

Por José Manuel Aroca Fernández

CIBERSEGURIDAD INFORMÁTICA Y FIRMA DIGITAL

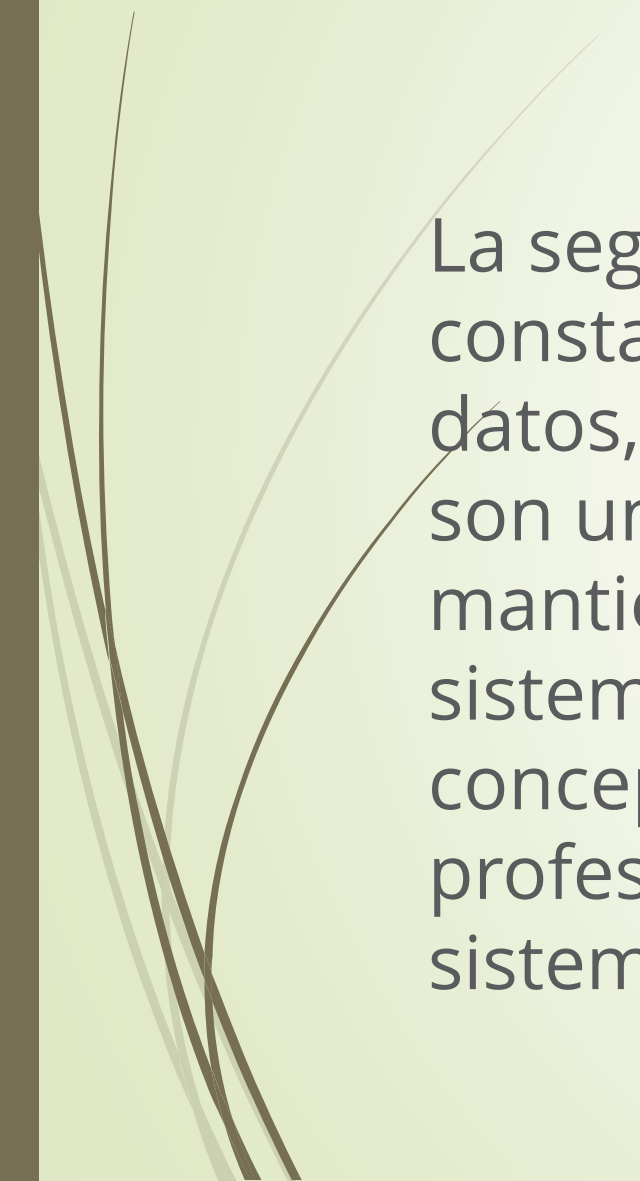


Indice

- Introducción
- Sistemas de seguridad en la empresa
 - Estándares de seguridad
 - Test módulo 1
 - Ciberseguridad: tipos de ataques y en qué consisten
 - Ciberseguridad: medidas de protección a nivel individual
 - Practicas módulo 1
 - Ciberseguridad: medidas de protección a nivel de empresa.
 - Ciberseguridad: Los 7 errores al implementar un sistema de gestión de seguridad de la información.
- Fundamentos de criptografía.
 - Introducción a la criptografía
 - Objetivos de la criptografía
 - Un poco de historia
 - Tipos de ataques criptográficos
 - Tipos de funciones criptográficas: SISTEMAS DE CIFRADO CLÁSICOS
 - Tipos de funciones criptográficas: SISTEMAS DE MODERNOS



Introducción



La seguridad informática es una preocupación constante de todas las organizaciones. Robo de datos, hackeos, malware y muchas otras amenazas son una de las tantas preocupaciones que mantienen sin dormir a los administradores de sistemas y profesionales de TI. Hablaremos de los conceptos básicos y mejores prácticas que muchos profesionales de TI usan para mantener sus sistemas protegidos.

Introducción

En el área de CIBERSEGURIDAD existen infinidad de términos, acrónimos y conceptos que el Instituto Nacional de Ciberseguridad ha incluido en un glosario que nos será de gran utilidad a lo largo de este curso.

[Glosario de términos de ciberseguridad.](#)



Introducción

- **¿Cuál es la meta de la seguridad informática?**
- La seguridad informática sigue 3 conceptos fundamentales:
 - **Confidencialidad:** La información solo debe de ser vista o utilizada por las personas autorizadas para tener acceso a ella.
 - **Integridad:** Prevenir e identificar cualquier cambio a la información por un usuario no autorizado y los usuarios que lo lleguen a realizar deben de ser rastreados.
 - **Disponibilidad:** La información debe estar disponible cuando los usuarios autorizados la necesiten.

En base a estos conceptos fundamentales, los especialistas en seguridad informática han creado mejores prácticas para ayudar a las organizaciones a proteger y salvaguardar la información.

Introducción

➤ Mejores prácticas de Seguridad Informática:

- 1. Balancear protección con utilidad.** Las computadoras en una oficina estarían completamente protegidas si no tuvieran acceso a internet y adicionalmente, estuvieran una habitación sin personas. Pero esto llevaría a que no podrían ser utilizadas por nadie. Este es uno de los más grandes retos en la seguridad informática, encontrar el balance entre disponibilidad de recursos y la confidencialidad e integridad de los mismos.
- 2. Dividir los usuarios y los recursos.** Para que la seguridad informática funcione, debe de conocerse quien está autorizado para ver y hacer cosas en particular. Alguien en contabilidad, por ejemplo, no necesita poder ver todos los nombres de los clientes en la base de datos de clientes, pero si ver todos los datos de ventas. Esto implica que el administrador de sistemas necesita asignar accesos a la información basado en el tipo de actividad del usuario y requiere de refinar estos límites basado en su posición dentro del organigrama. Esto asegura que, por ejemplo, El CFO o director de finanzas pueda ver todos los datos de un sistema y un contador junior solo ciertas partes de los mismos.

Introducción

➤ Mejores prácticas de Seguridad Informática:

3. **Asignar privilegios mínimos.** Un usuario deberá siempre recibir los mínimos privilegios para poder realizar de forma eficiente sus actividades diarias, si las responsabilidades de dichos usuarios cambian, los privilegios deben hacerlo también. Asignar los mínimos privilegios asegura reducir las probabilidades de que Juanito de ventas, saldrá por la puerta el día que sea despedido, con todo el catálogo de clientes en una USB.
4. **Utilizar defensas independientes.** Este es un principio militar, no tanto un principio de seguridad informática. Utilizar una defensa realmente efectiva, como protocolos de autenticación para lograr acceso a un sistema, es bueno hasta que alguien logra penetrarlo. Cuando se utilizan diferentes métodos independientes de defensa, un atacante deberá de utilizar diferentes estrategias y tácticos para poder atravesar. Utilizar este tipo de complejidad no provee el 100% de efectividad contra ataques, pero si reduce grandemente las probabilidades de un ataque exitoso.

Introducción

➤ Mejores prácticas de Seguridad Informática:

5. **Planear las contingencias.** Esto te ayudará a mitigar las consecuencias ante un ataque o una penetración de tu esquema de seguridad. Tener respaldos en anticipado, software de monitoreo y políticas de reacción inmediata ante una eventualidad, permite al departamento de TI y sus administradores reaccionar rápidamente ante una emergencia.
6. **Registrar, Registrar y Registrar.** En un estado ideal, la seguridad informática nunca será penetrada por extraños, pero si esto llega a suceder, el evento debe de ser registrado. De hecho, la mayoría de los administradores de TI, llevan tantos registros como sea posible, incluso si no ha sucedido un ataque. Algunas veces las causas de un ataque no son evidentes hasta mucho después del incidente, por eso es importante poder rastrear hacia atrás y hacia adelante en los eventos y cómo sucedieron en el tiempo. Los datos de ataques eventualmente te ayudaran a mejorar la calidad de la seguridad de los sistemas y mejorar la prevención en el futuro. Incluso si inicialmente esas medidas no hacen mucho sentido.

Introducción

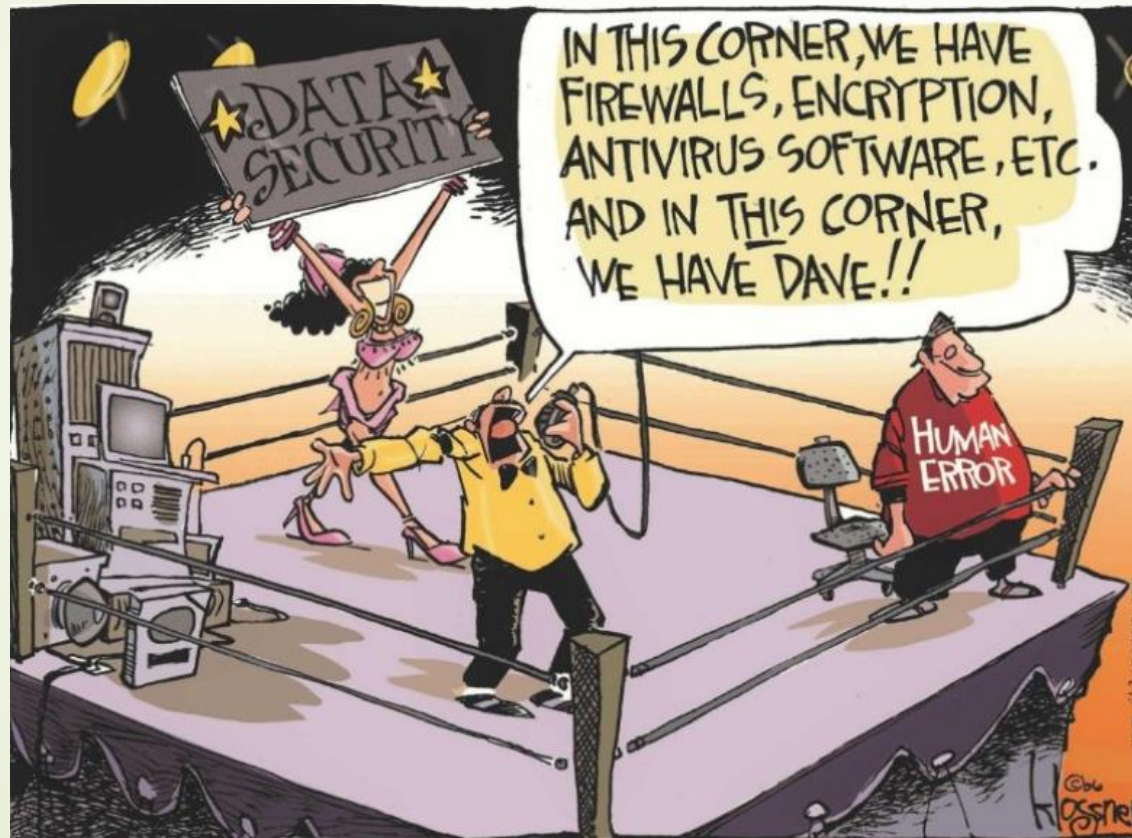
➤ Mejores prácticas de Seguridad Informática:

7. Realiza pruebas frecuentemente. Los hackers están constantemente puliendo y mejorando su armamento con técnicas cada vez más complejas, lo que significa que la seguridad informática debe evolucionar para mantener el ritmo. Los administradores de TI deben ejecutar pruebas, análisis de vulnerabilidades, actualizar el plan de recuperación de desastres, verificar que todos los elementos del plan de continuidad de negocio en caso de ataques están al día, etc.

La seguridad informática es un trabajo muy retador que requiere atención en todos los detalles al mismo tiempo y un alto nivel de conciencia de riesgo. Muchas de las tareas lucen complejas a primera vista, sin embargo, la seguridad informática se puede fragmentar en pasos básicos y así lograr simplificar los procesos para de esta manera, tratar de hacer más simple su diseño y ejecución y lograr que los administradores de TI tengan siempre un nivel de protección adecuado para soportar la misión crítica de la organización.

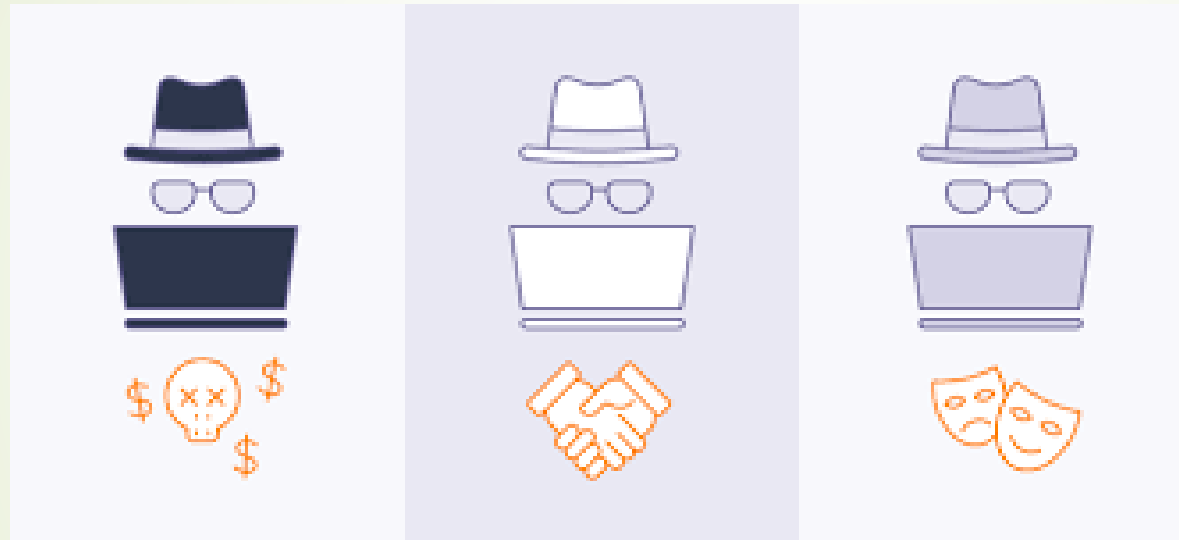
Introducción

Algunos ejemplos de brechas de seguridad y sus consecuencias



Introducción

Tipologías de hacker: White/Gray/Black Hat Hacker



Hay diferentes tipos de hacker en función de si su propósito es aprovechar sus conocimientos con fines benignos o malignos. Si buscáis en internet artículos sobre los tipos de hackers que hay, os podéis encontrar que enumeran desde 2 hasta 10 diferentes, aunque ciertamente hay 3 tipos que son los que más coinciden en nombrar todos y son los que os comentaré en este post: *White Hat Hacker*, *Black Hat Hacker* y *Grey Hat Hacker* (Hacker de sombrero blanco, Hacker de sombrero negro y Hacker de sombrero gris).

Introducción

➤ *White hat hackers* (Hackers de sombrero blanco)

También se les conoce como **hackers éticos**. Son aquellos hackers que utilizan sus conocimientos para encontrar vulnerabilidades en un sistema informático, y lo ponen en conocimiento de las compañías desarrolladoras o empresas, con el objetivo de poder estudiar y corregir los fallos. Buscan mejorar los sistemas en materia de seguridad, ya sea a través de la seguridad en aplicaciones, sistemas operativos y protección de datos sensibles, para poder garantizar la confidencialidad de la información de los usuarios.

En esta tipología de hackers podemos encontrar tanto los investigadores de seguridad, como los que hackean sistemas por razones no maliciosas para demostrar a un cliente o una empresa para la que trabajan que el sistema informático no es seguro. Existen certificaciones, cursos, y capacitaciones online que cubren toda la esfera del hacker ético, algunas de ellas acreditadas por la misma Agencia Nacional de Seguridad de los Estados Unidos (NSA).

