



INICIO GRABACIÓN



SANJOSÉ
FUNDACIÓN DE EDUCACIÓN SUPERIOR



OBJETIVOS

- Conocer las **principales amenazas** que pueden afectar a mi negocio. Identificar a los distintos **actores** que realizan ciberataques:
 - Clasificación
 - Cuáles son sus objetivos
 - Cuáles son sus motivaciones
- Distinguir y **prevenir los ataques internos**.
- Fomentar la **formación y concienciación** a empleados.

Los virus informáticos



- Unos de los primeros conceptos cuando se habla de seguridad informática, es el de virus informático. Las computadoras solo entienden código binario como ceros y unos, en el mundo de las computadoras y de la informática existen muchos conceptos como el de programas, videojuegos, sistemas operativos y cualquier clase de software.

El software es uno de los conceptos más abstractos, se lo define como todo lo intangible de la computadora, son instrucciones que el ordenador espera que se realicen, las cuales pueden ser instrucciones complejas o instrucciones sencillas.

Según Beynon-Davies, el término software o programa es utilizado para describir una secuencia de varias instrucciones que es leído por un computador, los cuales son escritos en un determinado lenguaje de programación que pueden ser clasificados de la siguiente manera:

- Lenguaje de máquina
- Lenguaje ensamblador
- Lenguajes de alto nivel

Las amenazas son elementos que pueden provocar **alteraciones, daños o fugas de información** de la organización ocasionando pérdidas materiales, económicas y de prestigio.

También se define como la **causa potencial de un incidente no deseado**, el cual puede ocasionar daño a un sistema o a una organización [UNE-ISO/IEC 27000:2014].






Los virus informáticos



Analizado el tema clave sobre el software, un virus informático es un programa que tiene como objetivo dañar o cambiar el funcionamiento de la computadora. Esta es una definición bastante clara, pero el virus informático no siempre tiene que ser un programa completo, puede ser hasta cierto punto fragmentos de un programa. Se define al virus informático, como un programa desarrollado en un determinado lenguaje de programación (C++, C, ensamblador, etc.) con el objetivo de infectar uno o varios sistemas informáticos, utilizando varios mecanismos de propagación o autoreplicación, el cual trata de reproducirse de forma acelerada para extender su alcance.

existen varios tipos de virus que se los puede definir de la siguiente manera:

- Virus de sector de arranque (BOOT)
 - Virus de archivos ejecutables
 - Virus de macros
 - Virus de lenguajes de Script
 - Malware
 - Gusanos
 - Troyanos
 - Spyware
 - Keyloggers
 - Adwares
 - Dialers
 - Backdoors
 - Otros
 - Rootkits
 - Bacterias
 - Bombas de tiempo
- 



MALWARE

También llamado código malicioso; incluye virus, gusanos, troyanos, etc.



EXPLOIT

Es un programa que aprovecha una vulnerabilidad de un sistema informático para robar datos o contraseñas de los usuarios, espiar la actividad de los mismos, controlar o modificar la configuración del equipo, entre otros.



ATAQUES DE DENEGACIÓN DE SERVICIO (DOS)

Se entiende como denegación de servicio a un conjunto de técnicas cuyo objetivo es inutilizar un servidor (por ejemplo la web de una empresa).

Un ataque de Denegación de Servicio Distribuido (DDoS) es más sofisticado y permite enviar peticiones coordinadas entre distintos equipos a un mismo servidor para inutilizarlo o «tirarlo».



PHISHING

Este tipo de ataque se realiza comúnmente a través de correos electrónicos (e-mail) donde se intenta convencer a un usuario para que confíe en el contenido del email, con la intención de obtener información (por ejemplo contraseñas o claves de acceso). Este tipo de ataques también puede realizarse a través de WhatsApp, servicios de mensajería, etc.



APT Amenaza persistente avanzada

Amenazas complejas avanzadas y persistentes, a través de ataques coordinados dirigidos a una entidad u organización específica.

El **Malware**, también llamado código malicioso, es el software diseñado para tener **acceso a los sistemas informáticos específicos, robar información o interrumpir las operaciones del ordenador**. Erróneamente se conocen como virus informáticos, pero realmente los virus son un tipo de malware. Hay otros tipos de malware: como los gusanos y los caballos de Troya, que se diferencian por la forma en que operan o se propagan.



VIRUS



Es un código de software que puede replicarse y propagarse de un ordenador a otro.



GUSANOS



Variante del virus pero es auto-replicante, diseñado para propagarse a través de redes informáticas.



