AlfaOnline

GUÍA DE ESTUDIO *Curso en línea*

Ciberseguridad

Autores: Miguel Guadalupe Patrón Bogarín
Luz Patricia Ramírez Aceves

Octubre 2020

AlfaDigital
Dirección de Alfabetización Digital

Recrea
Educación para refundar 2040

Educación

Jalisco
GOBIERNO DEL ESTADO

Educación

AlfaDigital
Dirección de Alfabetización Digital

Recrea
Educación para refundar 2040

Guía de Estudio

AlfaOnline

Curso en línea

Ciberseguridad

Asesor: Luz Patricia Ramírez Aceves

Octubre de 2020

Contenido

Ciberseguridad

Bienvenid@s

Estimados estudiantes reciban un cordial saludo de bienvenida a este curso en línea: Ciberseguridad, clases en línea; ofrecido por la Secretaria de Educación del Estado de Jalisco a través de la Dirección de Alfabetización Digital.

En la plataforma Alfa Online tenemos el objetivo de brindar al docente cursos en línea que le permitan fortalecer sus competencias tecnológicas.

Este curso pretende apoyar a la educación virtual y a distancia, uno de los grandes retos de Recrea Digital.

Con el presente curso recibirá una formación básica en materia de ciberseguridad. La cual es necesaria hoy día debido al auge de las nuevas tecnologías.

El uso de internet para el intercambio de información hace que la protección de los datos y de los sistemas sea de vital importancia, para poder garantizar la integración de la información protegiendo nuestros datos en la web, redes y los sistemas de información.

Te damos la bienvenida al curso de *Ciberseguridad, clases en línea.* Gracias por inscribirte, esperamos cumplir con tus expectativas.

Justificación

Este curso presenta una introducción a la seguridad cibernética mostrando diferentes aspectos de esta disciplina. Aprenderá cuáles son las principales amenazas de seguridad cibernética existentes y cómo protegerse contra ellas. El curso presenta un enfoque práctico en el que se proporcionará todo el material necesario para que pueda comprender mejor los ataques y establecer las contramedidas adecuadas.

Objetivo general del curso

Al finalizar el curso podrá proteger los datos de carácter personal, conociendo de ciberseguridad en entornos móviles y gestionando la seguridad de una red local.

Objetivos particulares del curso

- .Reconocer conceptos básicos y características de ciberseguridad
- Identificar herramientas para la ciberdefensa
- Diferenciar herramientas utilizadas para la gestión de vulnerabilidades

Contenido

Módulo 1: Introducción y conceptos básicos

- Introducción
- Impacto de la ciberseguridad
- Tipos de ciberamenazas
- Medidas de precaución
- Actividades para trabajar con los alumnos
- Evaluación Módulo 1 (calificación 80 mínima aprobatoria)

Módulo 2: Malaware y amenazas persistentes

- Introducción.
- Definición y tipos de malware.
- Principales técnicas para lograr la identificación.
- Malware en dispositivos móviles
- ¿Cómo puedo quitar el malware?
- Evaluación Módulo 2 (calificación 80 mínima aprobatoria)

Módulo 3: Vulnerabilidades y exposiciones

- Introducción
- Vulnerabilidad
- Amenaza

- Riesgos
- Áreas vulnerables
- Evaluación Módulo 3 (calificación 80 mínima aprobatoria)

Módulo 4: Ciberdefensa

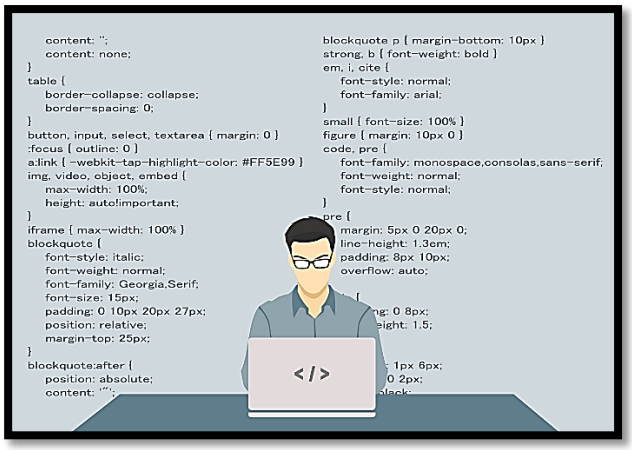
- Introducción
- ¿Qué es la ciberseguridad y cómo se puede aplicar?
- ¿Cómo bloquear el robo de datos?
- Evitando ciberataques
- Amenazas más comunes
- Fases de la ciberseguridad
- Las intrusiones informáticas
- Detección de intrusión
- Evaluación Módulo 4 (calificación 80 mínima aprobatoria)

Módulo 1: Introducción y conceptos básicos

Introducción

¿Has oído hablar de los ataques que reciben las grandes compañías o los bancos a través de sus sistemas informáticos? ¿Sabes detectar un archivo infectado por un virus? O ¿conoces medidas de seguridad para proteger un equipo o una red de ciberataques?

En este módulo aprenderás cuáles son las principales amenazas de seguridad cibernética existentes y cómo protegerte contra ellas desde un enfoque práctico, en el que se proporciona el material necesario para comprender mejor los ataques y establecer contramedidas apropiadas.



A continuación, te dejó este vídeo a manera de introducción; realizado por Mikel Murugarren y Álvaro Rodríguez.

https://youtu.be/3pydMCDZvMw

Impacto de la ciberseguridad

¿Qué es la ciberseguridad?

El concepto de ciberseguridad no está definido claramente. Se podría decir que la ciberseguridad o seguridad informática es aquella actividad que se ocupa

de evitar y gestionar los riesgos y amenazas derivados de la Red y del uso de dispositivos electrónicos.

Sin embargo, no afecta solamente a los propios dispositivos electrónicos, además, pueden verse vulnerados derechos fundamentales de las personas como, por ejemplo: a la intimidad, a la propia imagen y a la protección de los datos personales.

Así como la posibilidad de que se comentan delitos cibernéticos: estafas, fraudes electrónicos, daños económicos, entre otros.

Si añadimos a todo esto el efecto multiplicador de la Red, los riesgos y daños derivados de ella se incrementan desmesuradamente. Precisamente por ello, la ciberseguridad deberá ser abordada desde diferentes perspectivas:

- Riesgos y amenazas.
- Prevención y gestión de riesgos.

Por todo ello se puede decir que el concepto de ciberseguridad es complejo, y tiene por finalidad la prevención y gestión de riesgos y la respuesta inmediata ante las amenazas procedentes de la Red, requiriendo para ello soluciones multidisciplinares técnicas, legales, etc.

¿Cómo nos afecta la falta de ciberseguridad y sus problemas?

El generalizado uso de las Tecnologías de la Información y la Comunicación (TIC) en todos los ámbitos de la vida, afecta tanto a las personas individualmente como a las empresas y administraciones públicas, conteniendo diversos problemas.

Los más habituales suelen ser la recepción de correos electrónicos no deseados, la suplantación de identidad, los virus informáticos, el borrado de datos y archivos.