Introducción

➤ *Black hat* hackers (Hackers de sombrero negro)

Conocidos también como **crackers**, son realmente los hackers criminales causantes de todos los ciberataques que no paran de aparecer en prensa. Es un hacker que utiliza todo su conocimiento para introducirse en los sistemas como los hackers blancos pero de una manera maliciosa, buscando su beneficio personal/económico. Son los responsables de todo el spam que recibimos en el correo, los que hacen los virus malware, los que se cuelan en los sistemas de las grandes empresas para modificar o destruir datos, robar información de los usuarios para luego venderlo al mejor postor, colapsar el sistema, y un largo etcétera.

Introducción

➤ *Gray hat hackers* (Hackers de sombrero gris)

Entre los hackers blancos y los negros nos encontramos con los grises (parece broma pero no lo es). Se denominan así a los hackers que rompen los niveles de seguridad de los sistemas de una empresa para, posteriormente, ofrecer sus servicios para mejorar dicha seguridad. Es decir, atacan al sistema informático de una empresa para demostrar su valúa, y ser contratado para defenderla arreglando sus fallos de seguridad.

Aquí podríamos estar hablando de individuos anónimos contratados expresamente, o hackers grises que van por libre y después de hackear un sistema o empresa, le ofrecen sus servicios. Un ejemplo serían los hackers contratados por algunos gobiernos para espiar a otros países.

Introducción

Algunos ejemplos de brechas de seguridad y sus consecuencias

1. -El Ransomware (“Ramonware” en castizo)
2. “Ejque me se ha ido el dedo al enviar el imeil”
3. Tengo una secre que es “oro en barras”
4. Me guindaron el portátil en la T4. O lo perdí.
5. Este verano sí que he desconectado. Del todo

I certainly do. In fact I often forget my password and have to ask my staff what it is.

— Nick Boles MP (@NickBoles) 3 de diciembre de 2017

Consejo: Utiliza un gestor de contraseñas.

Introducción

Revisemos un informe de ciberseguridad

CADA DÍA, EL MUNDO SE ENFRENTA A MÁS DE **100.000** SITIOS WEB MALICIOSOS Y **10.000** ARCHIVOS MALICIOSOS, TODOS ELLOS CON EL OBJETIVO DE ROBAR, CAUSAR DAÑOS Y PERJUICIOS

EL 87% DE LAS ORGANIZACIONES HAN EXPERIMENTADO EL INTENTO DE UN EXPLOIT A UNA VULNERABILIDAD EXISTENTE

EL 46% DE LAS ORGANIZACIONES HAN TENIDO AL MENOS UN EMPLEADO QUE HA DESCARGADO UNA APLICACIÓN MÓVIL MALICIOSA QUE AMENAZA SUS REDES Y DATOS

ESTUDIOS MUESTRAN QUE EN EL TERCER TRIMESTRE DE 2020, CASI LA MITAD DE TODOS LOS CASOS DE RANSOMWARE INCLUÍAN LA AMENAZA DE LIBERAR DATOS ROBADOS, Y EL PAGO MEDIO DEL RESCATE FUE DE **233.817 DÓLARES, UN 30% MÁS QUE EN EL SEGUNDO TRIMESTRE DE 2020.**

CIBERATAQUES MENSUALES POR ORGANIZACIÓN SANITARIA ENERO 2020 - ENERO 2021

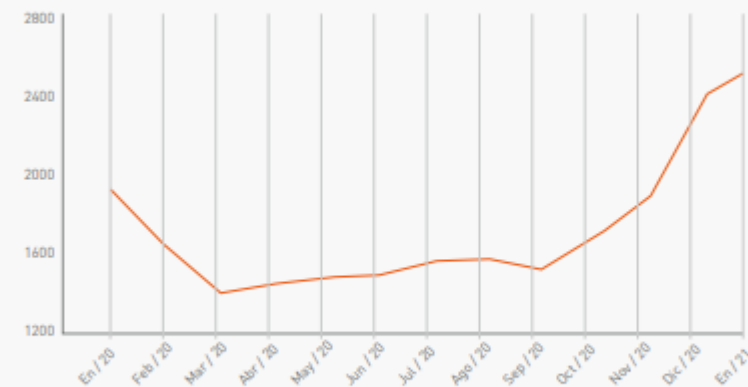


Figura 1: Marzo 2020 Los grupos de ransomware se comprometieron a no atacar a las instituciones sanitarias. En realidad, los ataques a la sanidad aumentaron considerablemente hacia finales de año.

Introducción

Revisemos un informe de ciberseguridad

AUMENTO DE LOS ATAQUES QUE EXPLOTAN LAS VULNERABILIDADES DE LOS PRODUCTOS DE CONEXIÓN REMOTA EN 2019-2020

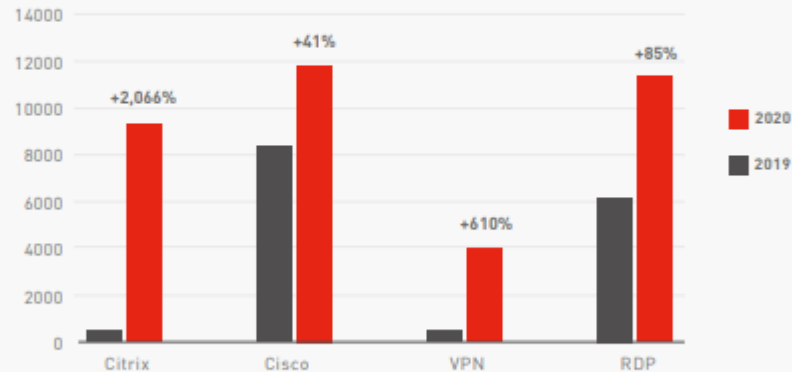


Figura 2: Grupos APT integran vulnerabilidades de acceso remoto nuevas y antiguas para obtener un punto de apoyo inicial.

INFORME DE CIBERSEGURIDAD 2021

cp<r>
CHECK POINT RESEARCH

EN 2020, EL TIEMPO PROMEDIO QUE SE TARDÓ EN IDENTIFICAR Y CONTENER UNA CIBERINFRACCIÓN FUE DE 280 DÍAS, Y EL COSTO PROMEDIO DE UNA INFRACCIÓN EN TÉRMINOS DE PÉRDIDAS Y REPARACIÓN FUE DE CASI 4 MILLONES DE DÓLARES ESTADOUNIDENSES.

DE AHÍ QUE LA PREVENCIÓN ES MEJOR QUE LA DETECCIÓN.

Introducción

- Los 11 mayores hackeos y brechas de seguridad de la década pasada en EEUU que a día de hoy siguen teniendo repercusión

**Anthem, en
2015: se robó la
información
personal de 78
millones de
personas**



Introducción

- Los 11 mayores hackeos y brechas de seguridad de la década pasada en EEUU que a día de hoy siguen teniendo repercusión

JPMorgan Chase descubrió en 2014 una filtración que comprometió los datos personales de 83 millones de clientes



Introducción

- Los 11 mayores hackeos y brechas de seguridad de la década pasada en EEUU que a día de hoy siguen teniendo repercusión

En 2021 unos criminales han aprovechado una vulnerabilidad en un software de servidores de correo Microsoft, lo que está provocando ataques a miles de empresas



Introducción

- Los 11 mayores hackeos y brechas de seguridad de la década pasada en EEUU que a día de hoy siguen teniendo repercusión

Ciberdelincuentes rusos se infiltraron en las redes de docenas de administraciones en EEUU y de multinacionales tras comprometer la seguridad de un proveedor de software, SolarWind



Introducción

- Los 11 mayores hackeos y brechas de seguridad de la década pasada en EEUU que a día de hoy siguen teniendo repercusión

Yahoo reconoció en 2016 que había sido víctima de dos agujeros de seguridad que podrían haber afectado a los datos de sus 3.000 millones de usuarios

Las redes de Yahoo se vieron comprometidas en 2013 y en 2014 por unos ciberdelincuentes que consiguieron robar nombres, fechas de nacimiento, direcciones de correo **y las contraseñas encriptadas de los 3.000 millones de usuarios** de esta plataforma.

Los ciberdelincuentes primero consiguieron acceder a las redes de Yahoo enviándole **un link fraudulento mediante un *phishing* a un empleado de la compañía**, según concluyó después el FBI.

Introducción

- Los 11 mayores hackeos y brechas de seguridad de la década pasada en EEUU que a día de hoy siguen teniendo repercusión

Target fue hackeada en 2013, exponiendo los datos de 40 millones de tarjetas de crédito y débito



Introducción

- Los 11 mayores hackeos y brechas de seguridad de la década pasada en EEUU que a día de hoy siguen teniendo repercusión

En 2017, Equifax sufrió un incidente que supuso el robo de información sensible de 143 millones de sus clientes

Robaron nombres, números de la seguridad social, direcciones, fechas de nacimiento, los carné de conducir e **incluso datos sobre los pasaportes** de algunos de los clientes de la compañía.



Introducción

- Los 11 mayores hackeos y brechas de seguridad de la década pasada en EEUU que a día de hoy siguen teniendo repercusión

Marriott fue hackeada en 2018 y los ciberdelincuentes se llevaron la información personal de más de 500 millones de personas



Introducción

- Los 11 mayores hackeos y brechas de seguridad de la década pasada en EEUU que a día de hoy siguen teniendo repercusión

Un ciberdelincuente accedió a los sistemas de Capital One, extrayendo datos como cuentas bancarias o números de la seguridad social de 100 millones de personas





Introducción

- Los 11 mayores hackeos y brechas de seguridad de la década pasada en EEUU que a día de hoy siguen teniendo repercusión

Una vulnerabilidad de Facebook filtra los datos de más de 500.000 usuarios

En abril de este año, los datos de 533 millones de usuarios se publicaron en un foro de hacking muy popular, haciendo esta base de datos más gratuita y accesible que nunca.



Introducción

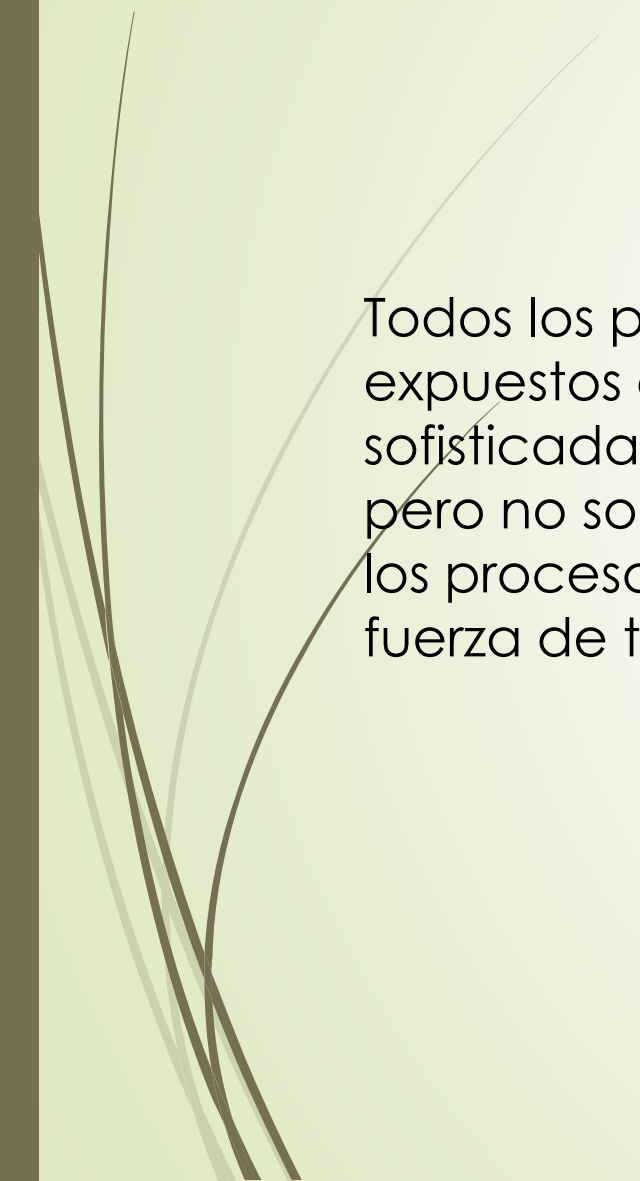
- Los 11 mayores hackeos y brechas de seguridad de la década pasada en EEUU que a día de hoy siguen teniendo repercusión

La aseguradora de hogar First American filtró sin querer 885 millones de datos de 2017 a 2019, incluyendo números de la seguridad social o fotos del carnet de conducir

First American después reconoció que **un bot creado por ciberdelincuentes había recopilado de forma masiva grandes cantidades de esta información** personal antes de que se eliminara de la red. Aunque no está claro a cuánta gente se pudo afectar, sí se sabe que se comprometieron 885 millones de registros, y a muchos de ellos podrían haber tenido acceso los criminales.



Sistemas de seguridad en la empresa



Todos los procesos empresariales impulsados por la tecnología están expuestos a amenazas a la seguridad y la privacidad. Las tecnologías sofisticadas son capaces de combatir los ataques a la ciberseguridad, pero no son suficientes: las organizaciones deben asegurarse de que los procesos empresariales, las políticas y el comportamiento de la fuerza de trabajo también minimicen o mitiguen estos riesgos.

Sistemas de seguridad en la empresa



Figura 1.2. Amenazas para la Seguridad [Martín, 2004].

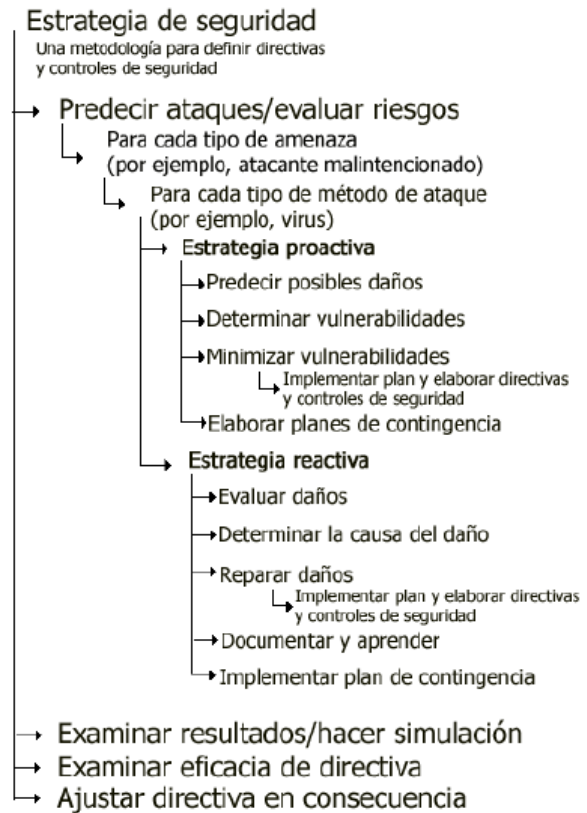
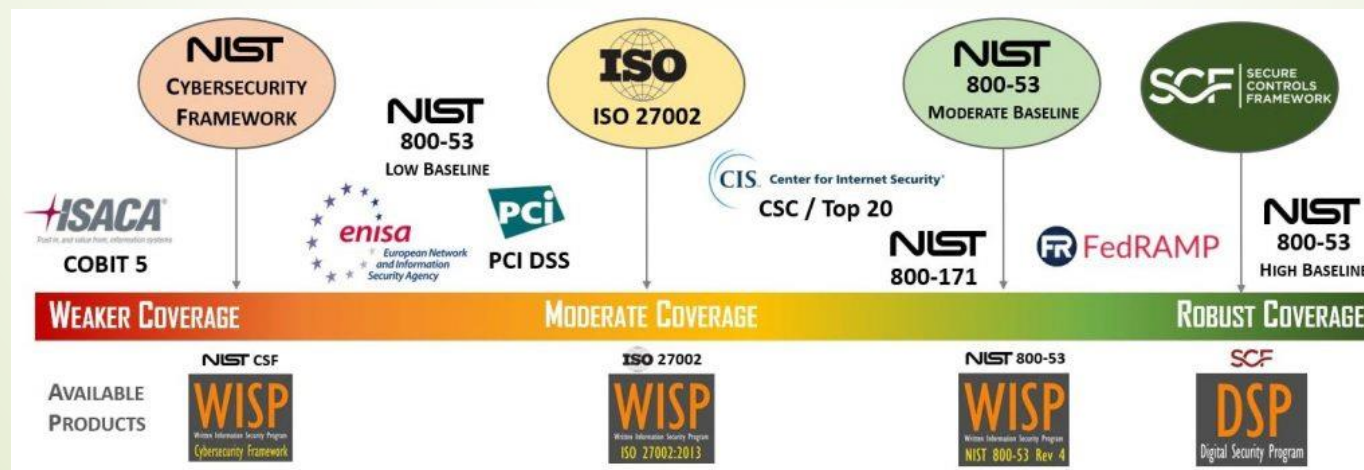


Figura 1.1 Metodología de estrategias de seguridad [Miguel, 1998].

