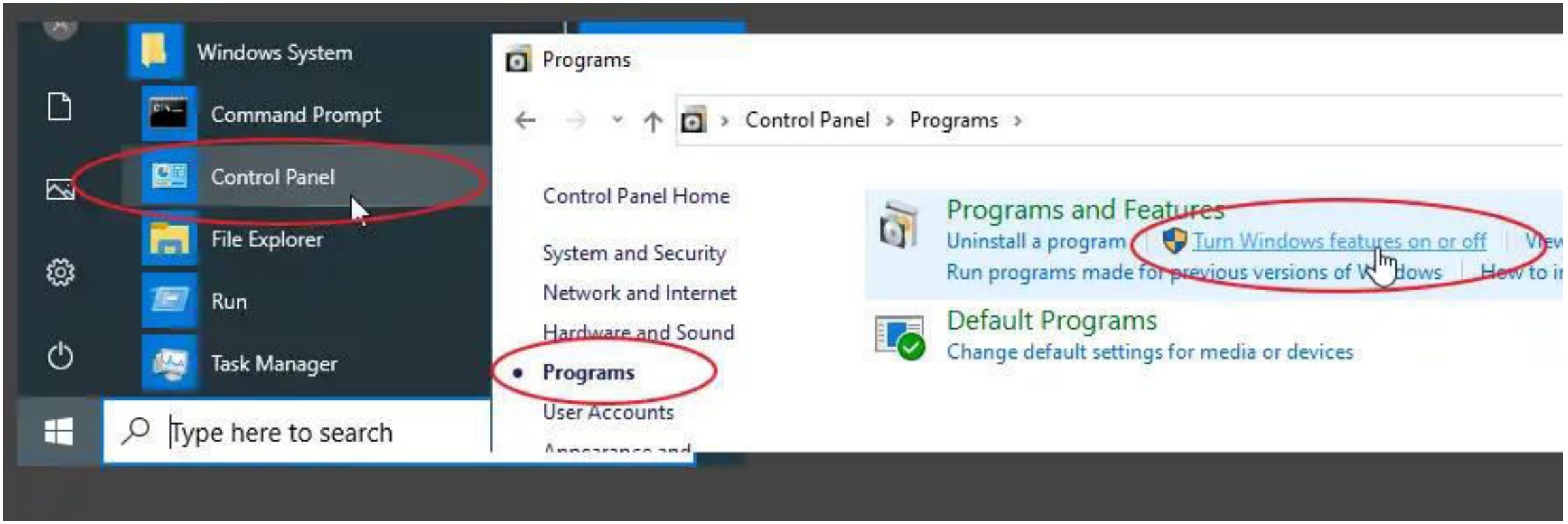
- Primero habilitamos la función Subsistema de Windows para Linux desde el panel de control.
- Luego instalamos la aplicación de Ubuntu desde la tienda de Microsoft.

Ubuntu en Windows

Habilitar el Subsistema de Windows para Linux

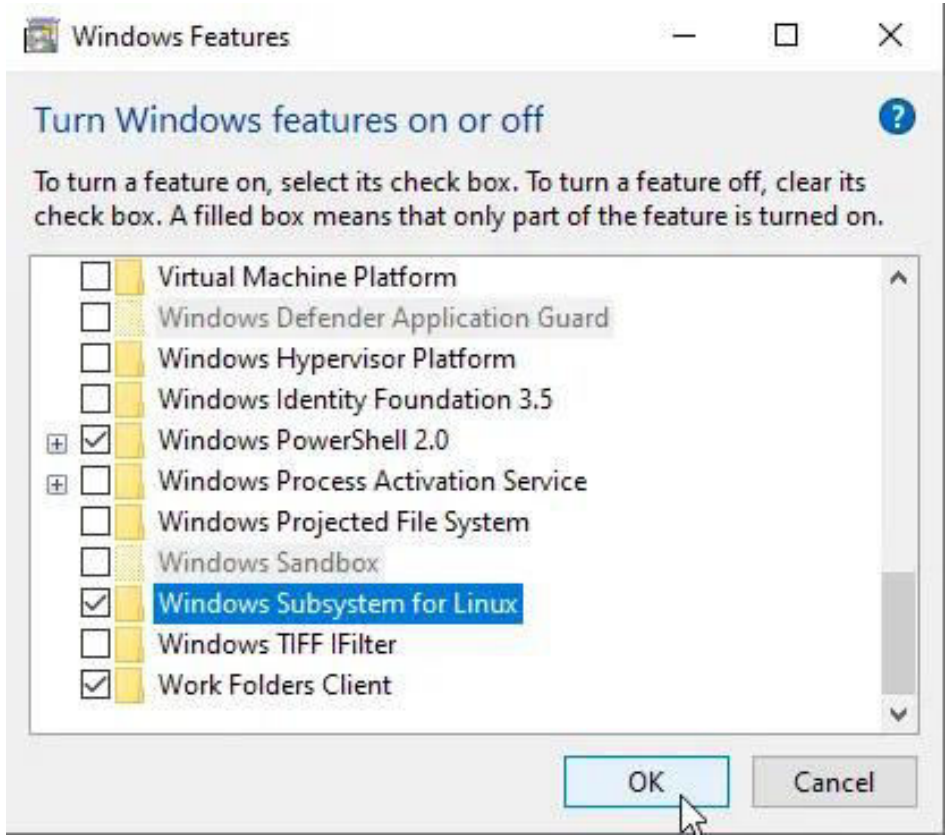
Primero debemos habilitar la función de WSL.

