**INICIO**

¿Qué es la ciberseguridad?

Según Cisco la ciberseguridad es la práctica de proteger sistemas, redes y programas de ataques digitales. Por lo general, estos ciberataques apuntan a acceder, modificar o destruir la información confidencial; Extorsionar a los usuarios o los usuarios o interrumpir la continuidad del negocio.

Actualmente, la implementación de medidas de seguridad digital se debe a que hay más dispositivos conectados que personas, y los atacantes son cada vez más creativos.

¿Sobre qué trata la ciberseguridad?

Un enfoque exitoso de ciberseguridad tiene múltiples capas de protección repartidas en las computadoras, redes, programas o datos que uno pretende mantener a salvo. En una organización, las personas, los procesos y la tecnología deben complementarse para crear una defensa eficaz contra los ciberataques. Un sistema unificado de gestión de amenazas puede automatizar las integraciones entre productos selectos de seguridad de Cisco y acelerar las funciones de operaciones de seguridad claves: detección, investigación y corrección.

Personas

Los usuarios deben comprender y cumplir con los principios básicos de seguridad de datos, como elegir contraseñas seguras, ser cautelosos con los archivos adjuntos de los correos electrónicos y hacer copias de seguridad de datos. Obtenga más información sobre los principios básicos de ciberseguridad.

Procesos

Las organizaciones deben tener una estructura para manejar los ciberataques tentativos y sospechosos. Una estructura de buena reputación puede guiarlo y explicar cómo puede identificar ataques, proteger sistemas, detectar y responder a amenazas, y recuperarse de ataques exitosos. Vea la explicación en video del marco de ciberseguridad del NIST (1:54)

Tecnología

La tecnología es esencial para brindar a las organizaciones y los individuos las herramientas de seguridad informática necesarias para protegerse de ciberataques. Se deben proteger tres entidades importantes: los dispositivos Endpoints (como computadoras, dispositivos inteligentes y routers), las redes y la nube. La tecnología común que se usa para proteger estas entidades incluye firewalls de próxima generación, filtrado de DNS, protección contra malware, software antivirus y soluciones de seguridad de correo electrónico.

¿Por qué es importante la ciberseguridad?

En el actual mundo conectado, todos se benefician de los programas de ciberdefensa avanzados. A nivel individual, un ataque a la ciberseguridad puede dar como resultado desde un robo de identidad hasta intentos de extorsión y la pérdida de datos importantes, como fotos familiares. Todos confían en las infraestructuras críticas, como las centrales eléctricas, los hospitales y las empresas de servicios financieros. Proteger estas y otras organizaciones es esencial para el funcionamiento de la sociedad.

Todos se benefician del trabajo de los investigadores de ciberamenazas, como el equipo de 250 investigadores de amenazas de Talos, que investiga las amenazas nuevas y emergentes y las estrategias de los ciberataques. Revelan nuevas vulnerabilidades, educan al público sobre la importancia de la ciberseguridad y refuerzan las herramientas de código abierto. Su trabajo hace que Internet sea más segura para todos.

**Ataques cibernéticos: causas**

Frente a la transformación digital que han tenido las empresas, de todas las industrias y tamaños, durante los últimos años, una realidad que no se puede ignorar es que ninguna está exenta de ser víctima de un ataque cibernético en cualquier momento.

Por eso, cada vez es más importante implementar estrategias y medidas que permitan reducir la posibilidad de sufrir un ataque de este tipo, que no solo pone en riesgo la reputación de la empresa sino también su operación, la relación con los clientes y proveedores, además, genera pérdidas de ingresos e incluso, de nuevas oportunidades de negocio.

A continuación, te contamos en este artículo cuáles son las principales causas de un ataque cibernético, cuáles son los ciberataques más comunes que se pueden materializar y cuáles son los impactos o consecuencias que esto puede significar para una organización. Igualmente, te compartimos algunas recomendaciones que te servirán para prevenir que esto ocurra en tu empresa.

**Principales causas de un ataque cibernético**

A partir de la transformación digital que viven las empresas y el uso masivo de nuevas tecnologías de información, cada vez estamos más conectados y tenemos acceso a muchos más datos.

Sin embargo, a pesar de las ventajas que esto representa, también ha facilitado que se presenten más ataques por parte de ciberdelincuentes que están atentos a las vulnerabilidades que puedan tener los sistemas informáticos para aprovecharse y hacer daños.

Entre las principales causas que pueden generar un ataque cibernético se destacan:

1. Vulnerabilidad de los sistemas informáticos, es decir, fallas o deficiencias que ponen en riesgo los activos al no estar protegidos de manera efectiva.