TROYANOS



Malware que obtiene acceso a un sistema que se suele «esconder» dentro de una aplicación real.



El objetivo de estas amenazas es llegar a la mayor cantidad de personas posibles.

también se aprovechan de los anuncios en aplicaciones para móviles. Otras vías de contagio son:

- dispositivos infectados (USB, DVD,...)
- sitios web fraudulentos (que suplantan a tiendas o bancos) o sitios web legítimos pero infectados
- enlaces a sitios comprometidos en correos masivos o por mensajería instantánea
- redes sociales
- programas de compartición de ficheros (P2P)
- software gratuito



BOTNETS

Una botnet (un término derivado de «robot» y «red (net)») es una red, automatizada y distribuida de ordenadores previamente comprometidos (infectados) que, controlados remotamente, realizan acciones maliciosas de forma simultánea, como el envío de *spam* o ataques de denegación de servicio distribuido (DDoS).



Un **exploit** es un programa que aprovecha una vulnerabilidad de un sistema informático en beneficio propio. Los llamados exploit de día-cero (zero-day) son aquellos que todavía no se han hecho públicos y, por tanto, no disponen de soluciones de seguridad que eviten la vulnerabilidad.

Actualmente, se ha desarrollado un mercado negro de exploits capaz de mover cada año enormes sumas de dinero.



Phishing



- ♦ Método de ataque que busca obtener información personal o confidencial de los usuarios a través de medios electrónicos (email, WhatsApp, mensajería instantánea, etc.) donde se intenta convencer a un usuario de que el autor es auténtico, pero con la intención de obtener información confidencial.
- ♦ Los mensajes de *phishing* han mejorado notablemente, cada vez son más sofisticados y personalizados. Lo más novedoso de este tipo de ataques es el uso combinado del correo electrónico y del teléfono. Se usa este engaño (llamado ingeniería social) para obtener información que de otra forma no daríamos.



Ataques DoS y DDoS

- ♦ Se entiende como Denegación de Servicio (DoS) a un conjunto de técnicas que tienen por objetivo dejar un **servidor inoperativo**. El ataque consiste en saturar con miles de peticiones de servicio al servidor, hasta que éste no puede atenderlas, provocando su colapso.
- ♦ Un método mas sofisticado es el Ataque de Denegación de Servicio Distribuido (DDoS), mediante el cual miles de peticiones son enviadas, de forma coordinada desde varios equipos (pertenecientes a una *botnet*), que están siendo utilizados para este fin sin el conocimiento de sus legítimos dueños.





Spear Phishing



- ♦ El *spear phishing* es otra de las modalidades utilizadas para realizar este tipo de ataques. El atacante redacta el correo electrónico utilizando información obtenida del contexto de la víctima (en muchos casos de las redes sociales) para dar mayor verosimilitud al email, incluyendo un enlace a contenidos de carácter malicioso dirigido a dañar los sistemas de la víctima. Las garantías de éxito son, por tanto, muy elevadas.

De: alertas@helpdesk.facebook.org
Para: xxxxxx@gmail.com
Asunto: Actualización cuenta de Facebook

Asunto con procedencia de la compañía : por ejemplo una red social

Estimado Juan,

Personalizado al nombre del usuario

Como parte de las actividades de seguridad del equipo de Facebook se realiza un revisión de conexiones de nuestros usuarios a sus perfiles.

Nuestro sistema ha detectado una actividad inusual en tu perfil de Facebook y en concreto en el uso de tus fotos. Es necesario que rellenes el siguiente formulario a través del siguiente enlace para poder aplicar la normativa vigente en materia de Propiedad intelectual y Copyrights de los contenidos de tu perfil.

http://www.systemadmin.facebook.org/formulario_copyright

Incluye un link muy dudoso

Nota: en caso de no proceder a rellenar el formulario facebook no se hace responsable del uso de contenidos de tu perfil y en caso que se siga detectando actividad inusual procederá a bloquear la cuenta.

Consecuencias en caso de no seguir las instrucciones

Gracias por su atención

Facebook – Help Desk

Firma de un departamento de compañía



ACTORES

Los agentes que ejecutan los ataques se pueden clasificar en función de sus motivaciones: amistosos (cuyo objetivo es detectar fallos de seguridad para anticiparse) o malintencionados (que tienen fines lucrativos o políticos generalmente).

