Fundamentos básicos de los conceptos de ataques informáticos

Contenido

Lista de figuras

Introducción

En esta actividad de aprendizaje, se proporciona a los aprendices los conceptos básicos sobre los ataques informáticos a los que están expuestas las empresas, se darán a conocer los posibles daños que causan a la información y algunas recomendaciones para evitar estos ataques a las empresas.

Mapa conceptual

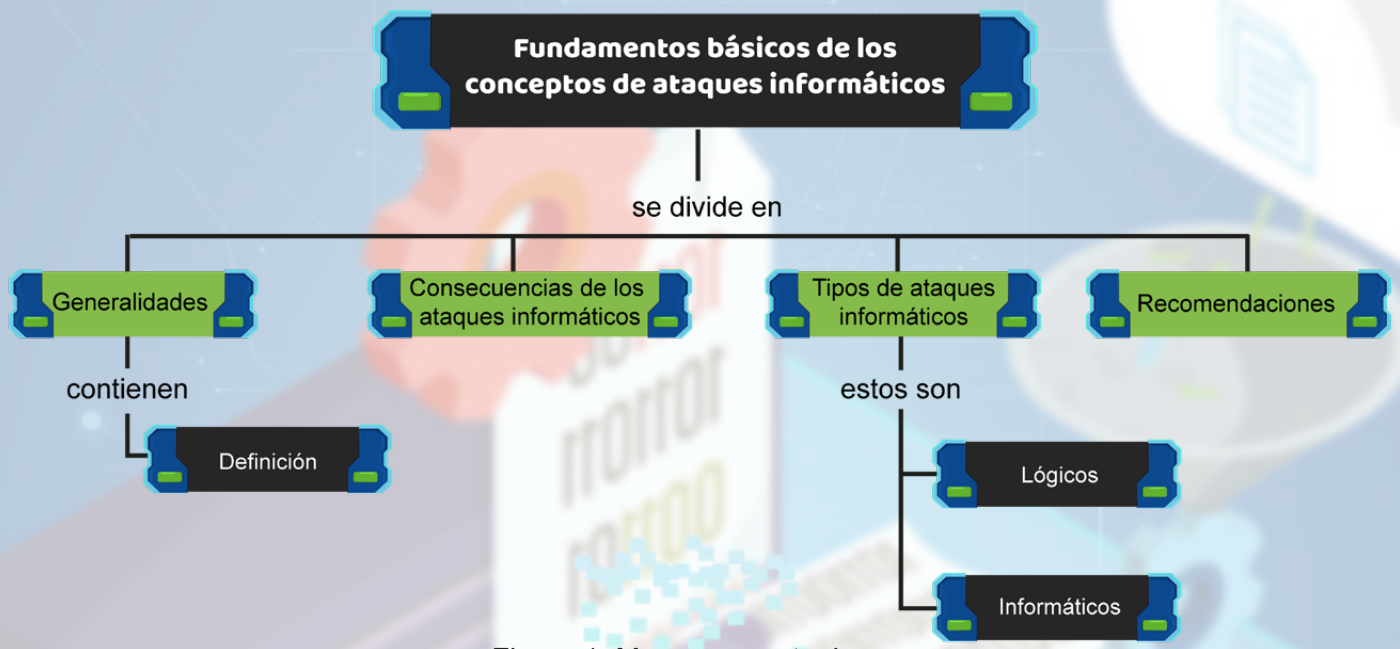

Figura 1. Mapa conceptual
Fuente: SENA (2019)

1. Generalidades

1.1 Definición de ataques informáticos

Figura 2. Pirata informático
Fuente: SENA (2019)

Un ataque informático, también denominado cibernético, es aquel método o procedimiento por medio del cual un grupo de personas, con conocimientos de sistemas y a quienes se les denomina piratas informáticos trata de tomar control de la información de un sistema o de la red, con el fin de hacer daño parcial o total.

El ataque más común que se conoce son los virus informáticos, que se transmiten a través de memorias USB y correos electrónicos maliciosos. Estos son capaces de dañar información del equipo e incluso generar daño total del disco duro, impidiendo la recuperación de la información.

2. Consecuencias de los ataques informáticos

Daños triviales

Son daños que el virus puede generar, pero se logran eliminar con facilidad y no requiere de muchos esfuerzos especiales para ello, solo un poco de tiempo.

Daños menores

En este tipo de daños, el virus ataca especialmente a los programas o aplicativos del sistema borrándolos por completo. Un ejemplo es el virus Jerusalén.

Daños moderados

El daño que produce el virus está directamente dirigido al disco duro, formateándolo por completo o sobreescribiendo información.

Daños mayores

El virus ataca un sector del disco duro dañando los archivos que reposan en él. *Dark Avenger* es un ejemplo.

Daños severos

Los virus atacan a los archivos del sistema, realizando cambios mínimos o progresivos en ellos y el usuario no puede identificar el archivo original del modificado.