2. Divulgación de información confidencial por parte de los empleados de forma accidental.

3. Pérdida y robo de dispositivos electrónicos que almacenan información privada de la empresa.

4. Empleados con malas intenciones y sin escrúpulos que ponen en riesgo la información de la empresa.

5. Brechas o falta de controles por parte de terceros, es decir, si estos son víctimas de un ataque, los ciberdelincuentes pueden acceder a información de otras empresas con las que tienen relaciones y buscar la manera de también perjudicarlas.

6. Ingeniería social, social engineering, que en términos generales consiste en la manipulación de personas específicas con el fin de obtener datos confidenciales como contraseñas u otros de gran valor e importancia para la empresa.

Todas estas situaciones pueden facilitar la materialización de un ataque cibernético, que puede presentarse de diferentes maneras.

**DELITOS**

DELITOS REDES SOCIALES

SEXTING

El término "*sexting*" es un neologismo integrado ya plenamente a la literatura médica hispanoparlante que significa "recibir, enviar o reenviar mensajes de texto, imágenes o fotografías que presentan un contenido sexual explícito, vía Internet o teléfono celular".1 Muchas, por no decir la mayoría o la totalidad de estas imágenes, se diseminan de manera inmediata, incontrolada y extensa a través de las redes sociales -particularmente, los teléfonos celulares y computadoras- con resultados impredecibles, en la inmensa mayoría de las veces, catastróficos.

Investigaciones recientes señalan que un número creciente de adolescentes ha enviado o "posteado" fotografías o videos de ellos mismos o de otros compañeros en situaciones por demás comprometedoras (desnudos o semidesnudos, solos o acompañados, incluso en pleno escarceo erótico), lo que ha representado graves problemas, incluyendo cargos criminales por felonía o pornografía,2 además de otras consecuencias, especialmente de orden emocional. En las siguientes líneas nos ocuparemos del tema, ilustrándole con dos casos clínicos representativos.

**PRESENTACIÓN DE CASOS**

**Caso clínico 1**

Paciente femenina de 13 años, acudió a consulta con su madre por haber sido expulsada de la escuela. Refiere la madre que el motivo de la expulsión fue porque su hija apareció desnuda en las redes sociales y todos los alumnos de la secundaria mostraban las imágenes entre ellos.

Al interrogar a la adolescente, refirió su atracción por un chico de tercero de secundaria; su comunicación fue exclusivamente a través de las redes sociales, "WhatsApp" o "Facebook". Al percatarse el chico de esta atracción, le envió una foto de cuerpo entero desnudo y otra de sus genitales; le propuso que le enviara una de ella, comentando que, seguramente como era niña, no se iba a atrever a hacerlo. La adolescente pidió al chico que guardaran el secreto, y su sorpresa fue saber que toda la secundaria la había visto desnuda.

Los antecedentes heredofamiliares, personales patológicos y no patológicos eran negativos. Se trató de una alumna de primer año de secundaria en una escuela bicultural, de nivel socioeconómico medio alto.

Familiograma: familia funcional integrada por ambos padres, madre dedicada al hogar, padre con empleo y recursos económicos de nivel medio alto; dos hermanos mayores de 18 y 21 años, ambos estudiantes de preparatoria y universidad, respectivamente. Educación sexual en la escuela y la familia. A la exploración física, sin alteraciones. Durante el interrogatorio, presentó onicofagia.

Se realizaron seis sesiones de terapia sistémica breve a la adolescente y su madre. En el caso de la madre, se trabajó con hipnosis ericksoniana. Ella fue una adolescente rebelde y retadora, especialmente con su madre, ya que en su familia nuclear existía inequidad de género y los privilegios, salidas a fiestas, hora de llegada tarde, amigos, etcétera eran sólo para los hermanos varones. A las mujeres se les restringían las salidas, las amistades y la hora de llegar a casa. Por este motivo, ella se expuso a riesgos en múltiples ocasiones, ya que "era imposible negociar con su madre".

La educación que esta madre decidió darle a su hija fue exactamente opuesta a la que ella recibió; libre de prejuicios, libertad para expresarse, énfasis en la equidad con sus hermanos varones. Sin embargo, proyectó directamente en su hija su herida emocional y el miedo al rechazo por su condición femenina e, inconscientemente, no sólo la expuso al rechazo, sino también a la inequidad de género, ya que al chico no lo expulsaron.