CIBERAGENTES



AMISTOSOS

Agentes del orden

Agencias de seguridad

Hackers «éticos»

Investigadores

MALINTENCIONADOS

Cibervándalos

Ciberactivistas

Exempleados

Estados

Corporaciones /empresas

Ciberterroristas

Cibercriminales

Es importante conocer a los actores ya que sus acciones pueden perjudicar tu negocio. Conociéndolos puedes anticiparte a ellos y adoptar medidas adecuadas para proteger tu negocio. Estos son algunos:

Cibervándalos y script kiddies

Se denomina cibervándalos a aquellos individuos que, poseyendo conocimientos técnicos, llevan a cabo sus acciones con el único motivo de demostrar públicamente que son capaces de hacerlo.

Ciberactivistas o Hacktivistas

Sus acciones responden a motivos ideológicos. Un grupo muy conocido es *Anonymous*.

Actores internos (insiders)

Personas que tienen o han tenido algún tipo de relación con la organización, incluyendo exempleados, personal temporal o proveedores.

Su motivación suele ser siempre similar: venganza, motivos financieros o políticos, etc. o simplemente pueden realizar acciones maliciosas por desconocimiento.

Ciberinvestigadores

Personas que persiguen el descubrimiento de las vulnerabilidades que pueden afectar a los sistemas (hardware o software).

La publicación de los resultados de sus investigaciones (al objeto de sensibilizar sobre las necesarias medidas de seguridad) puede suponer que se use por terceros malintencionados.

Las organizaciones privadas

Movidas por el interés económico que supone poseer los conocimientos que tiene la competencia, desarrollan acciones de ciberespionaje industrial.



Actor	Motivaciones	Nivel de conocimientos	Objetivos
Actores internos (insiders)	Venganza, o beneficios económicos o ideológicos (en ocasiones, dirigida desde el exterior)	Alto / Medio / Bajo	Entorno de trabajo, actual y/o anterior.
Organizaciones privadas	Obtener o vender información valiosa	Alto / Medio / Bajo	Competidores, clientes, público en general.
Ciberdelincuentes	Beneficio económico (directo o indirecto)	Alto / Medio	Ofrecer productos y servicios con muchos detalles sobre datos de identidad o financieros. Básicamente, cualquiera puede ser un objetivo, si puede obtenerse beneficio económico.



MALINTENCIONADOS

Los **usuarios internos malintencionados** son el tipo menos frecuente, pero tienen el potencial de ocasionar daños considerables por su capacidad de acceso interno.

Pueden ser empleados descontentos o despedidos cuyas credenciales no se han eliminado y si tenían permisos como administradores con privilegios, pueden provocar situaciones de riesgo más elevadas.



ENGÑADOS

Los **usuarios internos** pueden ser «**engañados**» por terceros (ciberdelincuentes) para proporcionar datos o contraseñas que no deberían compartir.



DESCUIDADOS

Un **usuario interno descuidado** puede simplemente presionar la tecla equivocada y borrar o modificar información esencial de manera no intencionada.



TIPOS DE AMENAZAS POR AGENTES INTERNOS




Los usuarios internos con falta de formación son el origen de algunas brechas de seguridad que son fácilmente evitables con la debida concienciación en ciberseguridad. Piensa que por mucha inversión que uno pueda hacer en tecnología, los usuarios son los que en último término manejan la información.

Por otro lado, los empleados que han salido de la empresa de forma poco amistosa o que estén descontentos con su situación laboral pueden realizar ataques o causar daños en el negocio de forma intencionada.

Y por último, no siempre es culpa del empleado, sino que se producen a causa de la inexistencia de políticas y procedimientos o bien por que éstos no se han aplicado bien.

Es el caso de cuentas de acceso de empleados que dejan la empresas y no se eliminan; o cuando no se tiene una buena gestión de los accesos a la información sensible de nuestro negocio (financiera o datos personales de clientes, proveedores o colaboradores).