Se puede destacar que el primer motivo de no utilización de medidas de seguridad es la creencia de “no necesitarlas o no estar interesados en ellas”. Ello debe llevarnos a una seria reflexión, y es que el principal error en materia de ciberseguridad parece ser el exceso de confianza de los usuarios. Pero en la Red

cualquier usuario está expuesto y es susceptible de ser víctima de un ataque de seguridad.

Destaca también que, tras sufrir un intento de fraude o perjuicio económico en relación con los servicios de banca online y comercio electrónico, la respuesta mayoritaria es no modificar los hábitos de banca electrónica y comercio electrónico.

Todos podemos vernos afectados por problemas de seguridad en el uso de Internet, por lo que debemos ser cada día más conscientes de que la ciberseguridad nos afecta a todos y, por consiguiente, corresponde a todos adoptar medidas con el fin de prevenir los riesgos derivados de Internet.

El sector educativo también sufre los efectos de la ciberseguridad

Las instituciones educativas manejan grandes volúmenes de datos personales de alumnos y del equipo docente, documentos de identidad, datos financieros, historial académico, registros médicos, por lo que se convierten en un blanco estratégico de los ciberdelincuentes para afectar la privacidad de las personas y sobre todo la integridad de la información.

ESET (Enjoy Safer Technology), compañía proveedora de soluciones de seguridad realizó una encuesta en la que participaron instituciones de primaria, secundaria, medio superior y superior de Latinoamérica con el objetivo de conocer la exposición de las instituciones educativas a riesgos de seguridad.

El principal hallazgo del estudio señala que 67% de las instituciones participantes aseguró haber sufrido al menos un incidente de seguridad. Y es que básicamente podrían quedar expuestas al acceso indebido de información sensible y robo de datos. Sin embargo, 72% dice realizar actividades de concientización, pero solamente un 31% lo hace de manera periódica.

Estar conectado a una red no del todo segura puede generar que los dispositivos vinculados sean vulnerados permitiendo a los atacantes acceder desde fotografías hasta la modificación de datos o notas académicas. Además,

se expone el prestigio de la institución a través del defacement y otras actividades hacktivistas.

Tipos de ciberamenazas

Estos son los tiempos del auge de las ciberamenazas, los ciberataques y el cibercrimen. Cuando se sufre robo de identidad o algún ciberataque, las víctimas del fraude pueden llegar a gastar 776 USD aproximadamente de su propio dinero y perderán 20 horas tratando de arreglar el desastre ocasionado por los ladrones de identidad.

A continuación, te presentamos las siete amenazas que representan los desafíos actuales a tener en cuenta para mantener tus datos protegidos.

1- Ataques a los datos de minoristas

Los ataques a minoristas son un grave peligro porque pueden afectar prácticamente a todo el mundo. En 2014 se observó un incremento de los ciberataques. Los hackers robaron 40 millones de números de tarjetas de crédito y débito de los clientes.

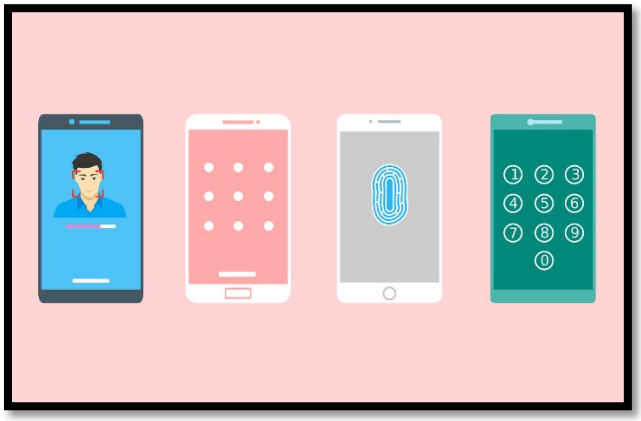
Los cibercriminales roban y venden esta información personal en el mercado negro, lo que conllevar fácilmente al robo de identidad. Si bien gran parte de la responsabilidad recae sobre el minorista, como mantener sus métodos de pago seguros y actualizados, vigilar atentamente tu cuenta bancaria y el extracto de la tarjeta de crédito es una buena forma de permanecer seguro durante ataques a minoristas.

2- Amenazas a la seguridad móvil y vulnerabilidades del smartphone

Los cibercriminales pueden aprovechar fácilmente las vulnerabilidades de tu teléfono móvil para obtener datos privados. Estas vulnerabilidades a veces provienen de las aplicaciones que utilizas, o bien de tu propio smartphone.

Los teléfonos móviles también son vulnerables a malware, que puede registrar pulsaciones de teclas y realizar capturas de pantalla.

Protégete mediante la investigación de las aplicaciones que descargas y teniendo cuidado con los mensajes de correo electrónico que abres y las fotos que decides cargar.



3- Ataques de phishing e ingeniería social

Cuando los cibercriminales engañan a las personas para que revelen información confidencial, como contraseñas y números de la seguridad social, la estafa se llama phishing.

Una de las maneras más comunes en las que se produce el phishing es cuando una persona recibe un correo electrónico, supuestamente de un banco o una organización gubernamental, y se les dirige a sitios que tienen un aspecto auténtico. Una vez allí, se le solicitará a la persona que introduzca su contraseña, los números de la seguridad social y los datos financieros.

Los cibercriminales aprovechan esta información y la utilizan para sus propios fines.

El phishing es parte de un problema más amplio llamado ingeniería social, que es esencialmente la manipulación de las emociones con el fin de obtener acceso a datos confidenciales.

No te dejes engañar por estos trucos.

Desconfía de todos los mensajes de correo electrónico que recibas, especialmente aquellos en los que se te solicita que vuelvas a introducir información privada.

Recuerda que los bancos y las organizaciones gubernamentales reales nunca te piden que verifiques la información potencialmente confidencial.

4- Robo de identidad

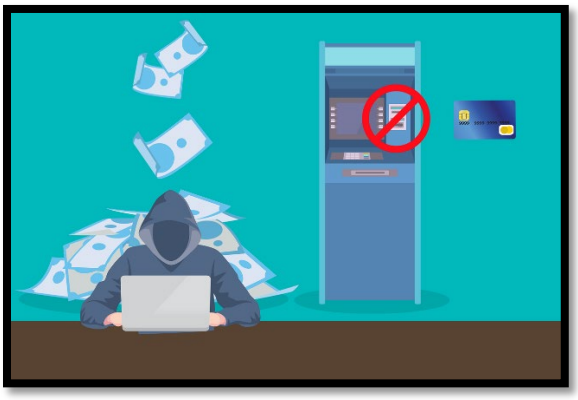
Uno de los delitos online que han visto un crecimiento más rápido es el robo de identidad.

Muchos de los puntos descritos anteriormente pueden llevar al robo de identidad, los correos electrónicos de phishing y los robos de datos.

Sin embargo, tu identidad está también en riesgo a través de materiales cotidianos, como tu currículum vitae, la dirección de tu casa, fotos y vídeos de las redes sociales, datos financieros, etc.

Los ladrones de identidad pueden robar tu información personal y abrir tarjetas de crédito y cuentas de préstamos en tu nombre. Aunque algunos de

estos métodos quedan fuera de las manos de una persona normal, todavía hay muchas cosas que puedes hacer para proteger tu identidad.