Abre el panel de control (botón de inicio > Sistema de Windows), ve a la categoría de Programas y selecciona "Activar o desactivar las características de Windows".



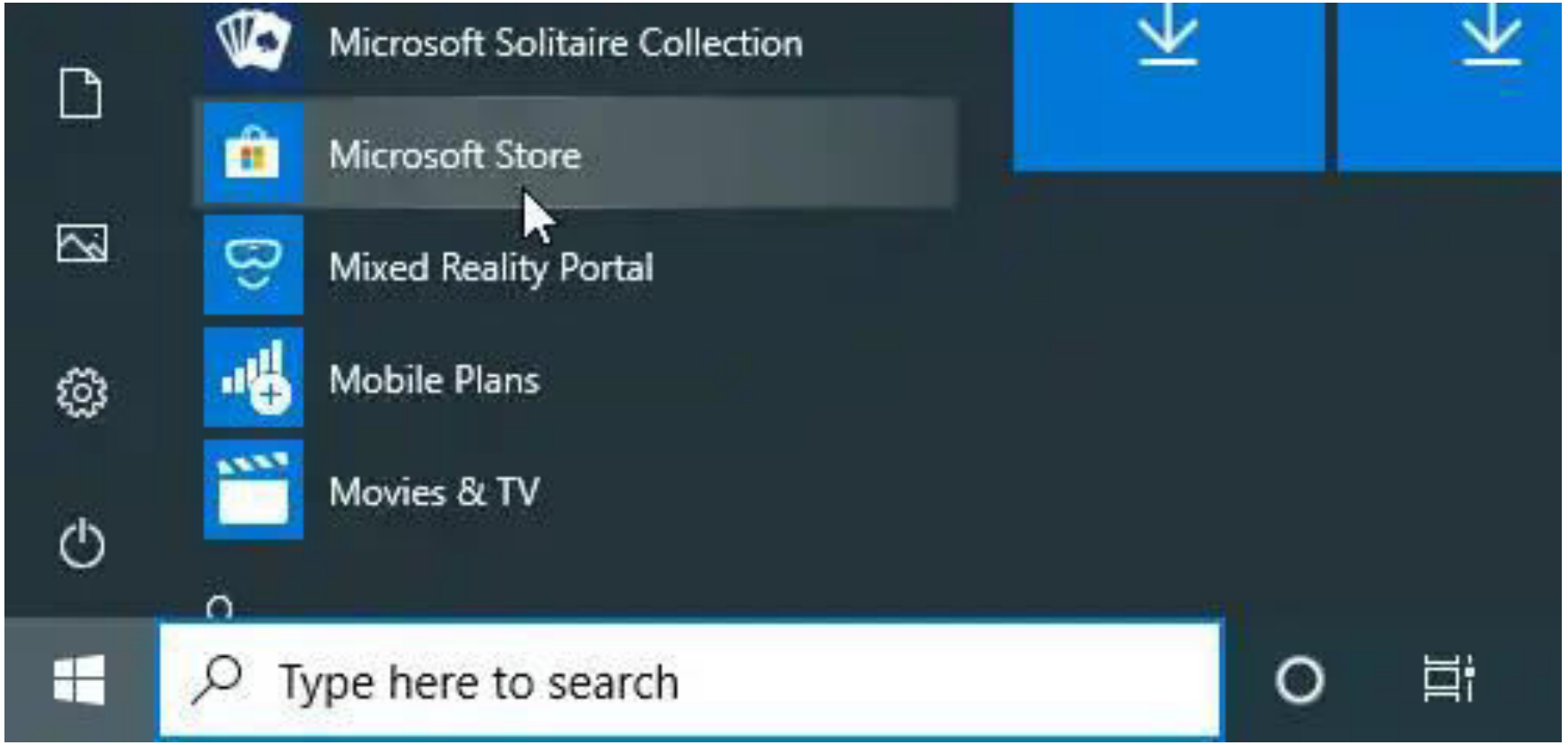
Ubuntu en Windows

- Encuentra la función llamada Subsistema de Windows para Linux, luego activa la casilla de verificación y haz clic en el botón "Aceptar" (o "OK").