Sistemas de seguridad en la empresa

Estándares de seguridad

Elegir un marco de ciberseguridad es más una decisión comercial que una decisión técnica. Esta decisión debe ser impulsada por una comprensión fundamental de lo que su organización necesita cumplir desde una perspectiva legal, reguladora y contractual, ya que esa comprensión establece el conjunto mínimo de requisitos necesarios para cumplir. Esta comprensión hace que sea bastante fácil determinar en qué parte del “espectro de cumplimiento” debe enfocarse para seleccionar un conjunto de principios de ciberseguridad a seguir que generalmente implica el Marco de Ciberseguridad NIST, ISO 27002 o NIST 800-53 como punto de partida. Una consideración clave para elegir un marco de seguridad cibernética se reduce al nivel de contenido que ofrece el marco:



Fuente: complianceforge.com

Sistemas de seguridad en la empresa

Estándares de seguridad

Si le pide a un profesional de ciberseguridad que identifique su mejor práctica preferida, generalmente se reduce a NIST o ISO. Los dos grandes atacantes de la seguridad de TI son NIST 800-53 e ISO 27002. Estos marcos líderes de ciberseguridad cubren los mismos componentes básicos de un programa de ciberseguridad, pero difieren en cierto contenido y diseño. Ambas pueden ser excelentes soluciones, pero es importante comprender que cada una tiene sus ventajas y desventajas. Por lo tanto, la elección debe ser impulsada por el tipo de negocio de su empresa. Ganar popularidad es el Marco de Seguridad Cibernética NIST (NIST CSF), pero carece de la cobertura adecuada para ser considerado un marco integral de seguridad cibernética.

Sistemas de seguridad en la empresa

Estándares de seguridad

NIST CSF < ISO 27002 < NIST 800-53 < Marco de control seguro

- **NIST Cybersecurity Framework (NIST CSF)** tiene la menor cobertura de los principales marcos de ciberseguridad. Funciona muy bien para empresas más pequeñas o no reguladas.
- **ISO 27002** es un marco de seguridad cibernética reconocido internacionalmente que proporciona cobertura para muchos requisitos comunes (por ejemplo, PCI DSS, HIPAA, etc.). Es importante tener en cuenta que las empresas no pueden certificar según ISO 27002, solo ISO 27001. El apéndice A de ISO 27001 contiene la descripción básica de los controles de seguridad necesarios para construir un Sistema de gestión de seguridad de la información (SGSI), pero ISO 27002 proporciona esos controles específicos que son necesario para implementar realmente ISO 27001.
- **NIST 800-53** incluye las direcciones ISO 27002 y NIST CSF, así como una gran cantidad de otros requisitos.
- El **Marco de controles seguros (SCF)** es un enfoque “mejor en su clase” que cubre NIST 800-53, ISO 27002 y NIST CSF. Al ser un híbrido, le permite abordar los tres marcos a la vez.

Sistemas de seguridad en la empresa

Estándares de seguridad

COBIT son las siglas de Control Objectives for Information and Related Technology . Es un marco creado por ISACA ([Information Systems Audit and Control Association](#)) para el gobierno y la gestión de TI. Fue diseñado para ser una herramienta de apoyo para los gerentes y permite salvar la brecha entre los problemas técnicos, los riesgos empresariales y los requisitos de control. En general, COBIT asegura la calidad, el control y la fiabilidad de los sistemas de información en una organización.

COBIT incluye la vinculación de los objetivos de negocio con su infraestructura de TI, proporcionando varios modelos de madurez y métricas que miden el logro al mismo tiempo que identifican las responsabilidades de negocio asociadas de los procesos de TI. El enfoque principal de COBIT fue ilustrado con un modelo basado en procesos subdividido en cuatro dominios específicos, incluyendo:

- Planificación y organización
- Entrega y apoyo
- Adquisición e implementación
- Monitoreo y evaluación

Todo esto se entiende también en 34 procesos según la línea específica de responsabilidades.

COBIT tiene una alta posición en los marcos de negocios y ha sido reconocido bajo varios estándares internacionales, incluyendo ITIL, CMMI, COSO, PRINCE2, TOGAF, PMBOK, TOGAF, e ISO 27000. COBIT actúa como un integrador de directrices, uniendo todas las soluciones bajo un mismo paraguas.

Sistemas de seguridad en la empresa

Estándares de seguridad

CSA

Cloud Security Alliance (CSA) es la organización líder mundial dedicada a definir y aumentar el conocimiento de las mejores prácticas para ayudar a garantizar un entorno de cloud computing seguro. CSA aprovecha la experiencia en la materia de los profesionales de la industria, asociaciones, gobiernos y sus miembros corporativos e individuales para ofrecer investigación, educación, certificación, eventos y productos específicos para la seguridad en la nube. Las actividades, el conocimiento y la extensa red de CSA benefician a toda la comunidad afectada por la nube – desde proveedores y clientes, hasta gobiernos, empresarios y la industria de seguros – y proporcionan un foro a través del cual diversas partes pueden trabajar juntas para crear y mantener un ecosistema de nube de confianza.

Sistemas de seguridad en la empresa

Estándares de seguridad

OWASP

El **Open Web Application Security Project**, o OWASP, es una organización internacional sin fines de lucro dedicada a la seguridad de aplicaciones web. Uno de los principios básicos de OWASP es que todos sus materiales estén disponibles gratuitamente y sean fácilmente accesibles en su sitio web, haciendo posible que cualquiera pueda mejorar la seguridad de su propia aplicación web. Los materiales que ofrecen incluyen documentación, herramientas, videos y foros. Quizás su proyecto más conocido es el Top 10 de OWASP.

La lista de las 10 principales vulnerabilidades de OWASP son:

- Inyección
- Autenticación rota
- Exposición de datos confidenciales
- Entidades externas XML (XXE)
- Control de acceso roto
- Errores de seguridad
- Secuencias de comandos entre sitios (XSS)
- Deserialización Insegura
- Uso de componentes con vulnerabilidades conocidas
- Registro y monitoreo insuficientes

Sistemas de seguridad en la empresa

Estándares de seguridad

¿Qué es un ISMS (Information Security Management Systems)?

Un sistema de gestión de la seguridad de la información, es un marco de políticas y controles que gestionan la seguridad y los riesgos de forma sistemática y a través de toda la seguridad de la información de la empresa.

Estos controles de seguridad pueden seguir las normas de seguridad comunes o estar más enfocados a su industria. Por ejemplo, ISO 27001 es un conjunto de especificaciones que detallan cómo crear, administrar e implementar políticas y controles del ISMS. La ISO no ordena acciones específicas, sino que proporciona directrices para el desarrollo de estrategias apropiadas para el ISMS.

El marco del ISMS suele centrarse en la evaluación y la gestión de riesgos. Piense en él como un enfoque estructurado para el equilibrio entre la mitigación de riesgos y el costo (riesgo) en que se incurre. Las organizaciones que operan en sectores verticales de la industria estrictamente regulados, como la atención sanitaria o la defensa nacional, pueden necesitar un amplio alcance de actividades de seguridad y una estrategia de mitigación de riesgos.

Sistemas de seguridad en la empresa

Estándares de seguridad

Marcos populares de la ISMS

La ISO 27001 es líder en seguridad de la información, pero otros marcos ofrecen también una valiosa orientación. Estos otros marcos suelen tomar prestado de la ISO 27001 o de otras directrices específicas de la industria.

- ➤ **ITIL**, el marco de trabajo ITSM ampliamente adoptado, tiene un componente dedicado llamado Gestión de la Seguridad de la Información (ISM). El objetivo de ISM es alinear la seguridad de la TI y de la empresa para garantizar que la InfoSec se gestione de forma eficaz en todas las actividades.
- ➤ **COBIT**, otro marco centrado en la tecnología de la información, dedica mucho tiempo a la forma en que la gestión de activos y la gestión de la configuración son fundamentales para la seguridad de la información, así como para casi todas las demás funciones de la ITSM, incluso las que no están relacionadas con InfoSec.

Sistemas de seguridad en la empresa

Estándares de seguridad

Controles de seguridad del ISMS

Los controles de seguridad del ISMS abarcan múltiples dominios de seguridad de la información, como se especifica en la norma ISO 27001. El catálogo contiene directrices prácticas con los siguientes objetivos:

- ➤ **Políticas de seguridad de la información.** Una dirección y un apoyo generales ayudan a establecer políticas de seguridad adecuadas. La política de seguridad es única para su empresa, concebida en el contexto de sus cambiantes necesidades empresariales y de seguridad.
- ➤ **Organización de la seguridad de la información.** Aborda las amenazas y los riesgos dentro de la red corporativa, incluidos los ciberataques de entidades externas, las amenazas internas, los fallos del sistema y la pérdida de datos.
- ➤ **Gestión de activos.** Este componente abarca los activos de la organización dentro y fuera de la red informática de la empresa, lo que puede implicar el intercambio de información empresarial sensible.

Sistemas de seguridad en la empresa

Estándares de seguridad

Controles de seguridad del ISMS

- ➤ **Seguridad de los recursos humanos.** Políticas y controles relativos a su personal, actividades y errores humanos, incluyendo medidas para reducir el riesgo de amenazas internas y capacitación de la fuerza laboral para reducir lapsos de seguridad no intencionales.
- ➤ **Seguridad física y ambiental.** Estas directrices cubren las medidas de seguridad para proteger el hardware físico de TI de daños, pérdidas o accesos no autorizados. Si bien muchas organizaciones están aprovechando la transformación digital y manteniendo la información confidencial en redes de nubes seguras fuera de las instalaciones, debe considerarse la seguridad de los dispositivos físicos utilizados para acceder a esa información.
- ➤ **Gestión de las comunicaciones y las operaciones.** Los sistemas deben funcionar respetando y manteniendo las políticas y controles de seguridad. Las operaciones diarias de TI, como el suministro de servicios y la gestión de problemas, deben seguir las políticas de seguridad de TI y los controles del SGSI.

Sistemas de seguridad en la empresa

Estándares de seguridad

Controles de seguridad del ISMS

- ➤ **Control de acceso.** Este dominio de políticas se ocupa de limitar el acceso al personal autorizado y de controlar el tráfico de la red para detectar comportamientos anómalos. Los permisos de acceso se relacionan con los medios digitales y físicos de la tecnología. Las funciones y responsabilidades de los individuos deben estar bien definidas, y el acceso a la información empresarial sólo debe estar disponible cuando sea necesario.
- ➤ **Adquisición, desarrollo y mantenimiento de sistemas de información.** Las mejores prácticas de seguridad deben mantenerse a lo largo de todo el ciclo de vida del sistema informático, incluidas las fases de adquisición, desarrollo y mantenimiento.
- ➤ **Seguridad de la información y gestión de incidentes.** Identificar y resolver los problemas de la TI de manera que se minimice el impacto para los usuarios finales. En entornos de infraestructura de red complejos, pueden requerirse soluciones tecnológicas avanzadas para identificar métricas de incidentes perspicaces y mitigar proactivamente los posibles problemas.

Sistemas de seguridad en la empresa

Estándares de seguridad

Controles de seguridad del ISMS

- ➤ **Gestión de la continuidad del negocio.** Evitar las interrupciones de los procesos comerciales siempre que sea posible. Lo ideal sería que cualquier situación de desastre fuera seguida inmediatamente por la recuperación y los procedimientos para minimizar los daños.
- ➤ **Cumplimiento.** Los requisitos de seguridad deben ser aplicados por los organismos reguladores.
- ➤ **Criptografía.** Entre los controles más importantes y eficaces para proteger la información sensible, no es una bala de plata por sí sola. Por lo tanto, el ISMS rige la forma en que se aplican y gestionan los controles criptográficos.
- ➤ **Relaciones con los proveedores.** Es posible que los proveedores y los socios comerciales de terceros necesiten acceder a la red y a los datos sensibles de los clientes. Puede que no sea posible aplicar controles de seguridad a algunos proveedores. Sin embargo, deben adoptarse controles adecuados para mitigar los posibles riesgos mediante políticas de seguridad de la tecnología de la información y obligaciones contractuales.

Test módulo 1

1.- Cual de los siguientes son fundamentales de la seguridad informática (se puede marcar mas de una opción)

- a. Confidencialidad
- b. Integridad
- c. Flexibilidad
- d. Disponibilidad
- e. Aislamiento

2.-Cual de las siguiente no es una prácticas de Seguridad Informática correcta (se puede marcar mas de una opción)

- a. Balancear protección con utilidad
- b. Basta con un antivirus
- c. Dividir los usuarios y los recursos
- d. Asignar privilegios mínimos
- e. Utilizar defensas independientes
- f. Planear las contingencias
- g. Registrar, Registrar y Registrar
- h. Realiza pruebas frecuentemente
- i. Solo los informáticos son los responsables

Test módulo 1

3.- Seleccionar la opción correcta

- a. El plan de seguridad de una empresa debe incluir una estrategia reactiva.
- b. El plan de seguridad de una empresa debe incluir una estrategia reactiva y proactiva.
- c. El plan de seguridad de una empresa debe incluir una estrategia proactiva.

4.-Escribe al menos tres métodos de ciberataques y explica uno de ellos

Test módulo 1

5.- Seleccionar la opción incorrecta. Tras un ciberataque es recomendable.....

- a. Evaluar la pérdida de productividad, de datos y el tiempo de recuperación.
- b. Determinar la causa del daño
- c. Documentar y aprender.
- d. Corregir el error de seguridad y no informar.
- e. Hacer un seguimiento del lugar donde se originó.

6.-Completa la frase

Si le pide a un profesional de ciberseguridad que identifique su mejor práctica preferida, generalmente se reduce a NIST o ISO. Los dos grandes atacantes de la seguridad de TI son NIST 800-53 e ISO 27002. Estos marcos líderes de ciberseguridad cubren los mismos componentes básicos de un programa de ciberseguridad, pero difieren en cierto contenido y diseño. Ambas pueden ser excelentes soluciones, pero es importante comprender que cada una tiene sus ventajas y desventajas. Por lo tanto, la elección debe ser impulsada por



Test módulo 1

7.- Escribe tu definición de ciberseguridad



Sistemas de seguridad en la empresa



Sistemas de seguridad en la empresa

Ciberseguridad: tipos de ataques y en qué consisten

Un ciberataque es un conjunto de acciones ofensivas contra sistemas de información. Estos pueden ser bases de datos, redes informáticas, etc. El objetivo es dañar, alterar o destruir organizaciones o personas. Además, pueden anular los servicios que prestan, robar datos o usarlos para espiar.

Vivimos en una era digital. Hoy en día la mayoría de las personas utilizan un ordenador con Internet. Por eso, debido a la dependencia de las herramientas digitales, la actividad informática ilegal crece sin parar y busca nuevas y más efectivas formas de delinquir.