5- Ataques a los datos

A principios de 2015, el videojuego Anthem experimentó un ataque masivo de robo de datos por parte de hackers que afectó a 78,8 millones de personas.

En julio de 2015, los hackers irrumpieron en la red informática del sistema de salud de UCLA; potencialmente, obtuvieron acceso a la información personal de 4,5 millones de pacientes.

Los registros sanitarios contienen información importante y confidencial, y son los objetivos principales para los cibercriminales, que pueden llevar fácilmente al robo de identidad. A veces, esta información se utiliza para cometer fraudes relacionados con los seguros de salud, tales como la compra y venta de recetas fraudulentas.

6- Ataques de depredadores sexuales dirigidos a niños

Los usuarios que buscan atacar a los niños acechan en los rincones oscuros de Internet para comerciar con fotos ilegales e indecentes de niños.

Esto se hace a través del correo electrónico, los programas punto a punto (P2P, del inglés Peer-to-Peer), o bien, cada vez más, a través de la "dark web", un área de Internet a la que no se puede acceder mediante los motores de búsqueda estándar. Aunque son tendencias inquietantes, es mejor dejar estos sitios a los funcionarios encargados de hacer cumplir la ley y que las personas normales los eviten totalmente.

Otro peligro online destinado a los niños es cuando los depredadores sexuales intentan atraerlos para quedar con ellos fuera de Internet, así como enviar o solicitar imágenes pornográficas e indecentes. Asegúrate de que tus hijos conocen bien los peligros de hablar con extraños online, y de que nunca comparten información personal con personas que nunca han conocido.

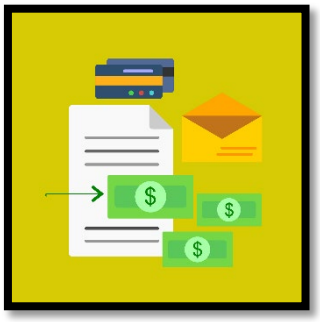
7- Ataques a bancos

En el siglo XXI, los robos de los bancos ahora se hacen en el ámbito digital. Un ejemplo famoso es el de una banda criminal que robó hasta mil millones de dólares en dos años aproximadamente de una amplia variedad de instituciones financieras de todo el mundo. Los cibercriminales dirigieron sus ataques a empleados y funcionarios de los bancos mediante un malware llamado "Carbanak" a través de correos electrónicos.

Una vez que infectaron con éxito los ordenadores deseados, los cibercriminales lograron imitar con éxito el comportamiento de los empleados para transferirse dinero a sí mismos, controlar los cajeros automáticos para que dispensaran dinero en determinados momentos y utilizar los sistemas de pago electrónicos para filtrar el dinero.

Investiga siempre el historial de seguridad de un banco antes de elegirlo, no hagas clic en ningún enlace extraño de los correos electrónicos, destruye los documentos financieros y vigila constantemente si hay irregularidades en tu cuenta.

En un mundo de crecientes ciberamenazas, ¿qué puedes hacer para protegerte? La conciencia sobre la seguridad es la primera línea de defensa. Hay potentes herramientas de seguridad disponibles que te podrán ayudar, pero recuerda que también necesitas usar el sentido común para proteger tu ordenador, tu información y a ti mismo.



Medidas de precaución:

- ✓ Utiliza contraseñas seguras para tus cuentas que incluyan números y letras mayúsculas y minúsculas, y que no sean fáciles de adivinar, como por ejemplo "contraseña", "12345", etc.
- ✓ Evita abrir correos electrónicos sospechosos en los que se te pida que vuelvas a introducir datos confidenciales.
- ✓ Destruye los documentos confidenciales.
- ✓ Utiliza una VPN para proteger tu conexión a Internet si necesitas utilizar una Wi-Fi pública.
- ✓ Mantén actualizado el software antivirus.

Ahora te invito a ver dos vídeos de Alberto Prieto Espinoza del Dto. de Arquitectura y Tecnología de Computadores de la Universidad de Granada.

Ciberseguridad: conceptos básicos: https://youtu.be/A5wsW3aE8E8

Ciberseguridad protección: https://youtu.be/hhKyo6XjOMc

Actividades para trabajar con los alumnos

Te dejamos un extracto del Programa Construye Paz, creado por la Dirección de Prevención del Delito de Fiscalía Estatal.

En este encontrarás actividades que puedes trabajar en clase con tus alumnos para prevenir Incidentes Cibernéticos, Robo y Extorsión Telefónica.

http://educacionvirtual.se.jalisco.gob.mx/dipta/pluginfile.php/75478/mod_resource/content/1/Constuye%20Paz%20desde%20casa%2C%20Incidentes%20Cibern%C3%A9ticos.pdf

Evaluación Módulo 1

Ingresa a la evaluación del Módulo 1

Recuerda descargar la Guía de estudio para que puedas tomar notas.

Ver los tres vídeos presentados en el Módulo

Contesta las 5 preguntas que vienen en el Examen.

Para que puedas acreditar el módulo necesitas tener una calificación mínima aprobatoria de 8.0

Módulo 2: Malaware y amenazas persistentes

Introducción

Estas amenazas las podemos comparar con las epidemias de gripe y por lo tanto la comunidad médica realiza campañas para que todo el mundo se vacune contra la misma. Esto debido a que los brotes de gripe se producen en una estación determinada del año en la que empiezan a extenderse y a contagiar a la gente.

Por el contrario, no hay epidemias estacionales previsibles para los PC, teléfonos inteligentes, tabletas y redes empresariales. En este caso, siempre es temporada de gripe. Pero en lugar de tener escalofríos y dolor por todo el cuerpo, los usuarios pueden padecer una especie de enfermedad de las máquinas: el **Malaware**.

Las infecciones por malware nos llegan como el caudal de agua de una manguera contra incendios, cada una con sus propios métodos de ataque, que pueden ser sigilosos y solapados o nada sutiles, como un golpe. Pero si el conocimiento es poder, aquí puede ver, a modo de inoculación preventiva contra la infección, un curso breve sobre el malware: qué es, sus síntomas, cómo se contagia, cómo tratarlo y cómo evitarlo en el futuro.

Definición y tipos de malware.

¿Qué es el malware?

Malware o “software malicioso” es un término amplio que describe cualquier programa o código dañino para los sistemas.

El malware hostil, intrusivo e intencionadamente desagradable intenta invadir, dañar o deshabilitar ordenadores, sistemas informáticos, redes, tabletas y dispositivos móviles, a menudo asumiendo el control parcial de las operaciones de un dispositivo.

La intención del malware es sacarle dinero al usuario ilícitamente. Aunque el malware no puede dañar el hardware de los sistemas o el equipo de red, sí puede robar, cifrar o borrar sus datos, alterar o secuestrar funciones básicas del ordenador y espiar su actividad en el ordenador sin su conocimiento o permiso.

¿Cómo me he infectado con malware?

Una infección de malware se puede producir por dos principales maneras: Internet y el correo electrónico, es decir, básicamente todo el tiempo que está conectado a Internet.