- Esto instalará la función WSL y te pedirá que reinicies tu PC al finalizar el proceso. Debes reiniciar tu computadora antes de utilizar esta función.



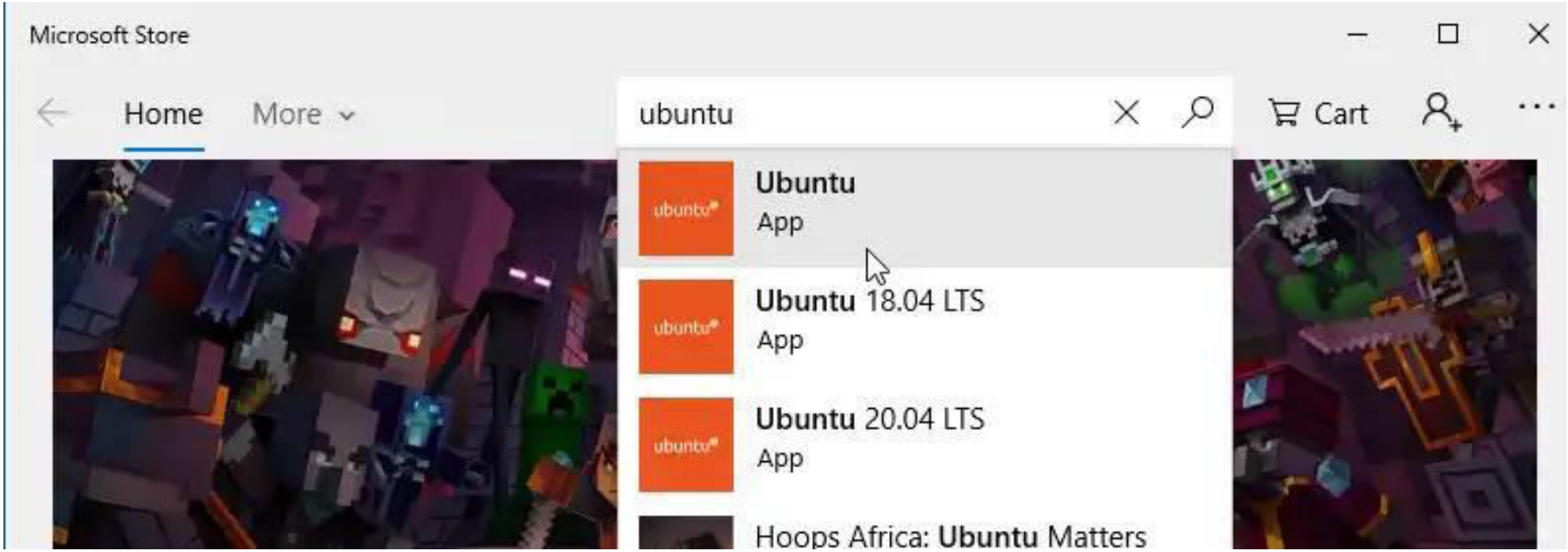
Ubuntu en Windows

- Instalar el sistema operativo Ubuntu Una vez que estés de vuelta en Windows, abre la tienda de Microsoft desde el menú de inicio y busca Ubuntu.