Link recomendado : <https://www.incibe.es/protege-tu-empresa/blog/sabes-funciona-ciberataque-utiliza-ingenieria-social>

Sistemas de seguridad en la empresa

Lista de métodos de ataque de ciberseguridad

- Ataque de denegación de servicio
- Ingeniería social
- Virus
- Gusanos
- Caballos de troya
- Modificación de paquetes (Tear Drop Attack)
- Adivinación de contraseñas
- Interceptación de correos electrónicos

Sistemas de seguridad en la empresa

Ciberseguridad: tipos de ataques y en qué consisten

Phishing

El phishing es un tipo de ingeniería social que se emplea, por lo general, para robar datos de usuario. Pueden ser números de tarjetas de crédito o contraseñas, por ejemplo. Ocurre cuando un delincuente se hace pasar por una persona de confianza. Entonces, engaña a la víctima para que abra un mensaje de texto, correo electrónico o SMS mediante un enlace malicioso. Este enlace puede causar la congelación de un sistema ransomware, revelar información confidencial o instalar malware.

Se trata de una técnica sencilla y muy fácil de utilizar, por eso es una de las más peligrosas. Puede tener resultados desastrosos. Para un individuo, puede suponer el robo de identidad, de fondos o la realización de compras no autorizadas.

Sistemas de seguridad en la empresa

Ciberseguridad: tipos de ataques y en qué consisten

Spear phishing

Por otro lado, los spear phishing son ataques informáticos que tienen como objetivo una persona o empleado específico de una compañía en concreto. Para llevar a cabo este tipo de ataques los criminales recopilan meticulosamente información sobre la víctima para ganarse su confianza. Caer en estos ataques suele ser muy usual, ya que un correo bien elaborado, ya sea con enlace o documento adjunto malicioso, es muy difícil de distinguir de uno legítimo.

Esta técnica se utiliza mucho para atacar empresas, bancos o personas influyentes.

Sistemas de seguridad en la empresa

Ciberseguridad: tipos de ataques y en qué consisten

Whaling

En el tercer lugar de la lista de tipos de ataques en ciberseguridad nos encontramos los ataques whaling. Estos ataques se centran en un perfil de alto directivo, como CEOs o CFOs. El objetivo, igual que los anteriores, es robar información vital, ya que aquellos que ocupan puestos altos en una empresa suelen tener acceso ilimitado a información confidencial. En la mayoría de estas estafas llamadas «caza de ballenas» el delincuente manipula a la víctima para permitir transferencias electrónicas de alto valor.

La frase «caza de ballenas» hace referencia al tamaño del ataque, ya que las ballenas son atacadas dependiendo de su posición dentro de la organización. Este tipo de ataques son más fáciles de detectar en comparación con los phishing estándar. Los responsables de seguridad informática de una empresa pueden disminuir la efectividad de este pirateo.

Sistemas de seguridad en la empresa

Ciberseguridad: tipos de ataques y en qué consisten

Malware o software malicioso

En segundo lugar, entre los tipos de ataques en ciberseguridad se encuentran los malware. Un malware es un código creado para corromper sigilosamente un sistema informático. Es un término amplio que describe cualquier programa o código malicioso perjudicial para los sistemas. Un malware intrusivo invade, daña o deshabilita ordenadores, sistemas informáticos, móviles, etc. asumiendo el control de las operaciones.

El objetivo del malware suele ser sacarle dinero al usuario de forma ilícita. Aunque este por lo general no puede dañar el hardware de los sistemas, sí puede robar, cifrar, borrar datos, o secuestrar funciones básicas de un ordenador, así como espiar su actividad sin que nadie lo note.

Los malware incluyen muchos tipos de softwares maliciosos, como spyware, ransomware, troyanos, etc.

Sistemas de seguridad en la empresa

Ciberseguridad: tipos de ataques y en qué consisten

Ransomware o secuestro de datos

El ransomware es un software malicioso que al penetrar en nuestro equipo le otorga al hacker la capacidad de bloquear un dispositivo desde una ubicación remota. También a encriptar los archivos quitándole al usuario el control de toda la información y datos almacenados.

En cuanto a su método de propagación, los ransomware normalmente se transmiten como un troyano. Es decir, infectando el sistema operativo. Por ejemplo, descargando un archivo o explotando una vulnerabilidad del software. El ciberdelincuente, que ha cifrado los archivos del sistema operativo inutilizando el dispositivo, suele pedir un rescate a cambio de quitar la restricción a los documentos.

Sistemas de seguridad en la empresa

Ciberseguridad: tipos de ataques y en qué consisten

Descargas automáticas

Las descargas automáticas para propagar malware son uno de los métodos más comunes entre los tipos de ataques en ciberseguridad. Los ciberdelincuentes buscan páginas web inseguras y plantan un script malicioso en el código HTTP o PHP en una de ellas. Este script puede instalar malware directamente en el dispositivo del usuario que visite el sitio. También puede coger la forma en un iframe que redirige a la víctima a un sitio controlado por los atacadores. Estos ataques se llaman «descargas automáticas» porque no requieren ninguna acción por parte de la víctima. Solo tiene que visitar dicha web.

Sistemas de seguridad en la empresa

Ciberseguridad: tipos de ataques y en qué consisten

Troyano

Un troyano es un programa de software malicioso que intenta camuflarse como herramienta útil. Se propagan al parecer un software y persuadir a una víctima para que lo instale. Los troyanos se consideran entre los tipos de ataques en ciberseguridad más peligrosos, a menudo diseñados para robar información financiera.

Los usuarios son engañados por alguna forma de ingeniería social para que carguen y ejecuten troyanos en sus sistemas. Una vez activados, estos permiten a los cibercriminales espiarte o robar tu información confidencial. A diferencia de virus y gusanos, los troyanos no pueden autorreplicarse.

Para que un malware sea un troyano solo tiene que acceder y controlar la máquina anfitriona sin ser advertido, bajo una apariencia inocua.

Sistemas de seguridad en la empresa

Ciberseguridad: tipos de ataques y en qué consisten

Ataques a una web

Inyección SQL

Entre los tipos de ataques en ciberseguridad más conocidos se encuentra la Inyección SQL. Se trata de un método de infiltración de un código intruso que se aprovecha de una vulnerabilidad informática presente en una aplicación. Es decir, se aprovechan de errores de diseño habituales en las páginas web. La amenaza de las inyecciones SQL supone un grave problema de seguridad relacionado con las bases de datos. Se emplean para manipular, robar o destruir datos.

Los ciberdelincuentes son capaces de inyectar consultas SQL maliciosas en el campo de entrada de una web, engañar a la aplicación para que haga uso de los comandos que deseen y acceder a la base de datos que quieran.

Un ataque de inyección SQL puede ralentizar el funcionamiento de una web, el robo, la pérdida o la corrupción de datos, la denegación de acceso de cualquier compañía o incluso la toma del control absoluto del servidor.

Sistemas de seguridad en la empresa

Ciberseguridad: tipos de ataques y en qué consisten

XSS o Cross Site Scripting

Los ataques XSS utilizan recursos web de terceros para ejecutar secuencias de comandos en el navegador web de la víctima o en la aplicación programable.

Son una especie de inyección en la que el atacante envía secuencias de comandos maliciosos al contenido de páginas web para desacreditarlas. Esto ocurre cuando una fuente dudosa puede adjuntar su propio código en las aplicaciones web. Este se envía en formas de fragmentos de código Javascript ejecutados por el navegador de la víctima.

Los exploits pueden incluir scripts ejecutables maliciosos en muchos idiomas, incluidos Flash, HTML, Java y Ajax. Los ataques XSS pueden ser muy devastadores. Sin embargo, aliviar las vulnerabilidades que permiten estos ataques es relativamente simple.

Sistemas de seguridad en la empresa

Ciberseguridad: medidas de protección a nivel individual

- ✓ **Utiliza un antivirus** para analizar todas las descargas y archivos sospechosos. Debes mantenerlo siempre actualizado y activo.
- ✓ **Mantén el sistema operativo, navegador y aplicaciones siempre actualizadas** a su última versión para evitar vulnerabilidades.
- ✓ **Utiliza contraseñas robustas y diferentes** para proteger todas tus cuentas. Si es posible, utiliza la verificación en dos pasos u otro factor de autenticación.
- ✓ **Desconfía de los adjuntos sospechosos, enlaces o promociones demasiado atractivos.** La mayoría de los fraudes se basan en ataques de ingeniería social que pueden ser detectados aplicando el sentido común.
- ✓ **Ten cuidado por dónde navegas.** Utiliza solo webs seguras con *https* y certificado digital y utiliza el modo incógnito cuando no quieras dejar rastro.
- ✓ **Descarga solo de sitios oficiales** aplicaciones o software legítimo para evitar acabar infectado por *malware*. En el caso de las aplicaciones, recuerda dar solo los *permisos* imprescindibles para su funcionamiento.
- ✓ **Evita conectarte a redes wifi públicas o a conexiones inalámbricas desconocidas.** Especialmente cuando vayas a intercambiar información sensible, como los datos bancarios. Y, en caso de que tengas que conectarte por una emergencia, trata de utilizar una *VPN*.
- ✓ **No compartas tu información personal** con cualquier desconocido ni la publiques o guardes en páginas o servicios webs no fiables.
- ✓ **Haz copias de seguridad** para minimizar el impacto de un posible ciberataque.

Recuerda que desde INCIBE, ponemos a tu disposición una línea telefónica gratuita de ayuda en ciberseguridad, 017.



TU AYUDA EN
CIBERSEGURIDAD

Practicas modulo 1

Crear usuarios en Windows

Acceso remoto Windows y pruebas

Firewall Windows y pruebas

Crear maquina virtual Linux Ubuntu con Virtual box

Crear usuarios en Linux

Control de acceso a Linux y gestión de usuarios en linux

Practicas modulo 1

<https://forum.huawei.com/enterprise/es/como-instalar-la-interface-de-loopback-en-windows-10-para-interactuar-con-el-simulador-ensp/thread/613300-100265>

<https://www.cyberciti.biz/faq/how-to-check-open-ports-in-linux-using-the-cli/>



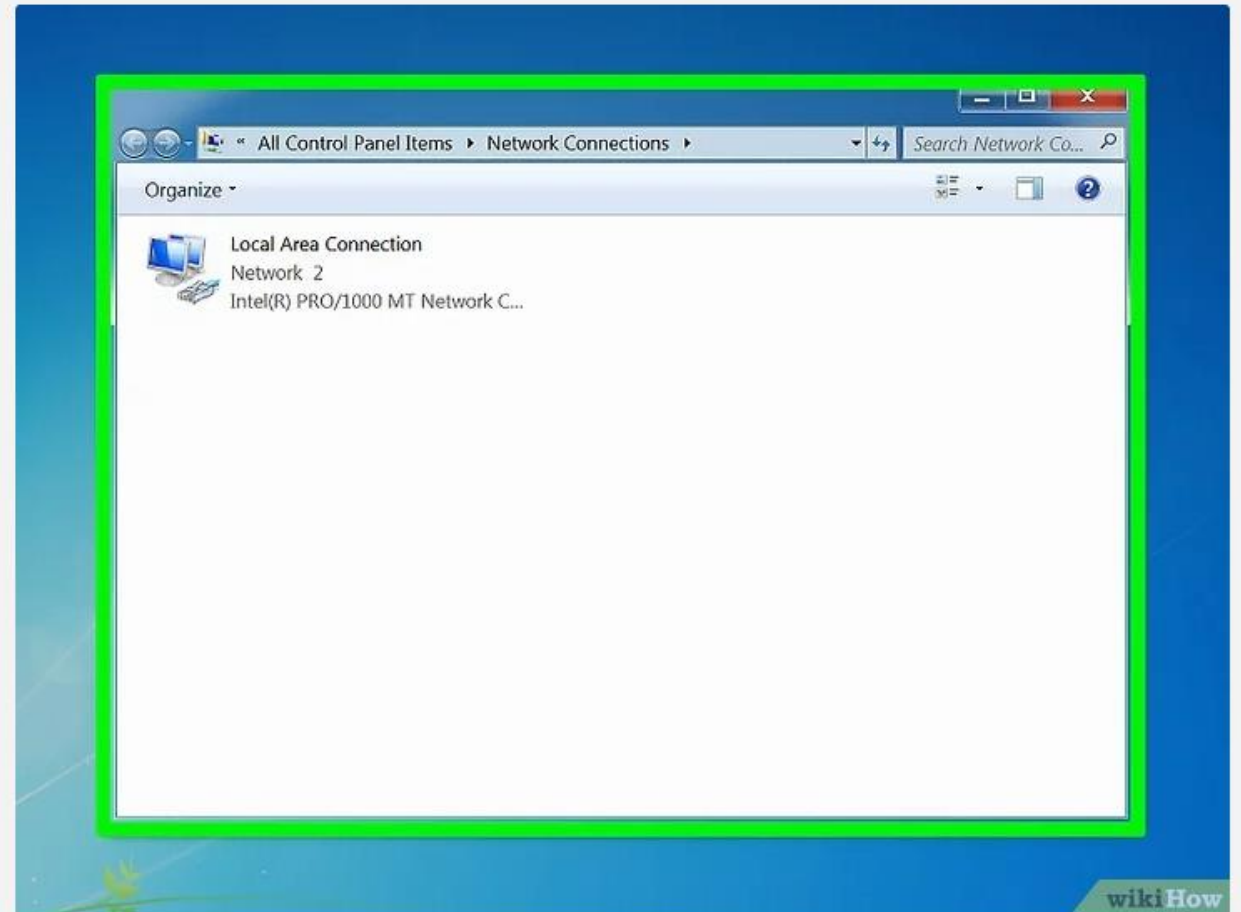
Praticas modulo 1

<https://forum.huawei.com/enterprise/es/como-instalar-la-interface-de-loopback-en-windows-10-para-interactuar-con-el-simulador-ensp/thread/613300-100265>

<https://www.cyberciti.biz/faq/how-to-check-open-ports-in-linux-using-the-cli/>

```
sudo tcpdump -i enp0s3 icmp and icmp[icmptype]=icmp-echo
```

2 Ingresa "ncpa.cpl" sin las comillas en el cuadro de búsqueda.



Practicas modulo 1: Seguridad en linux

<https://www.cyberciti.biz/faq/how-to-check-open-ports-in-linux-using-the-cli/>

¿Qué demonios son los puertos TCP y UDP?

Un puerto no es más que un número de 16 bits entre 0 y 65535. Por ejemplo, el puerto TCP número 22 puede reenviarse al servidor OpenSSH. Por lo tanto, el número de puerto 22 es una forma de identificar el proceso sshd (servidor OpenSSH).

Números de puerto;

- Los Puertos Conocidos son los del 0 al 1023.
- Los Puertos Registrados son los de 1024 a 49151.
- Los Puertos Dinámicos y Privados son los del 49152 al 65535.

Un puerto registrado es un puerto de red asignado por la Autoridad de Números Asignados de Internet (IANA) y almacenado en el archivo /etc/services. Utilice el comando `cat` o `grep/egrep` para ver los números de puerto y las asignaciones de servicio:

```
cat /etc/services
```

```
grep -w '80/tcp' /etc/services
```

```
grep -w '443/tcp' /etc/services
```

```
egrep -w '22/(tcp|udp)' /etc/services
```

Practicas modulo 1: Seguridad en linux

<https://www.cyberciti.biz/faq/how-to-check-open-ports-in-linux-using-the-cli/>

Comprobar puertos abiertos en Linux

El procedimiento para monitorear y mostrar puertos abiertos en Linux es el siguiente:

1. Abrir una aplicación de terminal Linux
2. Utilice el comando `ss` para mostrar todos los puertos TCP y UDP abiertos en Linux.
3. Otra opción es usar el comando `netstat` para enumerar todos los puertos en Linux.
4. Además de `ss/netstat` se puede utilizar el comando `lsof` para enumerar los archivos y puertos abiertos en el sistema basado en Linux.
5. Finalmente, uno puede usar el comando `nmap` para verificar los puertos TCP y UDP también.