Daños ilimitados

Este virus ataca al administrador del sistema, creando un nuevo usuario con su nombre y contraseña para tener privilegios de administrador. *Cheebas* es un causante de este ataque.

3. Tipos de ataques informáticos

3.1. Lógicos

Trashing (cartoneo)

Se presenta por descuido de las personas al escribir el usuario y contraseña en un papel y abandonarlo en cualquier lugar, lo que posibilita que un atacante utilice esta información para el acceso de los archivos de un computador.

Figura 3. Ataque
Fuente: SENA (2019)

Ataques de monitorización

El atacante mediante observación directa de la víctima, logra conseguir las contraseñas de entrada a los sistemas, para acceder en cualquier oportunidad y atacar la información.

Ataques de autenticación

Este ataque informático se hace a través de correos electrónicos falsos, donde se logra obtener el nombre del usuario y su respectiva contraseña para el acceso a información.

3.2. Informáticos

Malware

Se trata de *software* maliciosos que atacan directamente a los archivos volviéndolos ejecutables e impidiendo el acceso a ellos.

Ataque DDoS

Se conoce con el nombre denegación del servicio distribuida y su objetivo es bloquear el acceso a las páginas web. Al mismo tiempo ataca el servidor llenándolo de basura informática, responsable de impedir el ingreso a la web.

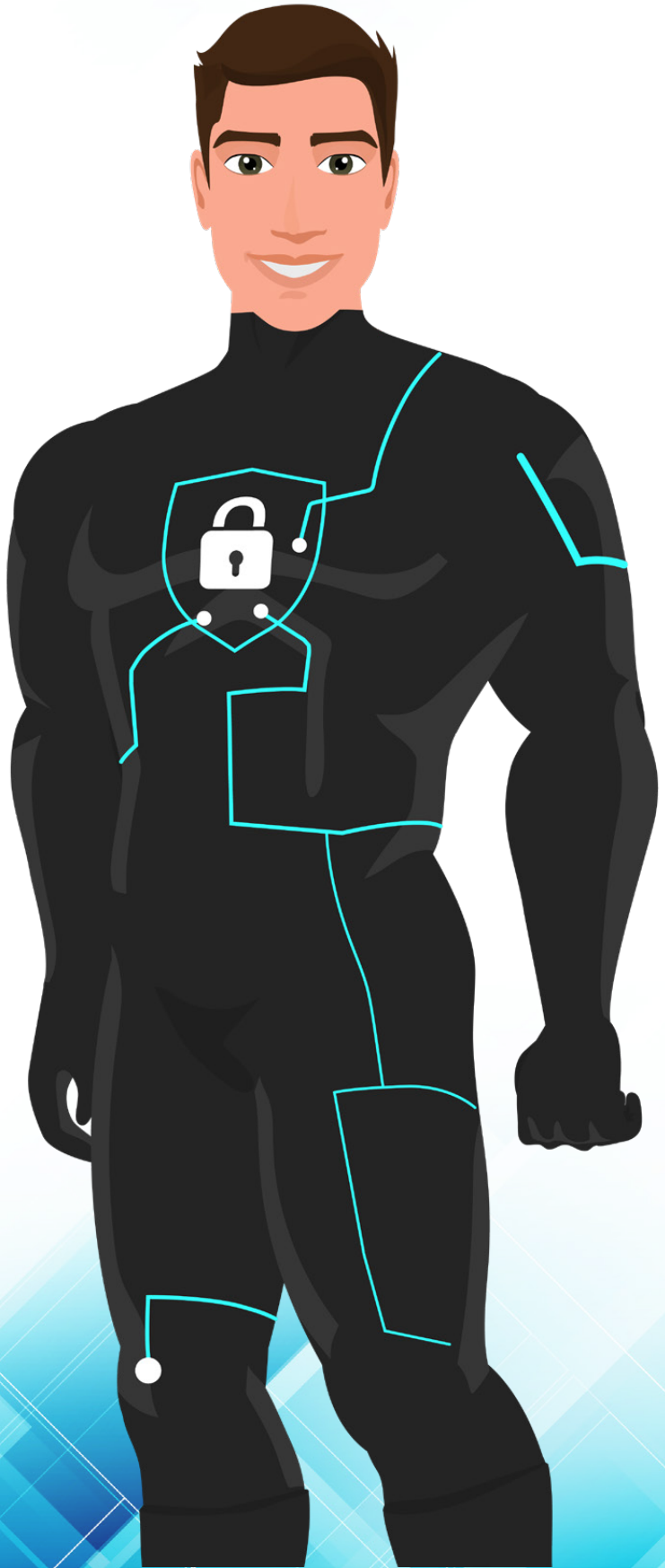

Figura 4. *Phishing*

Fuente: SENA (2019)

Figura 5. *Baiting*

Fuente: SENA (2019)

Phishing

Consiste en la suplantación de la identidad de un usuario a través de los correos electrónicos. El objetivo es obtener datos personales o bancarios.