La adolescente presentó crisis de ansiedad que fue resuelta exclusivamente con las intervenciones terapéuticas, sin requerir tratamiento farmacológico. Otras medidas fueron el cambio de escuela y la negociación con los padres en el establecimiento de reglas y límites claros, con énfasis en el uso de las redes sociales.

Se citó a la paciente a los tres y seis meses posteriores, consultas en las cuales la joven se encontró emocionalmente estable.

Grooming

Nuestro informe Violencia Viral incluye una encuesta con casi **400 jóvenes** de entre 18 y 20 años de toda **España**, para ver si durante su infancia y adolescencia les ha afectado alguno de los tipos de violencia online. El estudio nos ha confirmado que el online ***grooming*** es mucho más común de lo que pensamos. **Uno de cada cinco** de los encuestados **ha sufrido este tipo de**[**acoso**](https://www.savethechildren.es/donde/espana/violencia-contra-la-infancia/ciberacoso-ciberbullying) y el 15% en más de una ocasión. De media, la primera vez que sufrieron esta violencia fue con **15 años**.

LAS FASES DEL ‘ONLINE GROOMING’

El *online grooming* incluye una serie de conductas que pueden ser desordenadas, pero, por lo general, existen patrones de conducta y fases comunes que vamos a ver a continuación para poder detectarlo y prevenirlo.

1. **La creación de un vínculo de confianza.** En muchos casos a través de sobornos o engaños el agresor contacta con la niña o niño y establece el vínculo de confianza. Para ello normalmente finge otra edad, muy cercana a la de la víctima. Además, puede que el abusador haga regalos, empatice a un nivel profundo con los niños y niñas haciendo que escucha sus problemas y aproveche esa información para chantajear después.
2. **El aislamiento de la víctima.** En esta fase el agresor persigue arrancar la red de apoyo natural del menor (familiares, amistades, docentes, etc.) dejándolo desprotegido. De esta manera insiste en la necesidad de mantener todo en secreto.
3. **La valoración de los riesgos.** El agresor tiende siempre a asegurar su posición, así que suele preguntar a la víctima si alguien más conoce su relación e intenta averiguar quién más tiene acceso al ordenador o dispositivo que utiliza el menor.
4. **Conversaciones sobre sexo.** Una vez se siente con confianza, el abusador empieza a introducir conversaciones sexuales de manera paulatina. Busca que la víctima se familiarice tanto con la temática sexual como con el vocabulario.
5. **Las peticiones de naturaleza sexual**. Este es el objetivo principal del *online grooming*. En esta última fase el criminal utiliza la manipulación, las amenazas, el chantaje o la coerción para que la víctima le envíe material sexual, relate fantasías sexuales o la relación culmine con un encuentro físico.

## ¿CÓMO PREVENIR EL ‘GROOMING’?

Ante un fenómeno tan complejo, la respuesta debe ser integral y **la forma más eficaz de actuar contra la violencia viral se basa en la prevención**. Lo más indicado es intervenir en la educación en positivo a niños, niñas y adolescentes.

En primer lugar, es necesaria una **educación afectivo-sexual**, que forme a los más jóvenes en materia de sexualidad, y al mismo tiempo es importante la formación en un uso seguro y responsable de las herramientas digitales.

Es esencial tener en cuenta que especialmente en el **online grooming** el engaño es lento y **no hay consentimiento del niño o niña**, no son conscientes de lo que les ocurre, y no tienen las herramientas adecuadas para defenderse. Nunca podrá ser culpa de ellos.

En definitiva, la comunicación y la educación afectivo-sexual, juntas con el **apoyo del entorno más cercano a los menores**, son las herramientas más eficaces, tanto para prevenir la violencia, así como para no perpetuar sus consecuencias a largo plazo.

**Tipos de ataques cibernéticos**

Cuando hablamos de un ciberataque nos referimos a las acciones ofensivas y perjudiciales contra los sistemas de información, sea de una persona, una empresa o una entidad gubernamental. Estos sistemas pueden ser las redes informáticas, las bases de datos y todos los activos que almacenen datos e información confidencial y de valor de la organización.

Los ciberdelincuentes, generalmente, al cometer estos ataques buscan afectar, alterar o destruir no solo la reputación de una empresa o persona, sino también, impactar negativamente en su operación y en la relación con sus diferentes grupos de interés.

Por eso, es importante conocer cuáles son los principales ciberataques que pueden ocurrir para así, saber cómo actuar rápida e inteligentemente y poder mitigar los impactos.

Lo primero que hay que tener en cuenta es que estos ataques pueden ser tanto externos como internos, sí, en algunos casos puede ocurrir que un empleado ataque de forma voluntaria a la empresa, aunque la mayoría de veces esto sucede de forma accidental.