Veamos todos los comandos y ejemplos en detalle.

Practicas modulo 1 : Seguridad en linux

<https://www.cyberciti.biz/faq/how-to-check-open-ports-in-linux-using-the-cli/>

Uso de netstat para enumerar los puertos abiertos

Escriba el siguiente comando Netstat
`sudo netstat -tulpn | grep LISTEN`

```
[vivek@nixcraft-nuc ~]$ sudo netstat -tulpn | grep LISTEN
tcp        0      0 127.0.0.1:53306      0.0.0.0:*            LISTEN      3371/AgentConnectix
tcp        0      0 127.0.0.1:44321      0.0.0.0:*            LISTEN      3784/pnacd
tcp        0      0 127.0.0.1:4330       0.0.0.0:*            LISTEN      9725/pnlogger
tcp        0      0 0.0.0.0:5355         0.0.0.0:*            LISTEN      1566/systemd-resolv
tcp        0      0 10.205.77.1:53       0.0.0.0:*            LISTEN      2416/dnsmasq
tcp        0      0 192.168.122.1:53     0.0.0.0:*            LISTEN      2081/dnsmasq
tcp        0      0 127.0.0.53:53        0.0.0.0:*            LISTEN      1566/systemd-resolv
tcp        0      0 0.0.0.0:22           0.0.0.0:*            LISTEN      1823/sshd
tcp        0      0 127.0.0.1:631        0.0.0.0:*            LISTEN      1821/cupsd
tcp6       0      0 :::1:44321           :::*                  LISTEN      3784/pnacd
tcp6       0      0 :::1:4330             :::*                  LISTEN      9725/pnlogger
tcp6       0      0 :::5355               :::*                  LISTEN      1566/systemd-resolv
tcp6       0      0 fd42:400:b94d:ad98::53 :::*                  LISTEN      2416/dnsmasq
tcp6       0      0 fe80::e400:44ff:feb7:53 :::*                  LISTEN      2416/dnsmasq
tcp6       0      0 :::22                 :::*                  LISTEN      1823/sshd
tcp6       0      0 :::1:631              :::*                  LISTEN      1821/cupsd
[vivek@nixcraft-nuc ~]$
```

Por ejemplo, el puerto TCP 631 abierto por el proceso cupsd y cupsd solo aparece en la dirección de bucle invertido (127.0.0.1). Del mismo modo, el puerto TCP 22 abierto por el proceso sshd y la lista sshd en todas las direcciones IP para conexiones ssh:

Proto	Recv-Q	Send-Q	Local Address	Foreign Address	State	User	Inode	PID/Program name
tcp	0	0	127.0.0.1:631	0.0.0.0:*	LISTEN	0	43385	1821/cupsd
tcp	0	0	0.0.0.0:22	0.0.0.0:*	LISTEN	0	44064	1823/sshd

Practicas modulo 1 : Seguridad en linux

<https://www.cyberciti.biz/faq/how-to-check-open-ports-in-linux-using-the-cli/>

Uso de netstat para enumerar los puertos abiertos

Del mismo modo, el puerto TCP 22 abierto por el proceso sshd y la lista sshd en todas las direcciones IP para conexiones ssh:

Proto	Recv-Q	Send-Q	Local Address	Foreign Address	State	User	Inode	PID/Program name
tcp	0	0	127.0.0.1:631	0.0.0.0:*	LISTEN	0	43385	1821/cupsd
tcp	0	0	0.0.0.0:22	0.0.0.0:*	LISTEN	0	44064	1823/sshd

Dónde

- **-t** : Todos los puertos TCP
- **-u** : Todos los puertos UDP
- **-l** : Mostrar sockets de servidor de escucha
- **-p** : Mostrar el PID y el nombre del programa al que pertenece cada socket
- **-n** : No resolver nombres
- **| grep LISTEN** : Solo muestra los puertos abiertos aplicando el filtro de comando grep.

Practicas modulo 1 : Seguridad en linux

<https://www.cyberciti.biz/faq/how-to-check-open-ports-in-linux-using-the-cli/>

Usar ss para enumerar los puertos abiertos

El comando ss se utiliza para volcar estadísticas de sockets. Permite mostrar información similar a netstat. Puede mostrar más TCP e información de estado que otras herramientas. La sintaxis es:

```
sudo ss -tulpn
```

Salidas de ejemplo:

```
Netid State Recv-Q Send-Q Local Address:Port Peer Address:Port
udp UNCONN 0 0 224.0.0.251:5353 0.0.0.0:* usuarios:(("chromium-browser",pid=12893,fd=419))
udp UNCONN 0 0 224.0.0.251:5353 0.0.0.0:* usuarios:(("chromium-browser",pid=12938,fd=395))
udp UNCONN 0 0 224.0.0.251:5353 0.0.0.0:* usuarios:(("chrome",pid=10111,fd=178))
udp UNCONN 0 0 0.0.0.0:5355 0.0.0.0:* usuarios:(("systemd-resolve",pid=1566,fd=12))
usuarios:(("AgentAntidote.b",pid=6206,fd=16),("AgentAntidote",pid=6164,fd=16),("AgentConnectix.",pid=3371,fd=16))
tcp LISTEN 0 5 127.0.0.1:44321 0.0.0.0:* usuarios:(("pmcd",pid=3784,fd=0))
tcp LISTEN 0 5 127.0.0.1:4330 0.0.0.0:* usuarios:(("pmlogger",pid=9725,fd=9))
tcp LISTEN 0 128 0.0.0.0:5355 0.0.0.0:* usuarios:(("systemd-resolve",pid=1566,fd=13))
tcp LISTEN 0 5 10.205.77.1:53 0.0.0.0:* usuarios:(("dnsmasq",pid=2416,fd=9))
```

Practicas modulo 1 : Seguridad en linux

<https://www.cyberciti.biz/faq/how-to-check-open-ports-in-linux-using-the-cli/>

Puertos de escucha y aplicaciones mediante el comando lsof

Ejecutemos lo siguiente para verificar los puertos TCP y UDP abiertos usando el comando lsof:

`sudo lsof -i -P -n | grep LISTEN`

Donde,

- **-i** : Buscar puertos de listado
- **-P**: Inhibe la conversión de números de puerto a nombres de puerto para archivos de red. Inhibir la conversión puede hacer que lsof corra un poco más rápido. También es útil cuando la búsqueda de nombres de puerto no funciona correctamente.
- **-n** : No utilice el nombre DNS
- **| grep LISTEN** : De nuevo sólo mostrar los puertos en estado LISTEN utilizando el comando grep como filtro.

```
[vivek@nixcraft-nuc ~]$ sudo lsof -i -P -n | grep LISTEN
systemd-r 1566 systemd-resolve 13u IPv4 32639 0t0 TCP *:5355 (LISTEN)
systemd-r 1566 systemd-resolve 15u IPv6 32642 0t0 TCP *:5355 (LISTEN)
systemd-r 1566 systemd-resolve 18u IPv4 32645 0t0 TCP 127.0.0.53:53 (LISTEN)
cupsd     1821      root      9u IPv6 43384 0t0 TCP [::]:631 (LISTEN)
cupsd     1821      root     10u IPv4 43385 0t0 TCP 127.0.0.1:631 (LISTEN)
sshd      1823      root      5u IPv4 44064 0t0 TCP *:22 (LISTEN)
sshd      1823      root      7u IPv6 44066 0t0 TCP *:22 (LISTEN)
dnsmasq   2081     dnsmasq    6u IPv4 47651 0t0 TCP 192.168.122.1:53 (LISTEN)
dnsmasq   2416      lxd       9u IPv4 47044 0t0 TCP 10.205.77.1:53 (LISTEN)
dnsmasq   2416      lxd      11u IPv6 47046 0t0 TCP [fe80::e400:44ff:feb7:3233]:53 (LISTEN)
dnsmasq   2416      lxd      13u IPv6 47048 0t0 TCP [fd42:400:b94d:ad98::1]:53 (LISTEN)
AgentConn 3371     vivek     16u IPv4 65814 0t0 TCP 127.0.0.1:53306 (LISTEN)
pmcd      3784     pcpx      0u IPv4 63438 0t0 TCP 127.0.0.1:44321 (LISTEN)
pmcd      3784     pcpx      3u IPv6 63439 0t0 TCP [::]:44321 (LISTEN)
AgentAnti 6164     vivek     16u IPv4 65814 0t0 TCP 127.0.0.1:53306 (LISTEN)
AgentAnti 6206     vivek     16u IPv4 65814 0t0 TCP 127.0.0.1:53306 (LISTEN)
pmlogger  9725     pcpx      9u IPv4 74585 0t0 TCP 127.0.0.1:4330 (LISTEN)
pmlogger  9725     pcpx     10u IPv6 74586 0t0 TCP [::]:4330 (LISTEN)
```

Practicas modulo 1 : Seguridad en linux

<https://www.cyberciti.biz/faq/how-to-check-open-ports-in-linux-using-the-cli/>

Comando nmap

Además, a los comandos anteriores se puede usar el comando nmap, que es una herramienta de código abierto para la exploración de redes y la auditoría de seguridad. Vamos a usar nmap para encontrar y listar puertos abiertos en Linux:

```
$ sudo nmap -sT -O localhost
```

```
$ sudo nmap -sU -O 192.168.2.254 ##[ list open UDP ports ]##
```

```
$ sudo nmap -sT -O 127.0.0.1 ##[ list open TCP ports ]##
```

```
$ sudo nmap -sTU -O 192.168.2.24
```

Salidas de muestra:

```
Starting Nmap 7.70 ( https://nmap.org ) at 2019-07-22 23:49 IST
Nmap scan report for localhost (127.0.0.1)
Host is up (0.00024s latency).
Other addresses for localhost (not scanned): ::1
Not shown: 998 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
631/tcp    open  ipp
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6.32
OS details: Linux 2.6.32
Network Distance: 0 hops

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 2.31 seconds
```


Practicas modulo 1 : Seguridad en linux

<https://www.cyberciti.biz/faq/how-to-check-open-ports-in-linux-using-the-cli/>

El puerto abierto no significa que nadie de fuera pueda acceder a esos puertos.

Hasta ahora, usted sabe cómo encontrar y enumerar los puertos TCP y UDP abiertos en Linux. Sin embargo, esos puertos aún pueden ser bloqueados por software, nube o firewall de hardware. Por lo tanto, debe verificar que su firewall corporativo no esté bloqueando el acceso entrante o saliente. Por ejemplo, en el [servidor Linux enumeramos o volcamos las reglas](#) del firewall utilizando la siguiente sintaxis:

```
sudo iptables -S
```

```
# IPv6
```

```
sudo ip6tables -S
```

```
ubuntu@ubuntu1804:~$ sudo iptables -S
-P INPUT ACCEPT
-P FORWARD ACCEPT
-P OUTPUT ACCEPT
ubuntu@ubuntu1804:~$ sudo ip6tables -S
-P INPUT ACCEPT
-P FORWARD ACCEPT
-P OUTPUT ACCEPT
ubuntu@ubuntu1804:~$
```



Practicas modulo 1 : Seguridad en linux

<https://www.cyberciti.biz/faq/how-to-check-open-ports-in-linux-using-the-cli/>

Conclusión

En conclusión, encontrar puertos abiertos es una de las tareas más fundamentales de un administrador de sistemas Linux por razones de seguridad. Por lo tanto, cierre todos los puertos no deseados y configure el firewall como [UFW](#) y [Firewalld](#) para abrir o bloquear puertos según sus requisitos. Después de leer este tutorial, debe tener una buena comprensión de cómo verificar si hay puertos abiertos en Linux. Consulte la lista oficial de TCP, UDP y otros puertos de la IANA [aquí](#) para obtener más información.

Practicas modulo 1 : Seguridad en linux

Ataquemos desde window 10 a Linux con un ping

```
PS E:\cursos\IFCM026PO\repo\pingtest> ping 8.8.8.8 -t
```

```
Pinging 8.8.8.8 with 32 bytes of data:
```

```
Reply from 8.8.8.8: bytes=32 time=5ms TTL=119
```

```
Reply from 8.8.8.8: bytes=32 time=5ms TTL=119
```

```
Reply from 8.8.8.8: bytes=32 time=5ms TTL=119
```

```
Reply from 8.8.8.8: bytes=32 time=4ms TTL=119
```

```
Reply from 8.8.8.8: bytes=32 time=4ms TTL=119
```

```
Reply from 8.8.8.8: bytes=32 time=5ms TTL=119
```

```
Reply from 8.8.8.8: bytes=32 time=5ms TTL=119
```

```
Reply from 8.8.8.8: bytes=32 time=5ms TTL=119
```

```
Reply from 8.8.8.8: bytes=32 time=4ms TTL=119
```

```
Reply from 8.8.8.8: bytes=32 time=5ms TTL=119
```

```
Reply from 8.8.8.8: bytes=32 time=5ms TTL=119
```

```
Reply from 8.8.8.8: bytes=32 time=4ms TTL=119
```

```
Reply from 8.8.8.8: bytes=32 time=5ms TTL=119
```

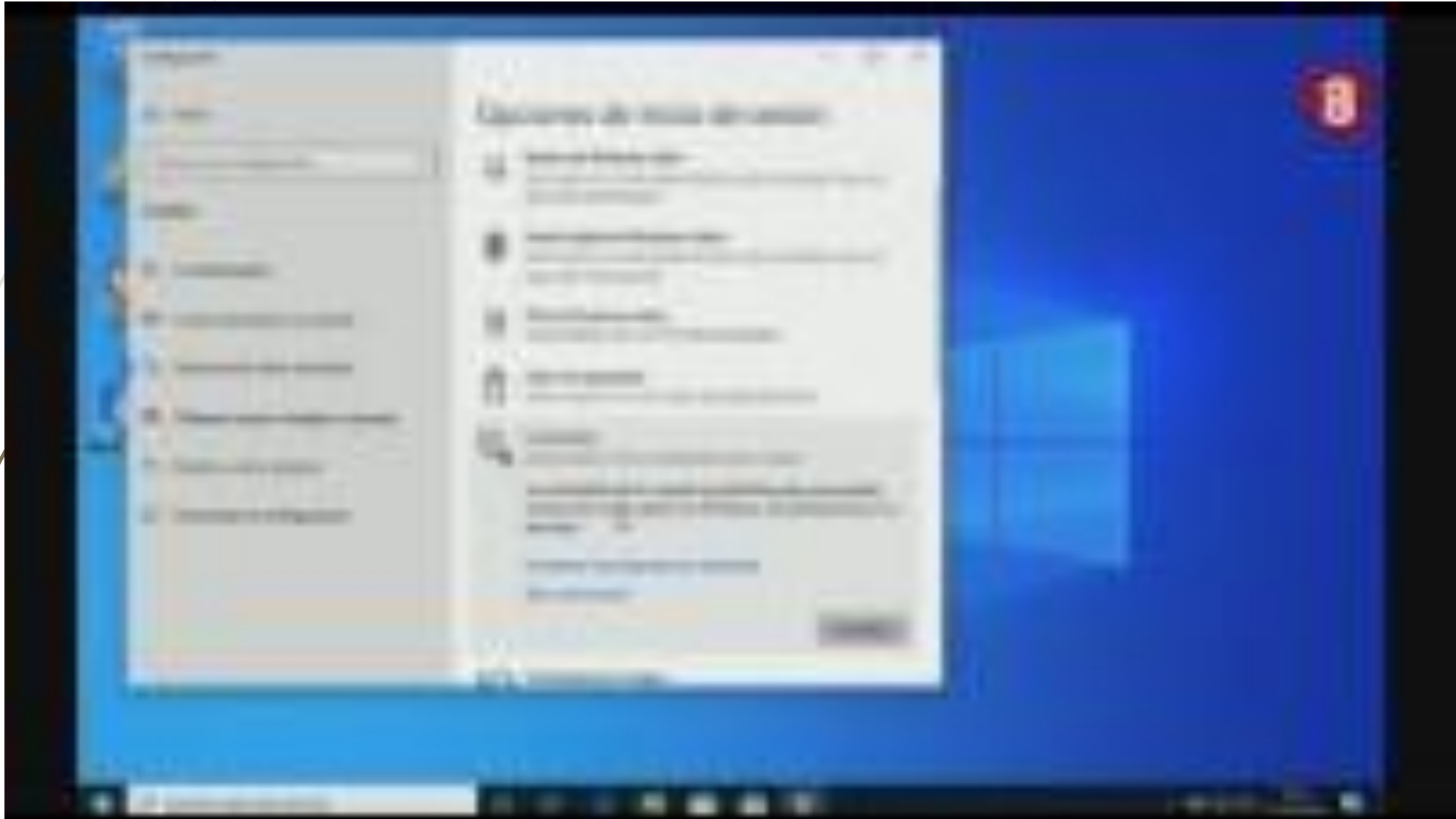
```
Reply from 8.8.8.8: bytes=32 time=4ms TTL=119
```

```
Reply from 8.8.8.8: bytes=32 time=5ms TTL=119
```

```
Reply from 8.8.8.8: bytes=32 time=5ms TTL=119
```

```
Reply from 8.8.8.8: bytes=32 time=4ms TTL=119
```

