INSTRUMENTO DE EVALUACIÓN

Proceso: Ejecución de la Formación
Procedimiento: Desarrollo Curricular

SENA REGIONAL CAUCA: Centro de Comercio y Servicios

1. IDENTIFICACIÓN DEL INSTRUMENTO:

Programa de Formación: Control De La Seguridad Digital

Código: 233103

Competencia a Desarrollar: 220501108. Diagnosticar la seguridad de la información de acuerdo con métodos de análisis y normativa técnica.

Resultado(s) de Aprendizaje :

- Preparar los instrumentos y técnicas de recolección de información de acuerdo con el modelo de negocio.
- Interpretar la política de seguridad y privacidad de la información según el modelo de
- Realizar el inventario de activos tecnológicos relacionados con el manejo de la información aplicando técnicas e instrumentos definidos por la organización.
- Documentar el proceso de realización de inventario según procedimientos establecidos por la organización.

Nombre del Aprendiz:
Nombre del Instructor: Sandra Yineth Macias
Duración de la evaluación: 48 Horas

2. INSTRUCCIONES PARA EL DILIGENCIAMIENTO:

Tengan todos un placentero día, el motivo de este instrumento es para evidenciar el proceso de aprendizaje:

1. Ejecución

Seguridad informática básica a nivel de usuario

1. Introducción
2. Amenazas físicas y su prevención
3. Amenazas lógicas y su prevención
4. Principales amenazas lógicas

1. Introducción

La seguridad informática se define como las medidas necesarias para que la información esté siempre disponible (disponibilidad), que sólo pueda ser accesible o estar al alcance del personal autorizado (confidencialidad), que sólo pueda ser modificada por personal autorizado (integridad), que cualquier persona que interactúe con dicha información debe estar siempre identificado (autenticación) y no pueda negar ser el autor de una acción (irrefutabilidad).

Una vez que sabemos, *grosso modo*, en qué consiste la seguridad informática, debemos distinguir entre los dos tipos de amenazas que existen:

- Físicas
- Lógicas

2. Amenazas físicas y su prevención

Todas pueden ocasionar pérdida de datos/información. Se recomienda siempre tener copia de seguridad de toda la información.

Incendio

- Medidas preventivas: no saturar enchufes; alejar fuentes de calor de materiales inflamables
- Medidas para minimizar su efecto: contar con equipos contraincendios (por ejemplo, extintores del tipo adecuado)

Inundación

- Medidas preventivas: realizar mantenimiento de infraestructuras periódicamente; cerrar correctamente puertas y ventanas para evitar la entrada de lluvia; tener el PC en lugar elevado.
- Medidas para minimizar su efecto: cuando la electrónica se moja, es muy difícil recuperar el dispositivo, pero sí podríamos sacar el disco e intentar rescatar los datos.

Temperaturas extremas

Tanto las temperaturas muy altas, como muy bajas, pueden ocasionar daños a los componentes electrónicos de los equipos. Lo recomendable es mantener una temperatura constante (sobre todo en armarios de comunicaciones).

- Medidas preventivas: equipos de aire acondicionado/climatizadores; no tapar las salidas del aire caliente de los PCs; si hay más de un equipo en el puesto, mantenerlos a cierta distancia entre ellos

Corte del suministro eléctrico

- Medidas preventivas: realizar mantenimiento de infraestructuras periódicamente; contar con Sistemas de Alimentación Ininterrumpida (SAI), que pueden aportar electricidad a los equipos por un periodo corto de tiempo, hasta que se restablezca el suministro.
- Medidas para minimizar su efecto: si tenemos SAI, podemos configurar que el equipo se apague cuando falte corriente, así no perdemos datos.

Picos de tensión

- Medidas preventivas: contar con una fuente de alimentación o con un SAI que sea capaz de manejar las fluctuaciones en la entrada de corriente

Robo

Además de la pérdida de información, supone que dicha información pasa a manos no deseadas.

- Medidas preventivas: instalar cerradura en cada entrada a despacho, aula, dependencia…; cerrar con llave el despacho/dependencia cuando no haya nadie; no permitir el acceso a toda persona ajena.
- Medidas para minimizar su efecto: tener usuario con contraseña; tener cifrado los ficheros/archivos más importantes para que nadie tenga acceso a ellos sin la clave privada/contraseña.