Baiting

El ataque de equipos y redes de información se llevan a cabo a través de medios extraíbles como memorias USB y discos duros externos, los cuales al ser conectados transmiten el virus provocando la pérdida de información.

4. Recomendaciones para prevenir los ataques informáticos

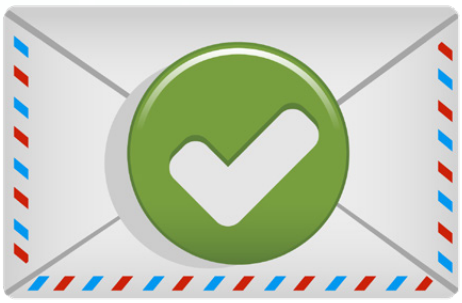

Figura 6. Correo electrónico

Fuente: SENA (2019)

Figura 7. Contraseña

Fuente: SENA (2019)

Verificar el origen de correos electrónicos

Los correos electrónicos son los medios más eficaces que las empresas utilizan para enviar y recibir información, por esta razón se debe sugerir a los usuarios de la empresa, que antes de dar respuesta a los correos electrónicos se percaten del origen del mismo, puesto que los piratas informáticos comprueban que el correo esté activo y así proceden a atacar la información.

Contraseñas de acceso

Son las llaves para estar en contacto con la información de la empresa, estas deben ser seguras y tener combinaciones de caracteres especiales, como por ejemplo letras mayúsculas y minúsculas. Se sugiere realizar el cambio de estas con frecuencia, de esta manera será difícil para los atacantes informáticos descifrarlas.

Figura 8. Copias de seguridad

Fuente: SENA (2019)

Figura 9. Antivirus

Fuente: SENA (2019)

Realizar copias de seguridad

La copia de seguridad o *backup* es una de las formas de seguridad utilizadas para no perder información. Estas deben estar actualizadas en un tiempo menor de un mes, la copia se debe realizar en servidores o en la nube que la empresa tenga disponible.

Instalar un antivirus seguro

Los antivirus son aplicaciones que protegen la información de atacantes externos como las memorias USB. Deben ser licenciados para actualizarlos y que cumplan con la función de detectar virus. Al momento de introducir una memoria se recomienda que esta sea examinada y desinfectada mediante el antivirus.

Figura 10. Capacitación

Fuente: SENA (2019)

Figura 11. Computadores

Fuente: SENA (2019)

Capacitaciones a los usuarios sobre los ataques informáticos

Es un deber del departamento de sistemas de la empresa, dar información periódica de los riesgos que pueden generar la pérdida de archivos y a través de talleres capacitar al personal sobre las diferentes maneras de prevenir los ataques informáticos.

Los computadores deben ser de uso exclusivo de la empresa

Se deben crear políticas de seguridad, las cuales aclaren que los computadores de la empresa son de uso exclusivo y para fines de la compañía.

Referentes bibliográficos

Equipo editorial. (2018). *10 consejos para evitar un ataque cibernético empresarial*. Recuperado de https://reportedigital.com/seguridad/ataque-cibernetico-empresa-consejos/

Freepik. (s.f.). *Pirata informático*. Recuperado de https://www.freepik.es/vector-premium/pirata-informatico-robar-datos-confidenciales_2156268.htm

Globalfinanz. (s.f.). *Empresas expuestas a ataques informáticos o cibernéticos*. Recuperado de https://www.responsabilidadconsejerosydirectivos.com/ataques-ciberneticos-en-las-empresas/

Impulsapopular. (2007). *¿Cómo prevenir la fuga de datos empresariales a través de sistemas informáticos?* Recuperado de https://www.impulsapopular.com/tecnologia/como-prevenir-la-fuga-de-datos-empresariales-a-traves-de-sistemas-informaticos/

Créditos

Gestor del proceso de recursos digitales

Juan Bautista Londoño Pineda

Responsable de producción y creación

Jhoana Andrea Vásquez Gómez

Evaluador de calidad instruccional

Erika Alejandra Beltrán Cuesta

Desarrollador de contenidos

Olga Elena Meneses Camino

E-pedagogo instruccional

Juan Carlos Ramírez Molina

Evaluador de contenidos

Lina Marcela Cardona Orozco

Creativo de recursos didácticos

Cristian Andrés Osorio Caiza

Carlos Andrés Díaz Botero

Carolina Ramírez Martínez

Melissa Ochoa Alvarado

Desarrollador Full-Stack

Daniel Enciso Arias

Francisco José Lizcano Reyes

Luis Felipe Zapata Castaño

Luis Gabriel Urueta Álvarez

Germán Alberto Rodríguez Lievano

Leyson Fabián Castaño Pérez

Centro Agroindustrial - Regional Quindío

Centro Agropecuario - Regional Risaralda

2019