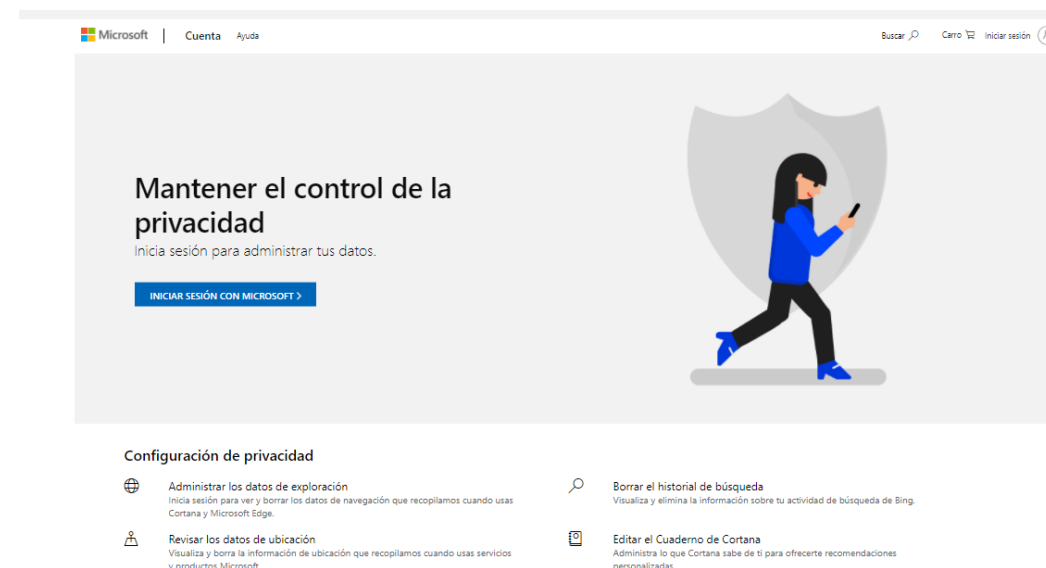
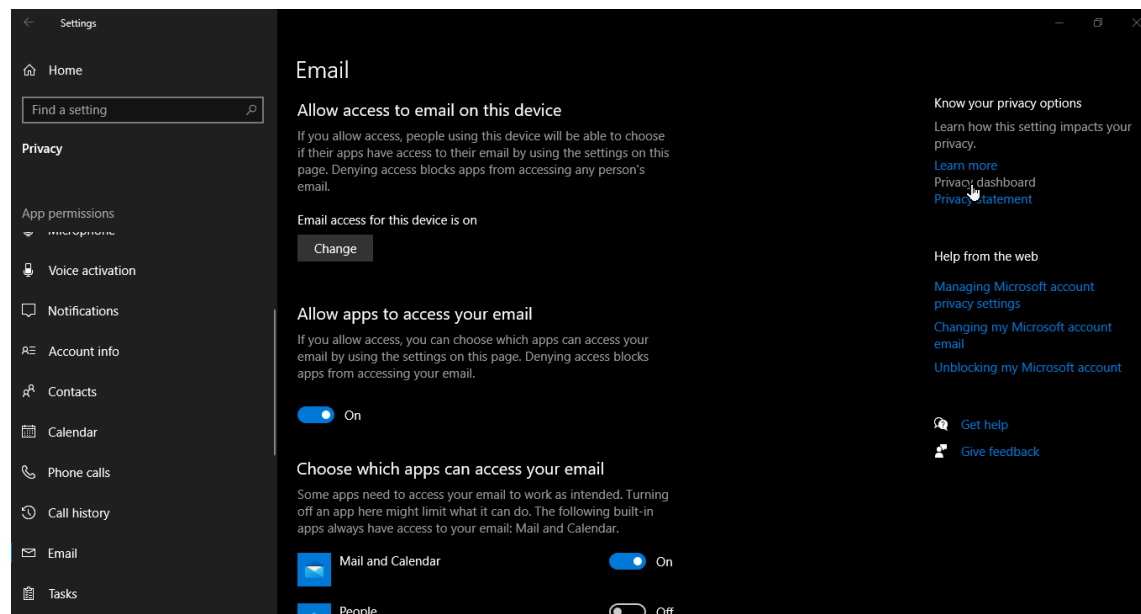
Practicas modulo 1 : Seguridad en Windows 10



Practicas modulo 1 : Seguridad en Windows 10



Practicass modulo 1 : Seguridad en Windows 10



Sistemas de seguridad en la empresa

Ciberseguridad: medidas de protección a nivel de empresa

¿Por qué es importante tener herramientas de ciberseguridad en tu empresa?

- Datos de un estudio de CISCO comentan que el cibercrimen es relativamente más rentable que todas las operaciones combinadas del tráfico de drogas en el mundo.
- En la Dark Web se pueden conseguir herramientas profesionales de hackeo de todo tipo.
- Una investigación de Netscout, afirma que solo se tardan 5 minutos en hackear un dispositivo de IOT no protegido.
- Según IBM, solo el 38% de las empresas a nivel mundial han declarado estar equipadas y preparadas para responder efectivamente frente a ciberataques de gran magnitud.

De acuerdo con una encuesta de AttackIQ, realizada a 577 profesionales de TI y seguridad de TI en los Estados Unidos, arrojó que ***el 53% de las empresas no saben si sus herramientas de ciberseguridad funcionan y no están completamente seguras de que eviten las violaciones de datos.***

Sistemas de seguridad en la empresa

Ciberseguridad: medidas de protección a nivel de empresa

1. Software antivirus.

En cualquier caso, todos los computadores conectados a la red, personales y corporativos, deben contar con un antivirus gratuito y confiable. Este tipo de programas permite contar con medidas de protección efectivas ante la detección de malware u otros elementos maliciosos, por medio de ofrecer la posibilidad de eliminar las posibles amenazas o poner al dispositivo en estado de “cuarentena”.

Dentro del mercado, existen soluciones que integran diferentes funcionalidades adaptables a las necesidades de cada organización. Sin embargo, es importante que la que se adopte cuente con las actualizaciones pertinentes para así no quedar caducas ante nuevas amenazas.

Sistemas de seguridad en la empresa

Ciberseguridad: medidas de protección a nivel de empresa

2. Firewall perimetral de red.

Es una de las herramientas de ciberseguridad más recomendadas. Su funcionamiento es simple: escanea los paquetes de red, permitiéndolos o bloqueándolos según las reglas definidas por un administrador.

Si bien es cierto que su estructura es básica si se compara a la sofisticación de las amenazas, se pueden encontrar firewalls modernos que pueden clasificar los archivos utilizando varios parámetros. Así, se puede inspeccionar con eficiencia el tráfico web, identificar a usuarios, bloquear el acceso que no está autorizado, entre otras acciones.

3. Servidor proxy.

Un proxy es un dispositivo o programa informático que actúa como intermediario entre las conexiones del navegador e Internet, filtrando todos los paquetes entre ambos. Está catalogada como una de las buenas herramientas de seguridad informática debido a que, por medio de ella, se puede bloquear sitios web que se estimen como peligrosos o prohibidos dentro del ambiente laboral.

Por otro lado, permite establecer un sistema de autenticación, el cual limita el acceso a la red externa, permitiendo contar con registros sobre sitios, visitas, entre otros datos.

Sistemas de seguridad en la empresa

Ciberseguridad: medidas de protección a nivel de empresa

4. Cifrado de punto final o end point disk encryption.

Es un proceso de codificación de datos para que no pueda ser leído o utilizado por nadie que no tenga la clave de descifrado correcta. En esencia, protege los sistemas operativos de la instalación de archivos de arranque corruptos, bloqueando los archivos almacenados en computadores, servidores, entre otros puntos finales.

5. Escáner de vulnerabilidades.

Es una de las herramientas de seguridad en sistemas informáticos fundamentales en las empresas de cualquier tamaño. Consiste en un software que se encarga de detectar, analizar y gestionar los puntos débiles del sistema.

Gracias a esta plataforma, se puede mantener controlada la exposición de los recursos empresariales a las amenazas de ciberseguridad y sus posibles consecuencias. Además, permite alertar en tiempo real, lo que ayuda a la solución de problemas de forma oportuna y sin comprometer la continuidad del negocio.

Sistemas de seguridad en la empresa

Ciberseguridad: Los 7 errores al implementar un sistema de gestión de seguridad de la información.

Implementar en tiempos record. Sé que una de las razones por la cuál una organización decide implementar un sistema de gestión de seguridad de la información (En adelante **SGSI**) es por que algún cliente lo está pidiendo o en alguna licitación. Sin embargo, implementar un sistema de gestión en un mes o incluso en 3 meses, se corre el riesgo de que los objetivos del sistema sean endebles y no se perciba el valor real de la gestión.

Separar la operación del SGSI de la real de la organización. Existen algunas organizaciones que piensan que un SGSI es una obligación lejos de un beneficio y la decisión más fácil es mantener un SGSI con evidencia que no refleja la realidad de la empresa o el negocio, en ese momento el SGSI se vuelve un gasto en lugar de una inversión.

Sistemas de seguridad en la empresa

Ciberseguridad: Los 7 errores al implementar un sistema de gestión de seguridad de la información.

Certificar solo una parte de la organización. Aun que esta opción es totalmente valida y no es algo malo, ya que la misma norma te pedirá un alcance, puede también que exista un riesgo latente de caer en el punto anterior y tener dos operaciones (Una dentro del SGSI y otra sin gestión) Sin embargo, para evitar este error, se puede implementar todo el SGSI en la empresa, pero para la certificación limitar el alcance, de esa manera se evita el error número 2.

Sin apoyo de la alta dirección. Cuando se le asigna un presupuesto a la implementación del SGSI no es la única acción que deberá hacer la dirección. Si bien, la dirección no tiene por que participar en la operación del sistema, es de suma importancia que la dirección siempre dirija y asigne hacia donde quiere llegar con el sistema, **no solamente obtener la certificación.**

Sistemas de seguridad en la empresa

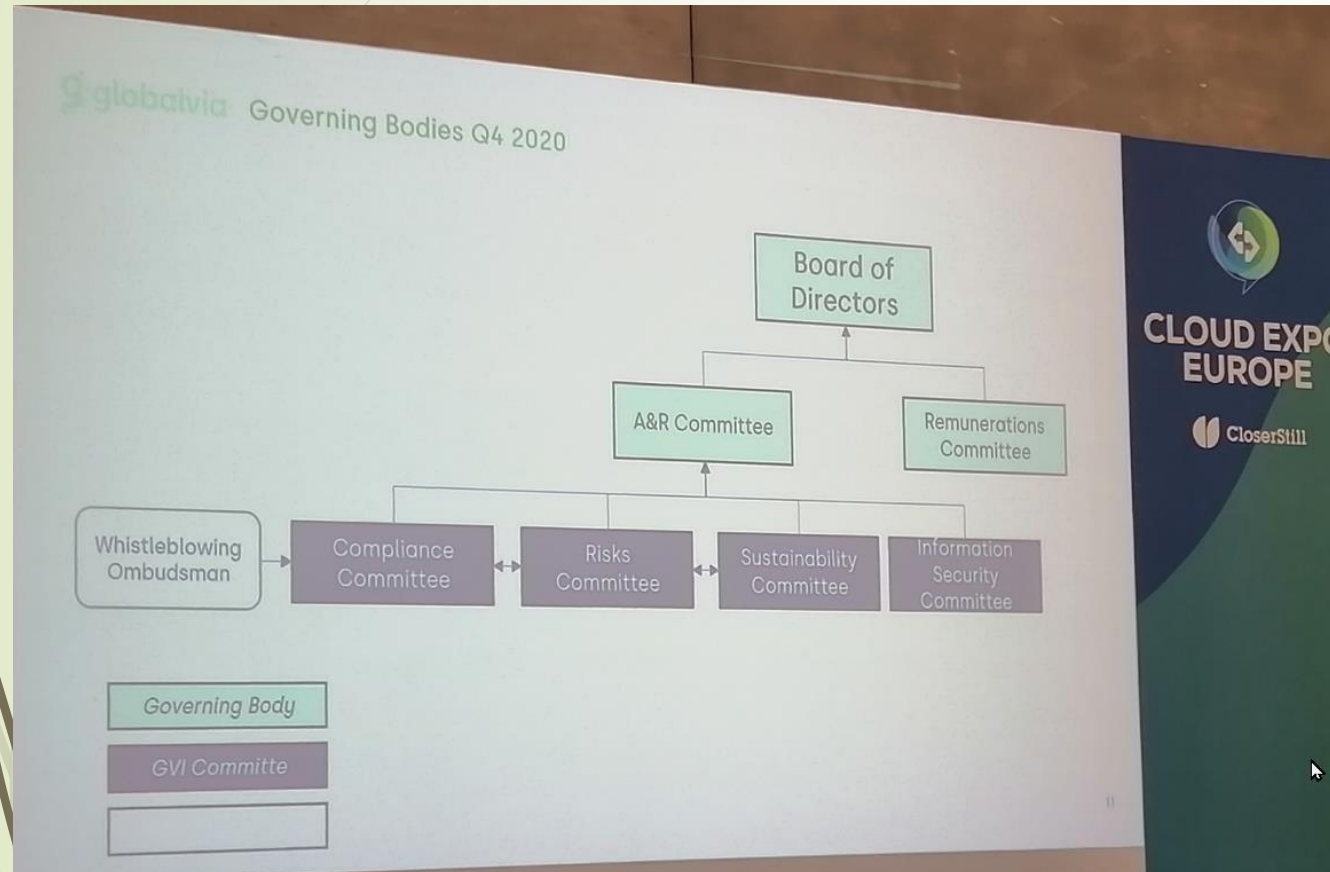
Ciberseguridad: Los 7 errores al implementar un sistema de gestión de seguridad de la información.