**Los ciberataques más comunes de los que pueden ser víctimas las empresas son:**

**el spear phishing** busca obtener datos de valor dirigiéndose a una persona o empresa específica luego de haberse ganado su confianza. Este ataque es muy utilizado con empresas y personas reconocidas.

**Whaling o “caza de ballenas”.** Están dirigidos a perfiles directivos como CEO’s o CFO’s y otros cargos altos de las organizaciones con el objetivo de robarles información confidencial a la que ellos tienen acceso.

**Malware.** Se trata de un programa o código malicioso que afecta de manera secreta y silenciosa a un sistema de información. Un malware tiene la capacidad de irrumpir, perjudicar y deshabilitar los ordenadores y demás activos de información, en otras palabras, a través de este se pueden robar y borrar datos, secuestrar funciones y espiar actividades sin ser notados. Algunos malware son los ransomware, troyanos y spyware.

**Ransomware**. También conocido como secuestro de datos consiste en el bloqueo, por parte de un hacker, de un dispositivo electrónico y en la encriptación de los archivos para que el usuario dueño no pueda acceder a la información y datos almacenados.

**Inyección SQL.** Es un ataque a la web que consiste en la infiltración de un código malicioso que aprovecha errores y vulnerabilidades de una página web. Es utilizado para robar bases de datos, manipular o destruir información.

**Otros ataques o ciberamenazas que se pueden presentar son:** ataques distribuidos de denegación de servicio (DDoS), troyanos o ataque de contraseñas.

**Ataques directos desde redes sociales son**

**Phishing (Suplantación de identidad).** El phishing consiste en correos electrónicos o mensajes de texto que aparentemente son enviados por fuentes confiables y que persuaden al destinatario a completar una acción, abrir un enlace malicioso, que va a poner en riesgo la información personal o de la empresa.

Sin duda uno de los ataques más comunes y que más presentes están en los últimos tiempos son los ataques Phishing. Básicamente consiste en recibir un mensaje con un link que en realidad es falso. Nos “invitan” a que entremos allí y posteriormente nos pedirá que iniciemos sesión.

La cuestión es que a la hora de iniciar sesión nuestros datos y contraseñas irán a parar a un servidor controlado por los piratas informáticos. Es muy importante que evitemos este tipo de ataques y siempre iniciemos sesión directamente desde sitios y aplicaciones legítimos.

**Bulos o Fake News**

Por supuesto los bulos y Fake News también están muy presentes. Son todas aquellas noticias falsas, mensajes erróneos y cualquier publicación que solo busca desinformar o llamar la atención de los usuarios pero en realidad es todo falso.

De esta forma logran que la víctima haga clic en esos enlaces y vaya a parar a una página fraudulenta. También puede que nos lleven a la descarga de software malicioso.

**Complementos falsos**

Como en muchas otras plataformas que utilizamos en nuestro día a día, las redes sociales también cuentan con complementos. Básicamente son ciertas herramientas que ofrecen mejoras. Esto nos permite tener una mayor usabilidad, por ejemplo.

Eso sí, hay que tener en cuenta que en la red hay una gran cantidad de complementos falsos. Software que ha sido modificado de forma maliciosa y tiene como objetivo robar nuestra información y, en definitiva, poner en riesgo nuestros dispositivos. Es otro de los ataques más frecuentes en redes sociales.

**Vulnerabilidades existentes**

Los ciberdelincuentes también pueden aprovecharse de vulnerabilidades existentes en los dispositivos de la víctima o en la propia red social. Como sabemos, en ocasiones surgen fallos que pueden poner en riesgo nuestra seguridad.

Para evitar esto es muy importante que siempre tengamos las últimas versiones instaladas. Necesitamos contar con los parches y actualizaciones que haya disponibles y de esta forma evitar que nos afecten las vulnerabilidades.

**La fuerza bruta**

Sin duda la fuerza bruta siempre será un tipo de ataque muy utilizado por los piratas informáticos también para afectar a nuestras redes sociales. Básicamente consiste en probar contraseñas hasta que den con la correcta. Incluso podrían simplemente probar claves básicas y muy utilizadas.

Para evitar este problema vital que activemos la autenticación en dos pasos siempre que sea posible. De esta forma necesitarían un segundo paso para poder entrar, que suele ser un SMS que recibimos por el móvil.