El malware puede penetrar en tu ordenador cuando: navegas por sitios web pirateados, haces clic en demostraciones de juegos, descargas archivos de música infectados, instalas nuevas barras de herramientas de un proveedor desconocido, instalando software de una fuente dudosa, abriendo un archivo adjunto de correo electrónico malicioso o descargando prácticamente cualquier cosa de la web en un dispositivo que carece de una aplicación de seguridad antimalware de calidad.

Las aplicaciones maliciosas pueden ocultarse en aplicaciones aparentemente legítimas, especialmente cuando se descargan a través de sitios web o mensajes y no desde una App Store segura.

Es importante, por tanto, prestar atención a los mensajes de advertencia al instalar las aplicaciones, sobre todo si solicitan permiso para acceder a su correo electrónico u otro tipo de información personal.

¿Cuáles son los tipos más comunes de malware?

Estos son los malware más comunes:

- El **adware** es un software no deseado diseñado para mostrar anuncios en su pantalla.
- El **spyware** observa las actividades del usuario en el ordenador en secreto y sin permiso, y se las comunica al autor del software.
- Un **virus** es malware que se adjunta a otro programa y, cuando se ejecuta —normalmente sin que lo advierta el usuario—, se replica modificando otros programas del ordenador e infectándolos con sus propios bits de código.
- Los **gusanos** son un tipo de malware similar a los virus, que se replica por sí solo con el fin de diseminarse por otros ordenadores en una red, normalmente provocando daños y destruyendo datos y archivos.
- Un **troyano**, o caballo de Troya, es uno de los tipos de malware más peligrosos. Normalmente se presenta como algo útil para engañar al usuario. Una vez que está en el sistema, los atacantes que se ocultan tras el troyano obtienen acceso no autorizado al ordenador infectado. Desde allí, los troyanos se pueden utilizar para robar información financiera o instalar amenazas como virus.
- El **ransomware** bloquea el acceso del usuario al dispositivo o cifra sus archivos y después lo fuerza a pagar un rescate para devolvérselos.
- El **rootkit** es un tipo de malware que proporciona al atacante privilegios de administrador en el sistema infectado.
- Un **registrador de pulsaciones de teclas** graba todas las pulsaciones de teclas del usuario, almacena la información recopilada y se la envía al atacante, que busca información confidencial, como nombres de usuario, contraseñas o detalles de la tarjeta de crédito.

- La **minería de criptomonedas** maliciosa, denominada también minería fortuita o **cryptojacking**, es un malware cada vez más prevalente instalado por un troyano. Permite que otras personas utilicen su ordenador para hacer minería de criptomonedas como bitcoin o monero. Los programas maliciosos de minería de criptomonedas utilizan los recursos de su ordenador, pero envían los coins obtenidos a sus propias cuentas, no a las del propietario del equipo. En pocas palabras, un programa de minería de criptomonedas malicioso, le roba recursos para hacer dinero.
- Los **exploits** son un tipo de malware que aprovecha los errores y vulnerabilidades de un sistema para que el creador del exploits pueda asumir el control. Los exploits están vinculados, entre otras amenazas, a la publicidad maliciosa, que ataca a través de un sitio legítimo que descarga contenido malicioso inadvertidamente desde un sitio peligroso. A continuación, el contenido dañino intenta instalarse en el ordenador tras una descarga involuntaria.

Principales técnicas para lograr la identificación de amenazas.

El malware puede manifestarse a través de varios comportamientos aberrantes. Estos son algunos signos reveladores de que tiene malware en su sistema:

- El ordenador se ralentiza. Uno de los efectos principales del malware es reducir la velocidad del sistema operativo, tanto si navega por Internet como si sólo utiliza sus aplicaciones localmente.
- La pantalla se llena de oleadas de publicidad fastidiosa que no tendría que mostrarse. Los anuncios emergentes inesperados son un signo típico de infección por malware. Es más, los mensajes emergentes suelen ir unidos a otras amenazas de malware ocultas. Por tanto, si aparece algo como "¡enhorabuena, ha ganado un teléfono nuevo!" en un mensaje emergente, no haga clic en él. Sea cual sea el premio que el anuncio promete, le saldrá muy caro.
- El sistema se bloquea constantemente o muestra una pantalla azul BSOD (Blue Screen of Death), que puede aparecer en los sistemas Windows cuando se encuentra un error grave.
- Observa una pérdida misteriosa de espacio disponible en disco, probablemente debido a un ocupante indeseado de malware que se oculta en su disco duro.
- Se produce un aumento extraño de la actividad del sistema en Internet.
- La utilización de recursos del sistema es anómalamente elevada y el ventilador del equipo comienza a funcionar a toda velocidad, lo cual señala que la actividad del malware se ha apropiado de recursos del sistema en segundo plano.
- La página de inicio del navegador cambia sin su permiso. Igualmente, los enlaces en los que hace clic lo llevan a un destino web no deseado. También es posible que el navegador responda muy lentamente.
- El navegador se llena inesperadamente de nuevas barras de herramientas, extensiones o complementos.

- Su producto antivirus deja de funcionar y no puede actualizarlo, dejándolo desprotegido contra el malware tramposo que lo deshabilitó.
- También puede producirse un ataque de malware obviamente dañino e intencionadamente provocador. Este es el caso del ransomware, que se anuncia sin disimulo, le dice que tiene sus datos y exige un rescate para devolverle sus archivos.
- Incluso si todo parece funcionar bien en su sistema, no se confíe, porque no conocer el problema no significa necesariamente que no existe. El malware potente puede ocultarse en lo más profundo de su ordenador y husmear sus datos sin disparar ninguna alarma mientras se apodera de sus contraseñas, roba archivos confidenciales o utiliza su PC para expandirse por otros equipos.

Malware en dispositivos móviles

A los delincuentes del malware les encanta el mercado de los dispositivos móviles. Después de todos, los teléfonos inteligentes, son ordenadores de mano sofisticados y complejos. Además, ofrecen una puerta de entrada a un tesoro de información personal, detalles financieros y todo tipo de datos valiosos para quienes intentan ganar dinero de forma deshonesta.

Desgraciadamente, esto ha generado un número de intentos maliciosos que crece exponencialmente para aprovechar las vulnerabilidades de los teléfonos inteligentes. El malware puede encontrar la manera de entrar en su teléfono por diversos medios, ya sea adware, troyanos, spyware, gusanos o ransomware. Hacer clic en un enlace sospechoso o descargar una aplicación poco fiable son algunas de las causas más obvias, pero una infección también puede provenir de correos electrónicos, mensajes de texto e incluso la conexión Bluetooth. Además, un malware como los gusanos puede difundirse de un teléfono infectado a otro.

El hecho es que se trata de un mercado enorme. Según una fuente de estadísticas, el número de usuarios de dispositivos móviles asciende a 2100 millones en todo el mundo y se prevé su crecimiento hasta 2500 millones de usuarios. Una cuarta parte de estos usuarios tiene más de un dispositivo. Los defraudadores encuentran muy atractivo el mercado de los teléfonos móviles

y se aprovechan de una economía de escala de proporciones gigantescas para sacar partido a sus esfuerzos.