Olvidar el SGSI después de la implementación. O también operarlo un mes antes de la siguiente visita de los auditores. Un sistema gestión contempla la mejora continua no de manera intermitente si no continua. Es como si los directores tomaran acciones en la empresa cuando solo pasan cosas malas, cuando es así, la empresa nunca llegará a ser estable.

Utilizar formatos sin conciencia. Yo no veo mal el uso de formatos, incluso yo llevo años trabajando con los propios. Pero también es cierto que al no tener conciencia al llenado de estos formatos o la debida conciencia, se pueden cometer errores de operaciones que no reflejen la realidad de la empresa. **Es importante usar los formatos adaptándolos a la organización y no adaptar la organización a los formatos.**

Sistemas de seguridad en la empresa

Ciberseguridad: Los 7 errores al implementar un sistema de gestión de seguridad de la información.



Realizar un SGSI para la auditoria y no para la organización. Yo como auditor puedo confesar que a veces es muy notorio la elaboración de documentación para facilitarle el trabajo al auditor, o incluso operar el sistema de gestión solo para la auditoria. Aun que eso facilita nuestro trabajo, no crea ningún beneficio para el negocio. **Dile no a las observaciones que no le den un valor al SGSI.**

Sistemas de seguridad en la empresa

Como denunciar un ciberdelito

Realidad del hecho

- Recabar toda la información que puedas.
- Si es necesario acude a un profesional.



Si dudas de si es delito...

- INCIBE puede facilitar asistencia técnica (mitigación, asesoramiento)

Acudir a denunciar a GC

- Agentes especializados
- Experiencia
- Proximidad

GUARDIA CIVIL



Fundamentos de criptografía

INTRODUCCIÓN A LA CRIPTOGRAFÍA

Se entiende por criptología el estudio y práctica de los sistemas de cifrado destinados a ocultar el contenido de mensajes enviados entre dos partes: emisor y receptor. La criptografía es la parte de la criptología que estudia como cifrar efectivamente los mensajes.

Para establecer una comunicación de datos entre dos entidades (personas, equipos informáticos, etc) hacen falta al menos tres elementos básicos: el emisor del mensaje (la fuente), el receptor del mismo (el destino) y un soporte físico por el cual se transfieran los datos (el medio).

En una comunicación normal los datos se envían a través del medio tal como son, sin sufrir modificaciones de ningún tipo, de tal forma que el mensaje que representan puede ser interceptado y leído por cualquier otra entidad que acceda a él durante su viaje por el medio.

Pero hay ocasiones en las que nos interesa que dicho mensaje solamente pueda ser interpretado correctamente por el emisor del mismo y por el receptor al que va dirigido.

En estas ocasiones es necesario implementar algún mecanismo de protección de la información sensible tal que el mensaje viaje seguro desde la fuente al destino, siendo imposible la interceptación por terceros del mensaje, o que si se produce ésta, el mensaje capturado sea incomprensible para quien tenga acceso al mismo.

Fundamentos de criptografía

INTRODUCCIÓN A LA CRIPTOGRAFÍA



La criptografía (del griego oculta y escribir, literalmente escritura oculta) es el arte o ciencia de cifrar y descifrar información utilizando técnicas que hagan posible el intercambio de mensajes de manera segura que solo puedan ser leídos por las personas a quienes van dirigidos.

Los mecanismos de cifrado se utilizan principalmente para proporcionar el servicio de confidencialidad, aunque también pueden soportar otros servicios de seguridad como la integridad de datos y la autenticación.

La criptografía que nosotros conocemos y utilizamos, data de los años 70 aunque ya se utilizaban técnicas criptográficas en la segunda guerra mundial e incluso pueblos de la antigüedad como los griegos y romanos utilizaban mecanismos para enviar mensajes << cifrados >> en sus campañas militares.

Fundamentos de criptografía

INTRODUCCIÓN A LA CRIPTOGRAFÍA

Una de las formas de conseguir esto es enviar el mensaje en claro, tal como lo ha redactado el emisor, y protegerlo en el camino mediante sistemas de fuerza que lo defiendan durante el camino, como es el caso de la protección de mensajes mediante personal de seguridad. Otro método posible es el enviar el mensaje por un camino con tanto tráfico de información que resulte muy difícil a las terceras personas detectar que se trata de información confidencial (la mejor forma de ocultar un árbol es dentro de un bosque), como es el caso de enviar el mensaje mediante una carta por el sistema estándar de correo.

Desafortunadamente estos métodos de protección de mensajes, al igual que otros análogos, han demostrado su ineffectividad a lo largo de los tiempos, por lo que hubo que buscar otro tipo de mecanismos para proteger la información sensible en su camino entre emisor y receptor.

La criptografía ha demostrado con el tiempo ser una de las mejores técnicas para resolver esta cuestión. Tanto es así que actualmente, en la época de los ordenadores y la información, es el mecanismo más usado en los procesos de protección de datos, como las transacciones bancarias por Internet, el correo electrónico cifrado, etc.

Fundamentos de criptografía

INTRODUCCIÓN A LA CRIPTOGRAFÍA

Esto es así porque es tal vez el único medio asequible y fácil de implementar para lograr un acceso controlado a la información en un medio, Internet, que por su propia naturaleza es abierto y de acceso libre a la información. Tanta ha sido la importancia de los sistemas criptográficos que, por ejemplo, en la Segunda Guerra Mundial la famosa máquina alemana ENIGMA trajo en jaque durante mucho tiempo al ejército aliado, al permitir a los nazis el envío de información cifrada a sus tropas. Y en la actualidad los sistemas de cifrado están financiados en su mayoría por los gobiernos y sus militares, constituyendo el resultado de las investigaciones materia reservada.

Fundamentos de criptografía

OBJETIVOS DE LA CRIPTOGRAFÍA

La criptografía puede aplicarse en dos ámbitos de la seguridad informática: en el almacenamiento de información y en la transmisión de la misma. La criptografía es fundamental para la seguridad incluso en sistemas inseguros. Aunque se superen las barreras de seguridad física establecidas, e incluso las barreras de seguridad lógica para el control de accesos en el S.O, la criptografía permite mantener algunas de las características de la seguridad informática. Aunque no salvaguarda la integridad de los datos ante un posible borrado total o parcial de los mismos, si asegura su integridad en el sentido en que facilita la detección de cualquier tipo de modificación, incluido el añadido o borrado de información.

Fundamentos de criptografía

OBJETIVOS DE LA CRIPTOGRAFÍA

Obviamente y en primera instancia protege el secreto/confidencialidad de la información. Veamos ahora como se relaciona la criptografía con cada una de las características de la seguridad informática y como puede utilizarse para añadir algunas nuevas.

Pongamos foco en los términos siguientes:

- Secreto o confidencialidad
- Integridad y precisión
- Autenticación
- No repudio

Fundamentos de criptografía

OBJETIVOS DE LA CRIPTOGRAFÍA

Secreto o confidencialidad: Obviamente el cifrado de la información es un excelente método para proteger la confidencialidad de la misma. Aunque se acceda a la información, o se intercepte mientras se transfiere, si está cifrada sigue siendo inútil a menos que pueda descifrarse.

Integridad y precisión: Algunos sistemas criptográficos incorporan medios para prevenir que se dañe la integridad de la información, esto es, que ésta sea modificada voluntaria o involuntariamente. El sistema permite detectar cualquier pequeño cambio que se haya producido en el mensaje original.

No repudio: Es una característica más inusual que se relaciona con la transmisión de mensajes cifrados. Se trata de prevenir que la persona que envió el mensaje (el emisor) pueda alegar con posterioridad que él no envió ese mensaje (repudiarlo). El receptor debe disponer de mecanismos que demuestren ante terceros que sólo el emisor pudo enviar el mensaje.

Fundamentos de criptografía

OBJETIVOS DE LA CRIPTOGRAFÍA

Autenticación

La criptografía también puede usarse para asegurar la autenticidad de los mensajes. Esto es, asegurar que el mensaje ha sido enviado por quién se identifica como su emisor. Se trata pues de identificar sin posible error el origen de los mensajes.

En relación con la autenticación suelen utilizarse las denominadas firmas digitales. Se trata de añadir algún tipo de información en el mensaje o de utilizar de algún modo las claves para validar en destino el origen del mensaje.

En el ámbito de la transferencia de mensajes cifrados la autenticación está muy relacionado con la integridad, y en muchas ocasiones se usa este término incluyendo al segundo.

Fundamentos de criptografía

OBJETIVOS DE LA CRIPTOGRAFÍA

Autenticación

Así, la autenticación de mensajes influiría tres aspectos:

- Asegurar que el mensaje no ha sido alterado, ni maliciosa ni inintencionadamente, durante su transmisión. El mensaje llegó tal y como se envió. (integridad).
- Asegurar que el mensaje no es el reenvío de uno previamente emitido e interceptado. (no reenvío).
- Asegurar que el emisor es quién dice que es. (autenticidad).

De hecho la autenticación puede usarse en conjunción con el cifrado o en solitario:

- En solitario se trata de autenticar el texto en claro.
- En combinación se autentifica el texto cifrado.

Fundamentos de criptografía

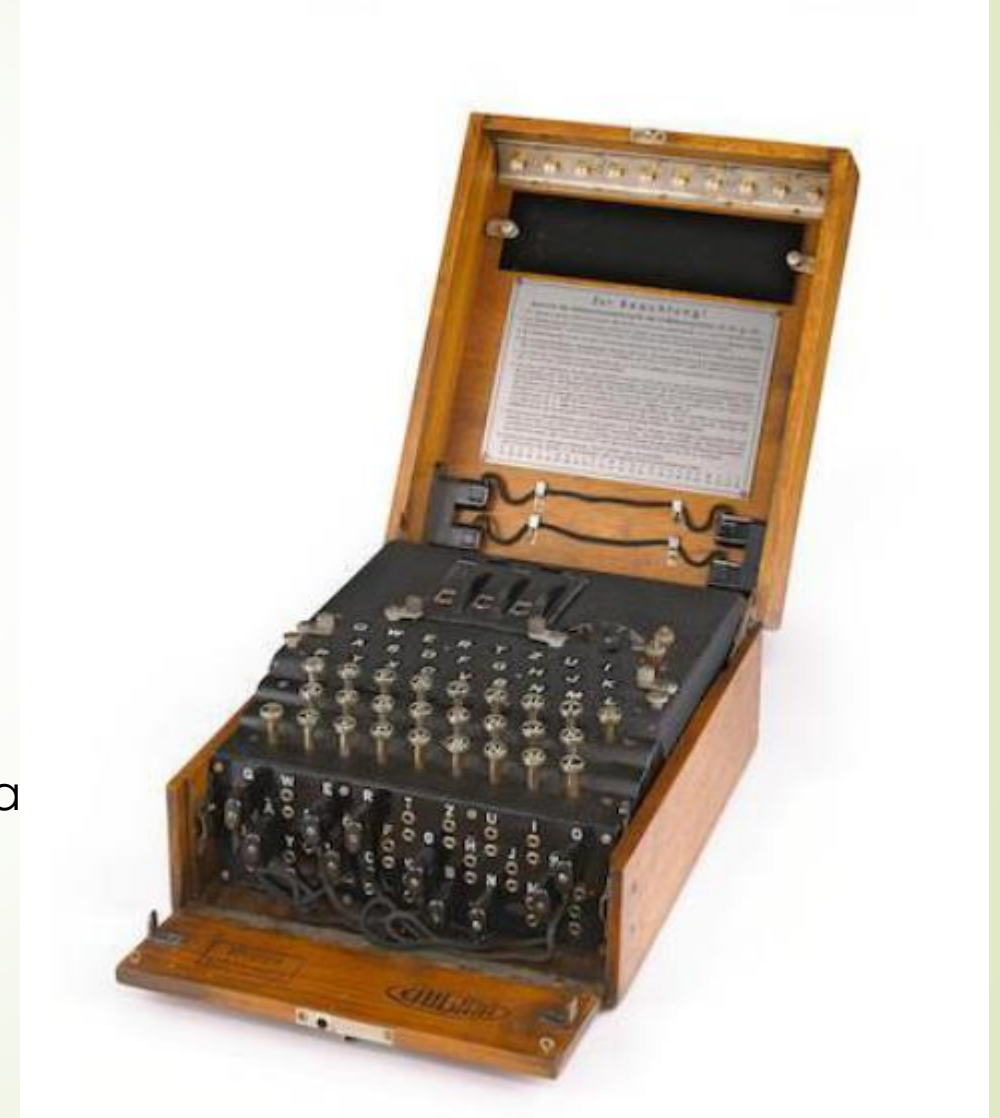
Historia de la criptografía

Orígenes de la Criptografía

- ❖ Los carteros en el Imperio romano
- ❖ La criptografía como cuestión de estado (II GM): NSA
- ❖ La máquina Enigma
- ❖ La criptografía vital para la privacidad humana
 - a) Información, libertad, privacidad y dinero anónimo
 - b) En un mundo cada vez más digitalizado

A partir de este momento se puede considerar que se comienzan a utilizar sistemáticamente los ordenadores para el cifrado de información y rotura de sistemas criptográficos. La criptología descansa sobre tres importantes campos teóricos:

- La teoría de la información
- La teoría de los números
- La teoría de la complejidad algorítmica.



Fundamentos de criptografía

Historia de la criptografía

Whitfield Diffie, Martin Hellman y Ralf Merkle (1976)

- ❖ “Code-breakers” (1967) de David Kahn
 - a) **Concepto de criptografía de clave pública (firmas digitales)**
 - b) y árboles de Merkle
 - c) Algoritmo Diffie-Hellman



Fundamentos de criptografía

Historia de la criptografía

❖ La ética del Hacker

- a) Acceso a los ordenadores y a todo lo que pueda enseñar alguna
- b) cosa sobre cómo funciona el mundo debe ser ilimitado y total
- c) Toda la información debe ser libre
- d) Desconfía de la Autoridad. Promueve la descentralización (y la no
- e) violencia)
- f) Los hackers deben ser juzgados por su hacking, no por sus títulos,
- g) edad, raza o posición
- h) Puedes crear arte y belleza en una computadora
- i) Las computadoras pueden cambiar tu vida para mejor

❖ The Mentor: *“La conciencia de un hacker”* (1986). *“Sí, soy un criminal. Mi crimen es la curiosidad”*

Fundamentos de criptografía

Historia de la criptografía

- ❖ Cypherpunks: Origen y motivaciones
 - a) Atkins, Graff, Leyland y Lenstra (1993): THE MAGIC WORDS ARE SQUEAMISH OSSIFRAGE
 - b) **Hal Finney, Adam Back** y el hackeo del navegador Netscape: encriptación de 40-bit internacional frente a los 128-bit en EE.UU (1993)



Fundamentos de criptografía

Historia de la criptografía

Destacaré tan solo que la seguridad de los sistemas criptográficos descansa sobre dos conceptos fundamentales, como son la difusión y la confusión.

El propósito de la difusión de la información es distribuir las propiedades estadísticas de los mensajes en claro, sobre todo el texto cifrado. Esto se puede conseguir de varias formas, por ejemplo:

- Haciendo que se altere la posición de los caracteres mediante cifrados por transposición.
- Haciendo que cada carácter del texto cifrado dependa de tantos caracteres del mensaje como sea posible.

El propósito de la confusión es establecer una relación lo más compleja posible entre la clave y el texto cifrado. De este modo, un criptoanalista no podrá deducir información acerca de la clave mediante un estudio del texto cifrado. Esta propiedad puede conseguirse por ejemplo mediante la aplicación de sustituciones.

Ambas técnicas, la difusión y la confusión, por separado, proporcionan fortaleza a los criptosistemas, **sin embargo utilizadas conjuntamente pueden dar lugar a sistemas muy difíciles de atacar.**

Fundamentos de criptografía

Tipos de ataques criptográficos

Existen tres técnicas fundamentales utilizadas por los criptoanalistas para atacar un criptosistema, aunque casi siempre se utilizan combinaciones de ellas. En general las modernas técnicas de criptoanálisis suponen unos conocimientos matemáticos avanzados y utilizan mecanismos estadísticos, software y hardware muy sofisticados y en ocasiones muy caros.