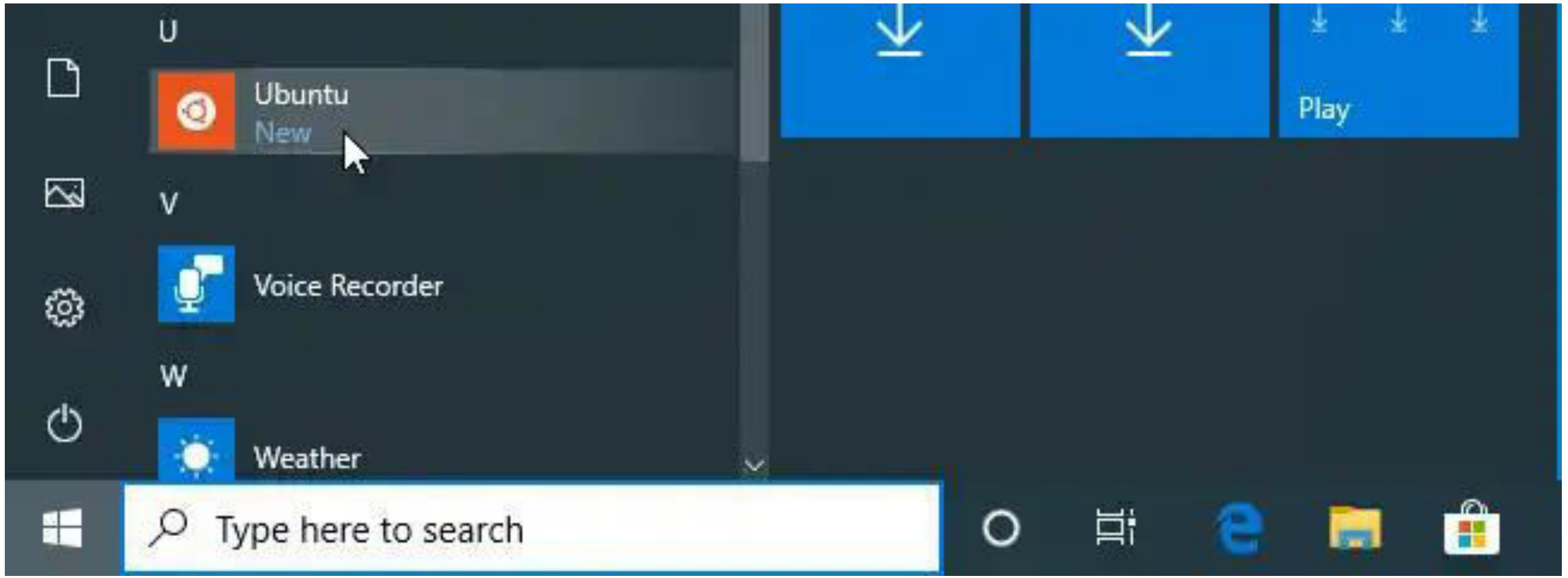
Ubuntu en Windows

- Selecciona el resultado superior, como se muestra en la siguiente captura de pantalla, e instala la aplicación una vez que se cargue la página de detalles..



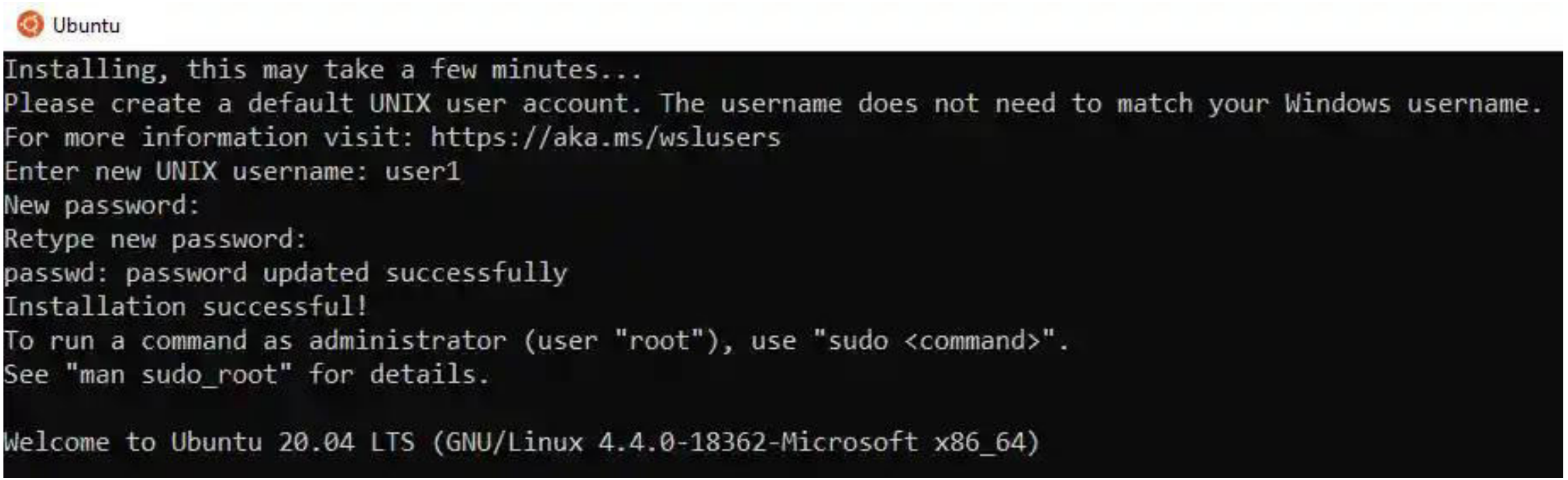
Ubuntu en Windows

- Después de eso, se creará un acceso directo en el menú de inicio para abrir la nueva aplicación de Ubuntu.