Los usuarios de teléfonos móviles suelen ser un objetivo más fácil también. La mayoría no protege su teléfono con tanta diligencia como protege su ordenador y no instala software de seguridad ni mantiene actualizado su sistema operativo. Debido a esto, son vulnerables incluso a malware primitivo. Como las pantallas de los dispositivos móviles son pequeñas y los usuarios no pueden ver fácilmente la actividad, los comportamientos típicos de alarma que señalan una infección en un PC pueden ejecutarse entre bambalinas en modo sigiloso, igual que en el caso del spyware.

Los dispositivos móviles infectados son un peligro especialmente insidioso en comparación con los PC infectados. Un micrófono o una cámara pirateados pueden seguir cada una de sus conversaciones y movimientos. Y lo que es peor, el malware de banca móvil intercepta las llamadas entrantes y los mensajes de texto para eludir la seguridad de autenticación en dos pasos que muchas aplicaciones de banca utilizan.

En cuanto al ecosistema de malware para móviles, los dos sistemas operativos de teléfono inteligente más comunes son iOS de Apple y Android de Google. Android es el líder del mercado con el 80% de las ventas de teléfonos inteligentes, seguido de iOS con un 15% de las ventas. Por eso no es nada extraño que la plataforma Android, más popular, atraiga más malware que la del iPhone.

¿Cómo puedo saber si mi dispositivo está infectado con malware?

Afortunadamente, hay algunos síntomas inconfundibles que le indican que su teléfono está infectado. Puede estarlo si observa algo de lo siguiente:

- ✓ Una aparición repentina de mensajes emergentes con anuncios invasivos.
- ✓ Un aumento desconcertante del uso de datos. El malware utiliza su plan de datos para mostrar anuncios y enviar la información sustraída de su teléfono.
- ✓ Cargos falsos en su factura. Esto ocurre cuando el software malicioso hace llamadas y envía mensajes de texto a teléfonos de pago.
- ✓ Un consumo de batería injustificado. El malware utiliza muchos recursos y agota la carga del batería más rápido de lo normal.
- ✓ Las personas de su lista de contactos reciben llamadas y mensajes de texto extraños desde su teléfono.
- ✓ El teléfono se calienta y el rendimiento disminuye.
- ✓ Aparecen aplicaciones "sorpresa" en la pantalla. A veces pueden descargarse aplicaciones que tienen malware superpuesto que se instala repentinamente.
- ✓ El teléfono activa las conexiones wifi y se conecta a Internet por sí solo. Esta es otra manera en la que se propaga el malware: ignora sus preferencias y abre canales de infección.

¿Cómo puedo quitar el malware?

Si sospecha que tiene malware —o simplemente quiere ser cuidadoso— puede tomar algunas medidas.

Primero, si no tiene instalado todavía un programa antimalware legítimo, descárguelo, por ejemplo, Malwarebytes for Windows, Malwarebytes for Mac, Malwarebytes for Android. A continuación, instálelo y ejecute un análisis. Los programas como estos están diseñados para buscar y eliminar cualquier malware de su dispositivo.

Una vez limpio el dispositivo, puede ser buena idea cambiar las contraseñas: no solo la del ordenador o la del dispositivo móvil, sino también la del correo electrónico, de sus cuentas en redes sociales, de sus páginas web favoritas para comprar en línea y de los centros de banca online y facturación que utilice.

Si su iPhone se ha infectado de alguna manera, las cosas pueden ser un poco más complicadas. Apple no permite los análisis del sistema del iPhone ni de otros archivos. Su única opción es reiniciar el teléfono a los valores de fábrica y después restaurarlo desde su copia de seguridad (porque tiene una, ¿no?). También puede utilizar un software de seguridad que filtre y bloquee las llamadas y mensajes de texto fraudulentos.

Evaluación Módulo 2

Ingresa a la evaluación del Módulo 2

Recuerda descargar la Guía de estudio para que puedas tomar notas.

Contesta las 8 preguntas que vienen en el Examen.

Para que puedas acreditar el módulo necesitas tener una calificación mínima aprobatoria de 8.0

Módulo 3: Vulnerabilidades y exposiciones

Introducción

Cuando hablamos de ciberseguridad o seguridad informática solemos utilizar a menudo los términos “amenaza” y “vulnerabilidad”, los cuales representan una realidad con la que nos enfrentamos a menudo en este trabajo.

Sin embargo, muchas personas los confunden. Por ello, vamos a hacer una comparativa Amenaza vs. Vulnerabilidad para mostrarte qué son ambos conceptos y en qué se diferencian.

Vulnerabilidad

La vulnerabilidad es la debilidad o fallo que presenta un sistema de información. Este es capaz de poner en riesgo la seguridad de toda o parte de la información. Es decir, es un problema que tiene nuestro sistema.

El motivo es que este fallo o debilidad permite que el atacante comprometa la integridad, confidencialidad e incluso la disponibilidad de la información y los datos.

Los orígenes de las vulnerabilidades son muy diferentes. Pueden ser debidas a fallos en el diseño del sistema, carencia de procedimientos o simples errores de configuración.

Amenaza

La amenaza es la acción que se vale de una vulnerabilidad para actuar contra la seguridad del sistema de información.

Estas actuaciones son siempre peligrosas, pero, obviamente, si existe una vulnerabilidad su efecto se posibilita y multiplica. La amenaza no forma parte de nuestro sistema.

Sus orígenes pueden ser muchísimos:

- ✓ **Código malicioso o malware**: Es el más general y permite ejecutar muchas acciones ofensivas muy variadas.
- ✓ **APTs**: Son elaborados, bien coordinados y se enfocan en una empresa u organización para realizar un ataque con un objetivo específico contra su información.
- ✓ **Ingeniería social:** Se utilizan técnicas persuasivas para aprovechar la buena voluntad de la gente; es decir, atacan al componente humano.
- ✓ **Botnets**: Son equipos infectados que se dedican a ejecutar, de manera automática, programas para realizar ataques sofisticados.
- ✓ **Servicios en la nube**: La nube es tremendamente vulnerable, por ello, es necesario que si contratas algún servicio exijas la misma seguridad que tienes en tus sistemas, con acuerdos de nivel de servicios firmados. Si no, se abrirán brechas muy rápidamente y quedaras tremendamente expuesto.

- ✓ **Redes sociales**: La reputación de la empresa se puede ver en entredicho con un uso descontrolado de estas, que, por otro lado, son tremendamente accesibles.

Por este motivo, es esencial estar perfectamente protegido. Las amenazas existentes son muchas y los atacantes están al acecho esperando su oportunidad.

Tenemos así que las vulnerabilidades son las condiciones de nuestro sistema que los hacen ser susceptibles a las amenazas, que son las circunstancias ajenas capaces de suponer un riesgo o ser un peligro.

Riesgo

El riesgo es una probabilidad de que se pueda producir un incidente relacionado con la ciberseguridad industrial y doméstica, y tiene como principales factores la existencia tanto de una vulnerabilidad como de una amenaza.

Se trata de una cifra que indica las posibilidades de que una amenaza, con el aprovechamiento de una vulnerabilidad, se materialice produciendo impactos negativos en el sistema de información.