El empleado es la pieza clave en la ciberseguridad

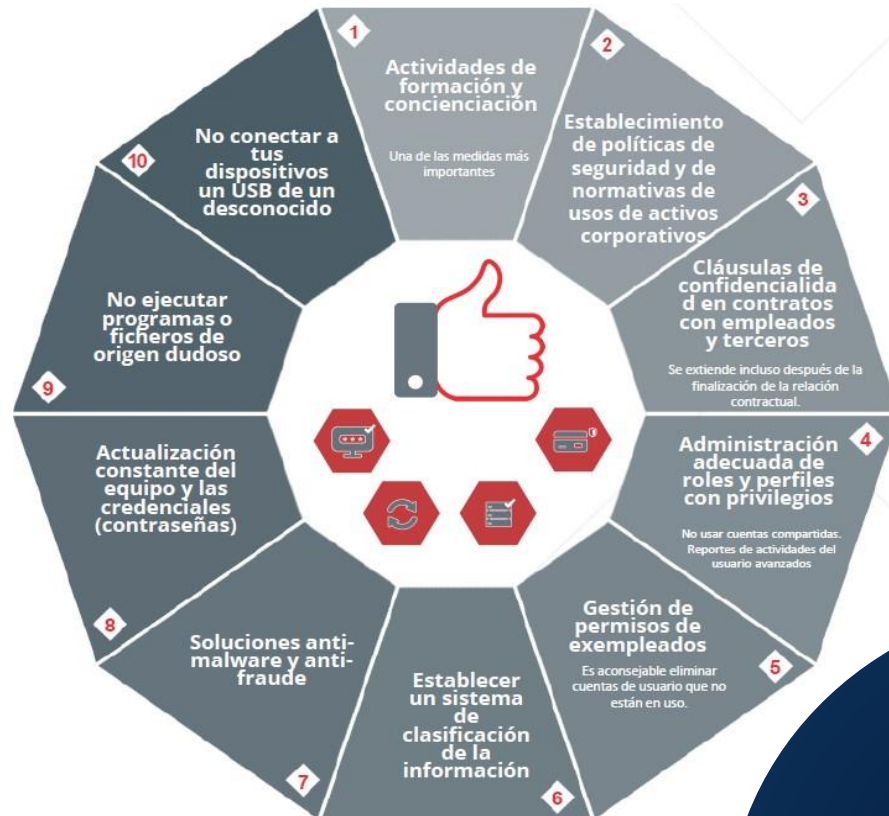


- ◊ Podemos implantar medidas de seguridad más o menos complejas, pero al final el empleado es el que trata con la información.
- ◊ Podemos aplicar todo tipo de políticas y normativas, pero es el empleado el que debe aplicarlas.
- ◊ El acceso a la información por parte de empleados es necesario y tanto intencionada como no intencionadamente, se pueden producir situaciones de riesgo.

Por eso es absolutamente imprescindible formar a los empleados en buenas prácticas de ciberseguridad.