Ubuntu en Windows

- La primera vez que inicies Ubuntu, se te solicitará que crees un nombre de usuario y una contraseña.



Ubuntu
Comandos

Comandos de red

- Ip: direccionamiento
- Ip link: direcciones físicas y estado de las interfaces
- Ip address: direcciones logicas
- Ip route show: tabla de rutas
- ip route add default via 10.102.66.1 : ruta estática
- ip addr add 10.102.66.200/24 dev *enp0s25 :configura IP*
- ip link set dev *enp0s25* up
- ip link set dev *enp0s25* down
- ip address show dev enp0s25
- netstat –rn: tabla de rutas
- lshw –class Network

https://ubuntu.com/server/docs/network-configuration

Ubuntu
Comandos

Comandos generales

- Ip: direccionamiento
- man <*comando*>: ayuda de comandos
- ls –asl: archivos
- Mkdir: make dir
- Cd: Change dir
- Rmdir: Remove Dir
- Cp: Copy
- Mv: move
- Touch: crea un archivo

Ubuntu
Comandos

Comandos generales cont.

- df –k: unidad de discos
- ps –ef: procesos
- top :procesos
- Lsb_release –a : versión
- Find:
- Poweroff:
- Cat:

Ubuntu Firewall

- Ufw enable
- Sudo ufw allow 22/tcp
- Sudo ufw enable
- Sudo ufw disable
- Sudo ufw status

Equivalencia de comandos

Equivalencias de comandos para Windows, OSX y Linux

Las palabras en Itálica son las opciones que debes proporcionar.

Linux	OSX	Windows
command --help	command --help	*command* /h, *command* /?
man *command*	man *command*	help *command*
cp	cp	copy
rm	rm	del
mv	mv	move
mv	mv	ren
more, less, cat	more, less, cat	type
lpr	lpr	print
rm -R	rm -R	deltree
ls	ls	dir
cd	cd	cd
mkdir	mkdir	md
rmdir	rmdir	rd
netstat -r	netstat -r	route print
traceroute	traceroute	tracert
ping	ping	ping
ifconfig	ifconfig	ipconfig

KALI LINUX

- Vulnerando passwords

Kali Linux (hashcat)

- Hashcat
- Man hashcat
- /attack mode
- Generación archivo
- echo -n "bob" | md5sum | cut -d' ' -f1>> hashes.txt
- echo –n “juan” | md5sum | cat –d ' ' –f1 >> hashes.txt
- echo –n “pablo” | md5sum | cat –d ' ' –f1 >> hashes.txt
- echo –n “abc123” | md5sum | cat –d ' ' –f1 >> hashes txt
- echo –n “password” | md5sum | cat –d ' ' –f1 >> hashes.txt
- echo –n “password123” | md5sum | cat –d ' ' –f1 >> hashes.txt

- Usando diccionario
- hashcat -a0 -m0 test1.txt Downloads/ignis-1M.txt

- rm ./.local/share/hashcat/hashcat.potfile !para poder ejecutar de nuevo

- Fuerza bruta
- hashcat -a3 -m0 test1.txt

Passwords

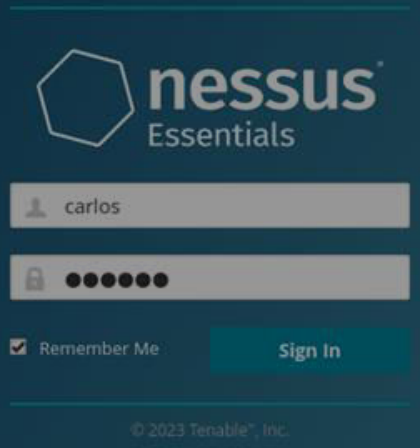
- https://Weakpass.com
- Password Strength Test - WhatIsMyIP.com®
- Password Strength Testing Tool | Bitwarden
- Strong Random Password Generator (passwordsgenerator.net)

KALI LINUX

- nessus

Nessus

- (root㉿kali)-[~]└─# /bin/systemctl start nessusd.service
  Para levantar el servicio
- https://kali:8834/ : Para acceder



Nessus

- Pantalla principal