Áreas vulnerables

Algunos aspectos de nuestras vidas digitales son particularmente vulnerables a los ataques. Considera cuán seguras pueden ser estas actividades en tu hogar u organización:

1. El intercambio de archivos puede abrir oportunidades para que el malware se propague.
2. Java, JavaScript y ActiveX se han considerado problemáticos desde hace mucho tiempo porque permiten que los programas se transmitan y se ejecuten en tu ordenador. Por lo tanto, es importante mantenerse actualizado con todos los parches de software.
3. El correo electrónico presenta múltiples oportunidades para propagar malware y caos. Las falsificaciones de correo electrónico aparecen como un mensaje legítimo, a menudo de una figura de autoridad. El mensaje te pide que actualices tu contraseña o que envíes datos personales, revelando así información confidencial a un criminal. El correo electrónico también puede transmitir virus en archivos adjuntos y enlaces.
4. Las extensiones ocultas te engañan para descargar y abrir archivos que parecen legítimos. Para combatir esto, no abras ni descargues archivos que parecen fuera de lugar.
5. Los clientes de chat pueden transmitir malware a través de archivos adjuntos y enlaces. También puedes ser engañado para revelar información segura a alguien que finge ser otra persona.
6. Las amenazas físicas todavía existen. Los discos se bloquean. Los rayos caen y provocan un aumento de potencia. Mientras caminas por la calle, alguien te quita el teléfono de la mano. Es importante hacer una copia de seguridad de sus datos y proporcionar borrados remotos cuando sea posible.

Evaluación Módulo 3

Ingresa a la evaluación del Módulo 3

Recuerda descargar la Guía de estudio para que puedas tomar notas.

Contesta las 8 preguntas que vienen en el Examen.

Para que puedas acreditar el módulo necesitas tener una calificación mínima aprobatoria de 8.0

Módulo 4: Ciberdefensa

Introducción

Cuanto más interconectado está el mundo digital, mayores son los peligros a los que se exponen, tanto particulares como empresas en la Red. Por tanto, la ciberseguridad en sectores como la tecnología de la información y de la comunicación resulta fundamental. Por esa razón, te presentamos algunas herramientas básicas para garantizar la seguridad informática y protegerse de los ataques en internet.

¿Qué es la ciberseguridad y cómo se puede aplicar?

El aumento del uso diario de dispositivos digitales y la interconexión entre ellos obliga a prestar especial atención a la seguridad informática. Para ello, tan sólo es necesario visualizar cuántos datos se procesan cada día en el ordenador, en la Tablet o en el Smartphone, cuántas cuentas se utilizan en las diferentes aplicaciones de las diversas plataformas de Internet y qué cantidad de datos bancarios y de crédito e información sensible se consultan. Todos estos datos son susceptibles de ataques y sin protección, están expuestos a las acciones de los cibercriminales.

¿Cómo bloquear el robo de datos?

Para evitar en la medida de lo posible la ciberdelincuencia sólo es necesario seguir una serie de pautas muy básicas y sencillas pero efectivas para ponérselo muy difícil a los ladrones de datos. Aquí te mostramos algunas:

- ✓ Instalar gadgets. Los soportes para tarjetas de crédito de plomo reforzado, por ejemplo, permiten prevenir el robo offline de datos y dificultar el acceso a información sensible.
- ✓ Insertar contraseñas seguras. Aunque parece un consejo obvio es el método de protección más sencillo y efectivo, ya sea, para impedir que un usuario inicie un ordenador ajeno o para bloquear a un hacker que intenta acceder una cuenta de correo electrónico.
- ✓ Utilizar cortafuegos. Este puede estar instalado en el ordenador o en el router. El firewall evita el acceso no autorizado al propio ordenador o a la propia red. Además, por medio de los ajustes correspondientes, se puede configurar qué personas o qué programas pueden acceder a Internet desde la red.
- ✓ Tener un antivirus. No sólo ofrece protección contra virus, troyanos y otro tipo de malware, sino que también los elimina en el acto. Es importante realizar análisis regulares en el ordenador o en la red para obtener un nivel de ciberseguridad óptimo.

Evitando ciberataques

Para garantizar la seguridad informática en cualquier otro entorno, además de herramientas especiales de ciberseguridad, es recomendable recurrir a una serie de trucos y buenas prácticas que han demostrado su eficacia durante años.

1. Tener el sistema operativo siempre actualizado

Instalar la versión más actual del sistema operativo y de las aplicaciones, portátiles, Tablet o Smartphone es fundamental, pues los programas anticuados son más susceptibles a los ataques.

2. Configurar la última versión de antivirus y firewalls

De esta manera se evitan peligros cotidianos y los de gran envergadura en empresas o puestos de trabajo equipados con ordenadores.

3. Controlar qué personas tienen acceso a datos

No perder nunca de vista a las personas que puedan acceder o editar ciertos datos de nuestra empresa. Los logs suelen ser de utilidad para vigilar qué usuarios han estado activos y cuándo, para descubrir y hacer un seguimiento de las irregularidades en caso de caída.

La ciberseguridad no es un tema sencillo. Independientemente del nivel de minuciosidad con el que se puedan implementar las medidas de protección en Internet y en otros sectores del entorno digital, siempre surgen brechas y debilidades de las que los atacantes se aprovechan con métodos sofisticados. Por lo que instalar herramientas para impedir ciberataques tanto en el ámbito laboral como en el privado es fundamental.

Amenazas más comunes

A pesar de que los ataques informáticos están a la orden del día y se van renovando de forma continua, podemos decir que existen varias amenazas que son comunes y habituales dentro de este sector. Nos estamos refiriendo a la ciberguerra, el ciberterrorismo y el cibercrimen. ¿En qué consiste cada una de estas amenazas?

Ciberguerra: Se trata de un ataque cuya finalidad por norma general es política. En este contexto, los ciberdelincuentes intentan recopilar el mayor número de información posible y datos relevantes que puedan comprometer, en un futuro, a un partido político o un gobierno.

Ciberterrorismo: Es otra forma de amenaza común, pero en esta ocasión, aunque también se intenta recopilar el máximo de información, la finalidad es diferente, puesto que el objetivo es crear un ambiente de terror entre los ciudadanos. Uno de los grandes miedos de la sociedad actual es perder la estabilidad debido a ello.

Cibercrimen: El cibercrimen es una de las amenazas más comunes y la que más se suele producir en todo tipo de países. A través de ella, los hackers acceden a sistemas informáticos protegidos e intentan obtener ganancias financieras. También se realiza a nivel de usuario, tomando el control de dispositivos concretos y solicitando cantidades económicas a cambio de su liberación entre otras posibilidades.

Fases de la ciberseguridad

Protegerse ante los peligros de la era actual implica llevar a cabo procesos de ciberseguridad que se sustenten sobre su efectividad y para hacerlo, hay que conocer las fases en las que aplicarlos. Podemos dividir el proceso en tres fases concretas que suelen ser temario habitual del máster en seguridad empresarial: prevención, localización y reacción.

1. Prevención

El primer paso siempre es la prevención, lo que reducirá en gran medida el margen de riesgo. Por ello, hay que actuar de forma temprana e informarnos de todo lo que puede ocurrirle a nuestro sistema. Determinar las posibles amenazas y cuáles serán las medidas de prevención y reacción en caso de vernos afectados por una de ellas, nos permitirá estar más preparados.