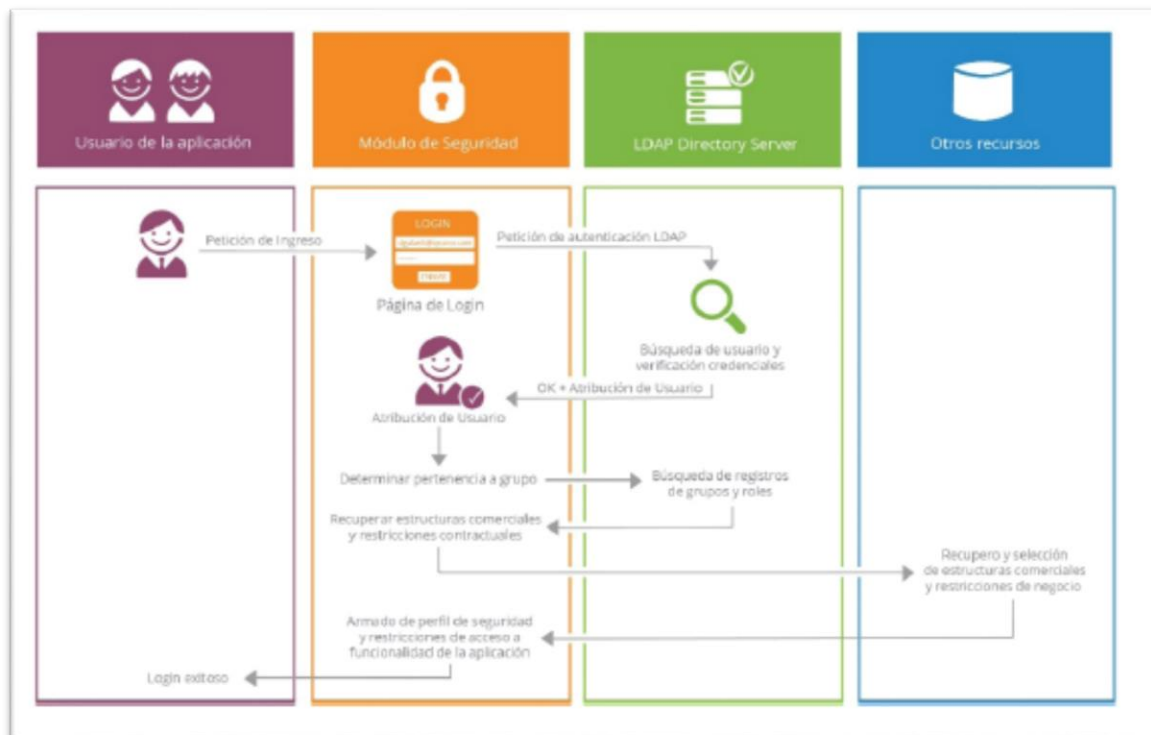
ACCIONES PARA MITIGAR EL RIESGO



Concepto de autenticación



La autenticación se puede definir como un proceso en el que se busca confirmar algo como verdadero, no se busca verificar un usuario, ya que la autenticación no siempre está relacionada con estos, en muchos casos se quiere saber si un cambio o un dato es correcto, no se debe cometer el error en pensar que solamente las personas necesitan este proceso, este puede ser para cualquiera, un sistema, un dispositivo o una persona.



Concepto de autenticación



Se tiene también los tipos de autenticación basados en una característica física, este tipo en comparación con lo que ya se mencionó se puede decir que son los más nuevos. Cuando se habla de características físicas se puede mencionar a:

- La voz
- Las huellas dactilares
- El ojo
- La escritura



Concepto de autenticación



La autenticación se puede considerar como parte de un método de control de acceso, la mayoría de las ocasiones esto se complementa con otras partes de un sistema, ya que hoy en día debido al manejo de la información y la personalización de los gadgets que se tiene disponibles, se vuelve una labor compleja la de tener control y manejo dentro del sistema.

Los tipos de autenticación no son excluyentes, así que, si se usa un método, no es una barrera para usar otro, de hecho, en sistemas complejos el usuario se puede encontrar con sistemas que utilizan tres tipos de autenticación, obviamente se tiene que pensar en el usuario,





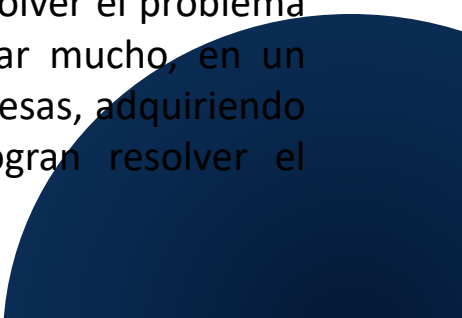
Mecanismos preventivos en seguridad informática

Los mecanismos preventivos en la seguridad informática son los más olvidados, los cuales son vistos como una pérdida de tiempo, la parte administrativa en la mayoría de los casos lo ve como un costo extra, es algo parecido como por ejemplo, con los seguros médicos o seguros de vehículos, se puede pagar 10 años el seguro de un carro y nunca tener un accidente, en primera instancia se podrá analizar que es algo muy bueno, pero después en algún momento se podrá pensar que es un desperdicio haber pagado una cantidad 10 años y sin usarla.

- Actualización de sistemas
- Antivirus
- Firewall
- Navegación por internet
- Contraseñas
- Accesos remotos.

Mecanismos correctivos en seguridad informática

Los mecanismos correctivos tienen una gran diferencia en tiempo con los mecanismos preventivos, estos se aplican cuando, después de que algo sucedió y la función principal es corregir las consecuencias. Entre las características que tienen los mecanismos correctivos normalmente son muy caros, esto se debe a que el problema ya se lo tiene encima y no se puede tenerlo durante mucho tiempo, así que, contratar expertos para resolver el problema o el tiempo que le dedicara a el equipo de trabajo siempre va a costar mucho, en un porcentaje muy alto se acaban pagando servicios de solución a otras empresas, adquiriendo soluciones o comprando software y parches de actualización que logran resolver el problema.





Encriptación en seguridad informática

La encriptación o también conocido como cifrado, es un procedimiento en el que se busca que la información sea ilegible, ya aplicado este procedimiento la información es inservible para cualquier persona que no sea la autorizada, aunque el mensaje sea interceptado, como en muchos casos la información simplemente no significa nada para el interceptor, ya que no cuenta con los elementos involucrados en la encriptación, así que la información simplemente no sirve, Algunos de los métodos de encriptación disponibles actualmente y que son bastantes conocidos se puede mencionar a:

- Encriptación simétrica
- Encriptación asimétrica de clave pública y privada
- Encriptación WPA
- Encriptación WEP
- Firma digital



FUNDACIÓN DE EDUCACIÓN SUPERIOR

SAN JOSÉ

INSTITUCIÓN TECNOLÓGICA

FIN DE
GRABACIÓN