**TIPS**

**EL OSCURO DILEMA DE LAS REDES SOCIALES:**

*Enlace https://www.youtube.com/watch?v=Wm6YFpStf6s (video tomado de pandora marketing y publicidad)*

**¿Qué hacer para prevenir un ciberataque?**

Para prevenir la materialización de una amenaza o riesgo cibernético, en primer lugar es clave implementar estrategias de formación y concientización sobre seguridad informática y ciberseguridad para los empleados de la organización, considerados el eslabón más débil de la cadena.

Esto es fundamental hacerlo de manera consistente y efectiva para lograr que todos entiendan la importancia de hacer un buen uso de los activos y de la información a la que tienen acceso, así como tener cuidado con las contraseñas que utilizan y estar alertas ante posibles casos de phishing, malware u otros ataques.

Adicional a esto, las empresas deben estar preparadas para evitar un ciberataque, es decir contar con herramientas y desarrollar prácticas que les permitan detectar a tiempo las vulnerabilidades y debilidades de sus sistemas para corregirlas a tiempo, por ejemplo, el hacking ético.

Los ataques ocurren cada vez más, pero la buena noticia es que hay formas de prevenirlos, aquí te compartimos una serie de pasos que, además de ayudarte, permiten generar una cultura de ciberseguridad:

1. No permitir que nadie que no sea explícitamente invitado entre al sistema. Esto se logrará mediante:

Proteger las computadoras, usando antimalware y aplicando actualizaciones.

Usar sólo software aprobado por la compañía.

2. Conciencia personal

Tener mucho cuidado con los correos electrónicos que recibes.

Siempre busca los datos esenciales, como el nombre de la persona/empresa que envió el correo electrónico.

Cuida mucho cualquier clic a un enlace o descarga de archivos.

3. Infiltración por malware. Para evitar que un hacker se infiltre a través de un malware:

Nunca insertes nada en la computadora antes de asegurarte que es un dispositivo limpio.

Escanea el dispositivo para detectar virus.

No permitas que terceros ingresen datos en tu equipo.

4. Protección física. Al igual que una puerta, las computadoras también deben protegerse físicamente. Esto puedes hacerlo:

Usando autenticación de 2 pasos.

Al establecer contraseñas largas de al menos 8 caracteres. Mientras más larga una contraseña, más difícil de romperse.

No usar la misma contraseña para todos tus equipos y servicios.

Al tapar la cámara de la computadora portátil.

5. Redes

Usar redes de invitados para personal externo.

No conectar dispositivos personales a redes empresariales sin aviso.

Tener cuidado con lo que compartes en línea.

6. En caso de un ataque. En caso de que ocurra un incidente se recomiendan tres pasos que debes realizar inmediatamente después de darte cuenta:

Seguir los procedimientos de la compañía.

Informar de inmediato a los supervisores.

Nunca pagar el rescate por los datos.

La seguridad cibernética necesita personal capacitado para comprender el valor total de las inversiones en tecnología y los procedimientos de TI; un software antimalware riguroso es muy importante para evitar que los equipos y dispositivos móviles se infecten. Sin embargo, también es aconsejable realizar periódicamente copias de seguridad de los datos.

Recuerda que incluso si tus dispositivos no se han infectado nunca con software malicioso, la falla de un disco duro u otros componentes podría dificultar el acceso a la información más preciada. En ese momento, te alegrarás de haber realizado una copia de seguridad de los datos.

Contar con un aliado de tecnología con el conocimiento necesario y consultar a los expertos, te ayudará a lograr tus objetivos

**Consecuencias de sufrir un ciberataque**

Sin duda, una de las principales consecuencias de ser víctima de un ciberdelincuente es la afectación a la reputación de la empresa, pues esta se basa en la confianza, que puede verse disminuida al conocerse que se ha sufrido un ataque de este tipo.

Pero este no es el único impacto generado por un ciberataque, otros, igual de importantes, son:

Cese de actividades o retrasos en los procesos de producción o prestación de los servicios porque los sistemas están bloqueados, hay secuestro de información y se deben centrar en el rescate para poder operar con normalidad.

Afectaciones económicas. Por un lado porque los delincuentes pueden exigir grandes cantidades de dinero por el rescate de la información, es decir, la empresa es víctima de una extorsión, y por otro lado porque aumentan los gastos empresariales ya que para dar solución al problema, muchas veces, se requiere acompañamiento y asesoramiento tecnológico y legal de expertos.

Pérdida de clientes y proveedores. Está relacionado con el daño a la reputación y a la imagen de la empresa, pues públicos como estos pueden dejar de confiar en la empresa que fue víctima de un ciberataque ya que ven que es vulnerable y puede ponerlos también en riesgo.