2. Localización

Después de prevenir, en el caso de haber sufrido algún tipo de problema, habrá que localizar dónde radica el problema. Para ello la mejor herramienta es disponer de un antivirus potente que nos ayude a detectar el ataque en tiempo real y concentrarnos en él de inmediato. Localizar el ataque o la infección no es tan fácil como pueda parecer, dado que los hackers son conscientes del uso de los antivirus y lo que hacen es trabajar de manera que sus ataques puedan

pasar desapercibidos. En algunos casos, desde el momento en el que se produce el golpe hasta lo detectan, pueden pasar más de 100 días. Para intentar reducir en la medida de lo posible este problema, hay que concentrarse en dos aspectos: *gestionar las vulnerabilidades de nuestro sistema y por otro llevar a cabo una monitorización de forma continua*.

3. Reacción

Una vez que hemos localizado la amenaza, tendremos que dar una respuesta técnica sobre la misma y para ello lo ideal es seguir cuatro pasos.

1- Desconectar los equipos de la red.
2- Instalar un antivirus que pueda satisfacer las necesidades o actualizar el que ya teníamos.
3- Análisis sobre el sistema y hacer cambios de todas las contraseñas.
4- Realizar una limpieza a fondo del sistema para comprobar que ya no existe ningún tipo de peligro.

En el caso de que nos hayan robado datos o información confidencial, también deberemos proceder de la manera pertinente para comunicarlo a los usuarios afectados y elevar lo ocurrido a una situación de delito informático.

Las intrusiones informáticas

En el mundo informático ocurre una lucha permanente entre las vulnerabilidades de seguridad y los distintos métodos para evitarlas. Es por ello que los hackers o piratas informáticos buscan aprovecharse de cualquier falla para realizar sus ataques.

Precisamente, la mayoría de las víctimas de estas amenazas son los usuarios empresariales, ya que sus negocios manejan grandes volúmenes de datos, además de contar con más recursos económicos que un usuario particular.

De hecho, en muchas ocasiones, los ciberdelincuentes actúan para extorsionar a sus víctimas, y obtener algún beneficio económico.

Por lo tanto, la vía más idónea para realizar sus ataques es por medio de una intrusión informática, es decir, un ingreso no autorizado a un sistema, red o

dispositivo. Para lograrlo, se aprovechan de diferentes técnicas, algunas muy básicas, y otras realmente complejas.

Lo cierto, es que los proveedores de seguridad informática han logrado desarrollar diferentes herramientas para combatir las intrusiones. Una de las más usadas en la actualidad es el sistema de detección de intrusiones, también conocido como IDS, por sus siglas en inglés. Veamos entonces en qué consiste el IDS.

Conociendo el sistema de detección de intrusiones (IDS)

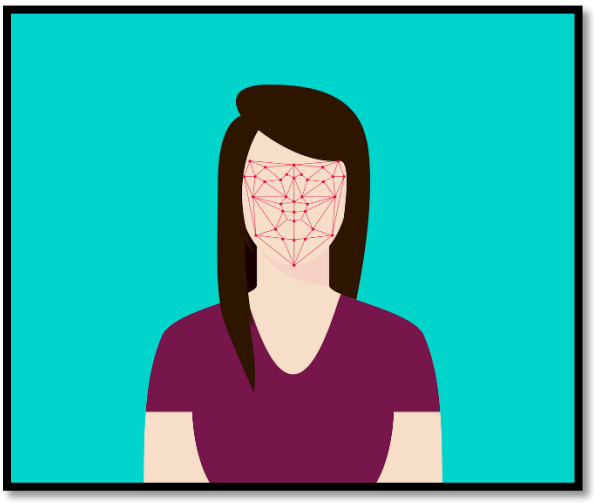
En primer lugar, se debe tener claro que un IDS es una herramienta informática bastante sofisticada, que se encarga de analizar el tráfico existente en una red. Como resultado, logra detectar movimientos sospechosos que pudiesen conducir a una intrusión.

Detección de intrusión

En la sociedad de la información en la que vivimos, es muy importante mantener seguras nuestras redes. Las empresas se esfuerzan en contener y evitar ataques que puedan poner en peligro esa información confidencial. Para ello, existen una serie de herramientas que intentan hacer lo más invulnerable posible nuestro sistema.

Actualmente, existen muchos Sistemas de Detección de Intrusiones (IDS), que van desde sistemas antivirus hasta sistemas jerárquicos, que monitorizan el tráfico de la red. Los más comunes son los siguientes:

- **NIDS**: Los sistemas de detección de intrusiones de red se colocan en puntos estratégicos de la red para supervisar el tráfico entrante y saliente de todos los dispositivos de la red. Pero la exploración de todo el tráfico podría conducir a la creación de cuellos de botella, lo que afecta a la velocidad general de la red.
- **HIDS**: Los sistemas de detección de intrusiones del host se ejecutan en máquinas o dispositivos separados de la red y proporcionan salvaguardias a la red general contra amenazas procedentes del exterior.
- **IDS basados en firmas**: Los IDS basados en firmas supervisan todos los paquetes de la red y los comparan con la base de datos de firmas, que son patrones de ataque preconfigurados y predeterminados. Funcionan de forma similar al software antivirus.
- **IDS basados en anomalías**: Estos IDS monitorean el tráfico de red y lo comparan con una línea de base establecida. La línea base determina lo que se considera normal para la red en términos de ancho de banda, protocolos, puertos y otros dispositivos, y el IDS alerta al administrador de todo tipo de actividad inusual.
- **IDS Pasivo**: Este sistema IDS realiza el sencillo trabajo de detección y alerta. Simplemente alerta al administrador de cualquier tipo de amenaza y bloquea la actividad en cuestión como medida preventiva.
- **Identificación reactiva**: detecta actividad malintencionada, alerta al administrador de las amenazas y también responde a esas amenazas.



Evaluación Módulo 4

Ingresa a la evaluación del Módulo 4

Recuerda descargar la Guía de estudio para que puedas tomar notas.

Contesta las 10 preguntas que vienen en el Examen.

Para que puedas acreditar el módulo necesitas tener una calificación mínima aprobatoria de 8.0

Bibliografía consultada

López, J. (05 de mayo de 2020). Ciberseguridad y su impacto en distintos sectores. El Economista. Website: https://www.eleconomista.com.mx/opinion/Ciberseguridad-y-su-impacto-en-distintos-sectores-20200505-0105.html

Nieto, E. (19 de febrero de 2018). El impacto de la ciberseguridad. Súmate Blog. Website: https://www.sumate.eu/blog/impacto-ciberseguridad/

Destino Negocio Mx (2015). El sector educativo también sufre los efectos de la ciberseguridad. Destino Negocio. Website: https://destinonegocio.com/mx/gestion-mx/sector-educativo-tambien-sufre-los-efectos-de-la-ciberseguridad/

Kaspersky Lab (2020). Las 7 principales ciberamenazas a las que hay que prestar atención. Kaspersky. Website: https://www.kaspersky.es/resource-center/threats/top-7-cyberthreats

Malwarebytes (2020). Malware. Malwarebytes. Website: https://es.malwarebytes.com/malware/