- Ataque a partir sólo del texto cifrado.
- Ataque a partir de algún mensaje conocido
- Ataque por elección de mensaje.

Un ejemplo de este tipo de ataque es el ataque mediante diccionario a las contraseñas cifradas de un sistema UNIX. El criptoanalista dispone de los textos cifrados y cifra toda una serie de textos en claro hasta encontrar uno que coincida con alguno de los cifrados.

Fundamentos de criptografía

Tipos de funciones criptográficas: SISTEMAS DE CIFRADO CLÁSICOS

Criptosistemas clásicos

Podemos considerar como criptosistemas clásicos aquellos que son anteriores al uso sistemático de los ordenadores en el campo de la criptografía.

Sus características fundamentales son su simplicidad y la facilidad para recordar los algoritmos y la clave. Dado que se aplicaban en el ámbito militar los mensajes tenían que poder cifrarse y descifrarse de modo rápido y sencillo. y el método utilizado debía ser fácil de recordar.

Cifrados por transposición (o permutación)

Se reordenan los bits, caracteres o bloques de caracteres del texto en claro para obtener el texto cifrado.

El ejemplo más sencillo de este tipo de sistema es el método de transposición simple, en el que se cambian las posiciones de las letras en bloques sucesivos de texto.

Cuando este sistema se aplica en ordenadores, el dispositivo encargado de permutar cada bloque de texto suele denominarse P-box (Permutation box).

Cifrados por sustitución.

Se reemplazan bits, caracteres o bloques de caracteres del texto en claro por otros en el texto cifrado.

La versión más sencilla de este tipo de método es el denominado cifrado por sustitución simple o monoalfabeto. En este sistema cada carácter del texto en claro es siempre sustituido por un mismo carácter en el texto cifrado.

Fundamentos de criptografía

Tipos de funciones criptográficas: SISTEMAS DE CIFRADO CLÁSICOS

Cifrados por transposición (o permutación)

Otro ejemplo de este sistema es el denominado de transposición por columnas. En este se dispone el texto por filas de una determinada longitud, rellenándose el final de la última fila con un carácter cualquiera. El texto cifrado se obtiene leyendo la matriz resultante por columnas. La clave de descifrado es simplemente el número de columnas utilizado.

EN UN LUGAR DE LA MANCHA

E	N	U
N	L	U
G	A	R
D	E	L
A	M	A
N	C	H
A	X	X

ENG DAN AN LA EM CX U URL AHX

Cifrados por sustitución.

Un caso especial de sustitución simple es el cifrado Cesar, en el que como ya vimos cada carácter es sustituido por el situado 3 posiciones por delante en el alfabeto.

EN UN LUGAR DE LA MANCHA

A B C D E F G H I J K L M N Ñ O P Q R S T U V W X Y Z

D E F G H I J K L M N Ñ O P Q R S T U V W X Y Z A B C

¿Cuál es el resultado?

Fundamentos de criptografía

Tipos de funciones criptográficas: SISTEMAS DE CIFRADO CLÁSICOS

Cifrados por sustitución.

Otra modalidad de sistema por sustitución es el cifrado por sustitución polialfabeto. En este, cada carácter del texto en claro es sustituido por un carácter distinto en el texto cifrado cada vez que aparece. En la práctica se utiliza un número limitado de alfabetos de modo que cada vez que aparece el carácter en el texto en claro se usa cíclicamente uno de los alfabetos.

La máquina Enigma utilizaba un sistema de sustitución polialfabeto para cifrar los textos.

Un ejemplo de sistema de cifrado polialfabeto es el Método de Vigenére. En este sistema se utiliza como clave una palabra cuyas letras definen el desplazamiento de los distintos alfabetos a usar.

Supongamos que utilizamos como palabra clave SOL

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z
alf. 1	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	Ñ	O	P	Q	R
alf. 2	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	Ñ
alf. 3	L	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K

Mensaje **P L A N T A A T O M I C A**

Clave **S O L S O L S O L S O L S**

¿Cuál es el resultado?

Fundamentos de criptografía

Tipos de funciones criptográficas: SISTEMAS DE CIFRADO CLÁSICOS

Summerside Makerspace

A shared workspace where people gather to make, teach and learn

[Home](#) [About](#) [Our Sponsors](#) [The Space](#) [Projects](#) [Events](#) [Join](#) [FAQs](#) [News](#)

Universal Enigma Machine Simulator

Enigma Machine Version: Enigma M4 (Navy)

Stepping: Ratchets

Plugboard Available: Yes

Plugboard Uhr: No

Reflector

D

A

Thin Rotor

3

A

A

Slow Rotor

I

Ring

A

A

Middle Rotor

II

Ring

A

B

Fast Rotor

III

Ring

A

B

Plugboard

A

B

C

D

E

F

G

H

I

J

K

L

M

N

O

P

Q

R

S

T

U

V

W

X

Y

Z

Entry Wheel

D → B

A

B

C

D

E

F

G

H

I

J

K

L

M

N

O

P

Q

R

S

T

U

V

W

X

Y

Z

Your message text here

Cipher One Letter

Cipher All


Play

x2

x10

PLWFXB

Clear Ciphertext



Summerside Makerspace Website is licensed under a [Creative Commons Attribution 4.0 International License](#).

Fundamentos de criptografía

Tipos de funciones criptográficas: SISTEMAS DE MODERNOS

Los sistemas criptográficos modernos se desarrollan con la aparición de los ordenadores, y basan su funcionamiento en la utilización de potentes y complejas herramientas hardware y software. Su funcionamiento no se basa en simples sustituciones o transposiciones. En lugar de ello, se utilizan claves secretas de gran longitud para controlar una compleja secuencia de operaciones con la información que pueden incluir tanto transposiciones como sustituciones. Su posibilidad de uso se basa en la potencia de los ordenadores, que permiten aplicar algoritmos de gran complejidad y coste en tiempos admisibles.

Los criptosistemas modernos pueden dividirse en dos grandes categorías en función del tipo y número de claves que utilizan:

- **Criptosistemas simétricos**, también llamados de clave única o de clave privada.
- **Criptosistemas asimétricos**, también llamados de clave pública o de dos claves.

Ambos sistemas tienen características bien diferenciadas, lo que define su uso para diferentes fines. De hecho ambos tipos de sistemas suelen combinarse para llevar a cabo distintas acciones y lograr ciertos objetivos de seguridad.

Además existe algún sistema adicional que no encaja bien en ninguna de las dos categorías anteriores, como es el denominado criptosistema one-time pad.

Fundamentos de criptografía

Tipos de funciones criptográficas: SISTEMAS DE MODERNOS

Criptosistemas de clave privada()*

En estos sistemas se utiliza la misma clave para el cifrado y para el descifrado. Esta clave se denomina clave privada (secreta o única) debido a que tan solo es conocida por el emisor y por el receptor del mensaje. Para que este tipo de sistema sea efectivo la clave debe ser mantenida en secreto por ambas componentes de la comunicación.

La seguridad de este tipo de sistemas depende totalmente del nivel de protección de la clave.

Un ejemplo clásico de criptosistema de clave privada es el DES (Data Encryption Standard) que describiremos con mayor detalle en un apartado posterior.

En este tipo de sistemas, el secreto (confidencialidad) y la autenticidad se obtienen al mismo tiempo.

Cuando se descifra un mensaje usando la clave privada, el hecho de que ésta sea tan solo conocida por el emisor y el receptor garantiza dos propiedades:

1. Que el mensaje no es inteligible por nadie más, es decir, que es confidencial.
2. Que si el texto descifrado es inteligible, sólo hay un emisor posible, aquel que conoce la clave privada. Esto garantiza la autenticidad del mensaje.



Fundamentos de criptografía

Tipos de funciones criptográficas: SISTEMAS DE MODERNOS

Modos de operación básica

- Cifrado en bloques:** La información a cifrar se divide en bloques de longitud fija, por ejemplo 64 o 128 bits, y luego se aplica el algoritmo de cifrado a cada bloque utilizando una clave secreta. Utiliza combinaciones complejas basadas en sustituciones y cambios de posición que se regirán por la clave de cifrado. Ejemplos: DES, 3DES, AES.

- Cifrado de flujo:** Son algoritmos que pueden realizar el cifrado incrementalmente, convirtiendo el texto en claro en texto cifrado bit a bit. El cifrado de flujo se utiliza mucho en las telecomunicaciones. Por ejemplo, en una conversación de telefonía móvil la voz se digitaliza (es decir, se convierte a un flujo de bits) y se envía cifrada por la red de comunicaciones. Con el fin de no entorpecer la conversación, el proceso de cifrado debería ser lo bastante rápido como para no añadir retraso a la comunicación. Por ello, conviene que la operación de cifrado sea rápida. Ejemplo: RC4.



Fundamentos de criptografía

Tipos de funciones criptográficas: SISTEMAS DE MODERNOS

Criptosistemas de clave pública.

En este tipo de sistemas se utilizan dos claves: una clave pública y una clave privada. En un grupo de usuarios, cada uno de ellos posee dos claves distintas:

- o La clave pública, K' , como su propio nombre indica, puede ser conocida por todos los usuarios del sistema.
- o La clave privada, K , tan solo es conocida por su propietario.

Aunque estas claves están relacionadas matemáticamente, la fortaleza del sistema depende de la imposibilidad computacional de obtener una a partir de la otra.

Este tipo de sistemas se denominan asimétricos porque no podemos usar una misma clave para cifrar y descifrar un mensaje. Ambas claves deben usarse en el proceso. Si ciframos un mensaje con una de ellas, debemos descifrarlo con la otra.

¿Cómo usar ambas claves para obtener un sistema seguro?

Si un usuario (emisor) quiere enviar un mensaje secreto a otro (receptor), debe cifrarlo utilizando la clave pública del receptor.

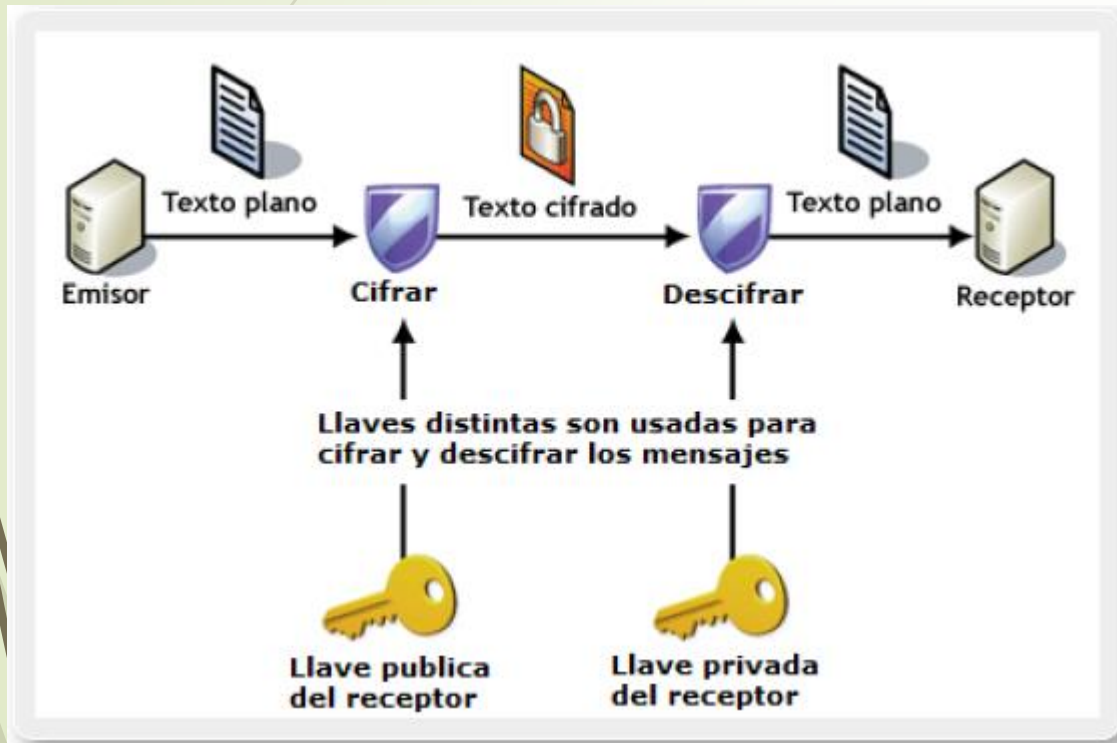
El mensaje tan solo puede descifrarse utilizando la clave privada del receptor, con lo que se garantiza la confidencialidad del mismo. La clave pública del receptor no sirve para descifrar el mensaje, y por tanto tan solo el receptor (que es el único que conoce su propia clave privada), puede descifrarlo.

Fundamentos de criptografía

Tipos de funciones criptográficas: SISTEMAS DE MODERNOS

Criptosistemas de clave pública.

Veamos el esquema



El proceso se describe a continuación:

- 1) Cada usuario genera un par de claves: la pública y la privada.
- 2) Cada usuario deposita su clave pública en un lugar accesible.
- 3) Si el usuario B quiere comunicarse con A usa la clave pública de éste.
- 4) Cuando A recibe un mensaje cifrado de B lo descifra usando su clave privada.

Fundamentos de criptografía

Prácticas con ssh y linux

<https://hub.packtpub.com/making-simple-web-based-ssh-client-using-nodejs-and-socketio/>

<https://askubuntu.com/questions/346857/how-do-i-force-ssh-to-only-allow-users-with-a-key-to-log-in/346863#346863>

<https://lani78.com/2008/08/08/generate-a-ssh-key-and-disable-password-authentication-on-ubuntu-server/>

Referencias

- <https://cerounosoftware.com.mx/2016/08/17/7-conceptos-b%C3%A1sicos-de-seguridad-inform%C3%A1tica/>
- <https://jorgegarciaherrero.com/que-es-una-brecha-de-seguridad-7-ejemplos/>
- <https://www.businessinsider.es/11-mayores-hackeos-brechas-seguridad-decada-pasada-843097>
- <https://www.viafirma.com/blog-xnoccio/es/tipos-de-firma-electronica-desde-movil/>
- <https://www.xolido.com/lang/xolidosign/modulo/faq-xolidosign-desktop/desktop-faq/441/>
- <http://openaccess.uoc.edu/webapps/o2/bitstream/10609/95806/2/gmorenopeTFM0619.pdf>
- <https://www.axpe-blogs.com/uncategorized/diferencias-entre-certificado-electronico-firma-digital-y-firma-electronica/>
- <https://naps.com.mx/blog/que-es-un-certificado-digital-en-que-es-diferente-de-una-firma-digital/>
- http://sededocumentacion.unizar.es/curso/certificado_firma_sede_tramitacion.pdf
- https://virtual.itca.edu.sv/Mediadores/cms/u61_concepto_de_criptografa.html
- <https://www.slideserve.com/erol/sistema-de-autenticaci-n-y-autorizaci-n>
- <https://www.evidian.com/pdf/wp-strongauth-es.pdf>
- <https://www.iniseg.es/blog/ciberseguridad/tipologias-de-hacker-whitegrayblack-hat-hacker/>
- <https://www.infosecuritymexico.com/es/blog/herramientas-de-ciberseguridad-para-proteger-tu-empresa.html>



Lecturas recomendadas

- El huevo del CUCO
- Guía de ciberataques, documento creado por INCIBE y al servicio de la Oficina de Seguridad del Internauta (OSI) y sus sitios web: <https://www.incibe.es> y <https://www.osi.es>