Net Cloud Engineering (16 de junio de 2017). Ciberseguridad: Amenaza vs. Vulnerabilidad. Net Cloud Engineering. Website: https://netcloudengineering.com/ciberseguridad-amenaza-vulnerabilidad/

Ciberseguridad (junio de 2016). Seguridad en la Red. Ciberseguridad. https://ciberseguridad.com/normativa/espana/medidas/seguridad-red/#%C2%BFQue_supone_una_amenaza_para_la_red

Izertis (2018). Ciberseguridad: qué es y cómo aplicarla para proteger a tu empresa. Izertis. Website: https://www.izertis.com/es/-/blog/ciberseguridad-que-es-y-como-aplicarla-para-proteger-a-tu-empresa

OBS (2020). ¿Qué es ciberseguridad y de qué fases consta? OBS Business School. Website: https://obsbusiness.school/es/blog-investigacion/sistemas/que-es-ciberseguridad-y-de-que-fases-consta

USS (20 de febrero de 2019). Sistema de detección de intrusos: tipos y ejemplos. USS. Website: https://uss.com.ar/preguntas-frecuentes/sistema-de-deteccion-de-intrusos/

Glosario

A

Antivirus: programa diseñado para detectar, detener y remover códigos maliciosos.

Ataque de "agujero de agua" o "watering": creación de un sitio web falso o comprometer uno real, con el objetivo de explotar a los usuarios visitantes. Se trata de un tipo de ataque informático.

Autenticación: Procedimiento para comprobar que alguien es realmente quien dice ser cuando accede a un ordenador o a un servicio online.

B

Biometría: Método de reconocimiento de personas basado en sus características fisiológicas como la huella dactilar, iris, cara, o en su comportamiento (firma, forma de andar…).

BOTNET: Red de dispositivos infectados que tienen conexión a internet, utilizados para cometer ciberataques coordinados y sin el conocimiento de sus dueños.

C

Centro Especializado en Respuesta Tecnológica (CERT): nombre que reciben aquellos equipos de respuesta a emergencias cibernéticas, cuyos integrantes realizan un permanente monitoreo de la red para identificar y mitigar tanto amenazas como ataques cibernéticos contra infraestructuras tecnológicas.

Ciberataque: intentos maliciosos de daño, interrupción y acceso no autorizado a sistemas computacionales, redes o dispositivos por medios cibernéticos.

Ciberguerra: Término se utiliza para designar ataques, represalias o intrusión ilícita en un ordenador o en una red.

Ciberseguridad: Protección de dispositivos, servicios o redes, así como la protección de datos frente a intentos de robo o daño.

Códigos maliciosos: Programas diseñados para infiltrarse en los sistemas y ocasionar daños en los dispositivos electrónicos como ordenadores, tabletas, Smartphones, alterando su funcionamiento y poniendo en riesgo la información de los usuarios.

Contraseña segura: Clave de identificación virtual que permite acceder a la información privada que se almacena en dispositivos electrónicos o servicios en línea como el correo electrónico, las redes sociales, la banca en línea. En términos generales, para que esta sea segura se recomienda que está compuesta por una combinación de ocho caracteres intercalando mayúsculas, minúsculas, números y símbolos.

Cortafuegos o Firewall: Hardware o software que utiliza un conjunto de reglas definidas para restringir el tráfico de la red e impedir accesos no autorizados.

D

Denegación del servicio o DoS: denegación a un usuario legítimo de acceder a servicios de cómputo o recursos, resultado de la saturación de número de solicitudes de servicio.

Día Cero: vulnerabilidades recientemente descubiertas, aún no conocidas por los vendedores o compañías antivirus, que los delincuentes pueden explotar.

Dispositivo de Usuario Final: término utilizado para describir a los teléfonos celulares inteligentes o Smartphone, computadoras portátiles y tabletas electrónicas que se conectan a la red de una organización.

E

Encriptación: Función matemática que protege la información haciéndola ilegible excepto para quienes tengan la clave.

F

Fraude contra Directores Ejecutivos o CEO Fraud: ataques de phishing distribuidos a través de correos electrónicos, orientados a altos ejecutivos de una organización.

H

Herramientas de protección en línea: Programas que al instalarlos protegen los dispositivos electrónicos con los que se navega en internet.

Huella digital: rastro de información digital que el usuario deja durante sus actividades en línea.

Huella digital en Internet: Rastro de información digital que el usuario deja mientras navega por Internet.

I

Identidad digital: Es lo que somos para otros en la red; un perfil que se crea de cada usuario a partir de la información que se almacena en la red.

Ingeniería social: Técnicas utilizadas para manipular a la gente a fin de que realice acciones específicas o se sume a la difusión de información que es útil para un atacante.

Internet de las cosas o IoT: es la capacidad que tienen otros objetos, distintos a las computadoras y dispositivos móviles, de conectarse a internet.

L

Lista Blanca: listado de programas aprobados y autorizados para ser utilizados al interior de una organización con el fin de proteger los sistemas de aplicaciones potencialmente dañinas.

M

Macro: programa que puede automatizar tareas en aplicaciones, que a su vez es útil para que los atacantes puedan acceder o dañar un sistema.

Malware: Abreviatura de Malicious Software que hace referencia a todos los programas o códigos informáticos cuya función es dañar o causar el mal funcionamiento de un sistema

N

Nube: lugar en el que la información es almacenada y compartida, en lugar de su resguardo de manera física, como a través de discos compactos, memorias usb, discos duros, etcétera.

P

Parche: Actualizaciones de seguridad que permiten mejorar la misma y el funcionamiento de un software.

Phishing: Envío masivo de mensajes de correo electrónico con el objetivo de apropiarse de información confidencial de los usuarios o incitarlos a visitar sitios web falsos.

Política BYOD (Brign Your Own Devices): estrategia o política de una organización que permite a sus empleados llevar al centro de trabajo sus propios dispositivos con fines laborales.

Privacidad en redes sociales: mecanismos de protección de datos íntimos o confidenciales en un perfil de red social de una persona, con la finalidad de no exponerlos abiertamente y evitar que alguien los utilice de forma negativa.

R

Ransomware: Códigos maliciosos creados por ciberdelincuentes que bloquean el acceso a los dispositivos de los usuarios para después pedirles un pago a las víctimas para recuperar su información.

S

Seguridad de la Información: Medidas de protección enfocadas a preservar la confidencialidad, integridad y disponibilidad de la información.

Software como Servicio o SaaS: se describe como un modelo de negocio en el que consumidores acceden a aplicaciones de software alojadas a través de internet.

Spear-Phishing: Ataque dirigido de phishing, que se lleva a cabo una vez que el delincuente ha estudiado a su posible víctima a través de mensajes de correo electrónico muy específicos.

Suplantación de Identidad o Phishing: es el envío masivo de mensajes de correo con el objetivo de obtener información confidencial de los usuarios o incitarlos a visitar sitios web falsos.

T

Troyano: Código malicioso con apariencia de software fiable que se oculta en el sistema para infectarlo.

AlfaDigital
Dirección de Alfabetización Digital

Recrea
Educación para refundar 2040

Educación

Jalisco
GOBIERNO DEL ESTADO

AlfaOnline