Destrucción deliberada

- Medidas preventivas: las mismas que para el *Robo*

Desastre natural

- Medidas para minimizar su efecto: no hay mucho que se pueda hacer, salvo tener todo replicado en un lugar que se haya salvado del desastre.

3. Amenazas lógicas y su prevención

Las amenazas lógicas se aprovechan de las vulnerabilidades (agujeros de seguridad) que pueda tener nuestro sistema/red. Su fin es acceder o conseguir información que para nosotros es valiosa. Raro sería que entraran en nuestro equipo sólo para destruir la información sin más (cosa que podría darse si lo que se quiere es eliminar pruebas necesarias en alguna situación concreta).

Se recomienda tener siempre actualizado el Sistema Operativo y el resto de aplicaciones, sobretodo ANTIVIRUS y ANTIMALWARE

De esta manera, conseguimos minimizar las posibilidades de acceder o entrar a nuestro PC sin nuestro consentimiento. A día de hoy, no hay programa antivirus o antimalware capaz de detectar y/o eliminar el 100% de las amenazas existentes, y cada día aparecen nuevas. De ahí que se deba actualizar las bases de datos de los antivirus siempre que se pueda, para estar preparado ante las nuevas formas de ataque que tienen los hackers[1].

Se recomienda tener siempre copia de seguridad o respaldo de nuestros datos. Nunca se sabe lo que puede pasar, o cuando los vamos a necesitar

4. Principales amenazas lógicas.

Errores de programación en nuestro software

Es suficiente con saber que, teniendo actualizadas las aplicaciones instaladas y el Sistema Operativo, la mayoría de los problemas que genera, se solucionan.

Malware o software malicioso

Es software creado específicamente para dañar el equipo, proporcionar acceso al mismo, destruir la información que contiene o robarla directamente. Como ya hemos mencionado, se aprovechan de vulnerabilidades del sistema provocadas por errores de programación; configuración deficiente por parte del usuario; desconocimiento y/o malas praxis del usuario. Estos son los más importantes:

- Virus
- Troyano
- Spyware

[1] informático que busca y detecta agujeros de seguridad o vulnerabilidades de nuestro Sistema

- Gusanos
- Exploits
- Ransomware
- Adware

Para evitar que nuestro equipo se vea afectado por alguno de ellos, es fundamental tomar una serie de medidas preventivas:

- Un usuario por cada persona que utilice el mismo equipo
- Usuario siempre con contraseña
- Contraseña difícil
- Cerrar sesión mientras no se está utilizando el PC
- Tener instalado, activo y actualizado un programa antivirus
- Realizar escaneos del sistema en busca de amenazas periódicamente
- Instalar y utilizar herramientas adicionales para buscar malware independientes al antivirus
- Navegar por páginas web seguras y de confianza
- Si descargamos algún archivo, que se haga desde una web segura y de confianza
- Escanear en busca de amenazas cualquier archivo que descarguemos

Phishing

Ésta es una amenaza que merece una mención aparte por su candente actualidad.

Phishing es un método de robo de información mediante suplantación de identidad.

Ejemplo:

Nos ha llegado un email en el que el banco X nos indica que, debido a un error, se ha generado a nuestro favor un saldo de 1.500€. Sólo necesitan que ingresemos en su página web para facilitar los datos de nuestra cuenta y nuestra tarjeta de crédito/débito.

Pensando que puede ser cierto, ya que el correo parece veraz (viene con el logo y datos del banco), hacemos clic en el enlace que nos mandan. Éste, nos lleva a una página web que es prácticamente igual que la oficial de dicho banco; por tanto, no sospechamos que sea fraudulenta.

Ingresamos los datos que nos han solicitado.

Ya tienen nuestra información.

También se puede dar el caso, que lo que nos mandan es algún archivo que hay que descargar. Lo mismo. Pensamos que es verdadero y lo descargamos. Lo ejecutamos.

Ya tienen acceso a nuestro sistema.

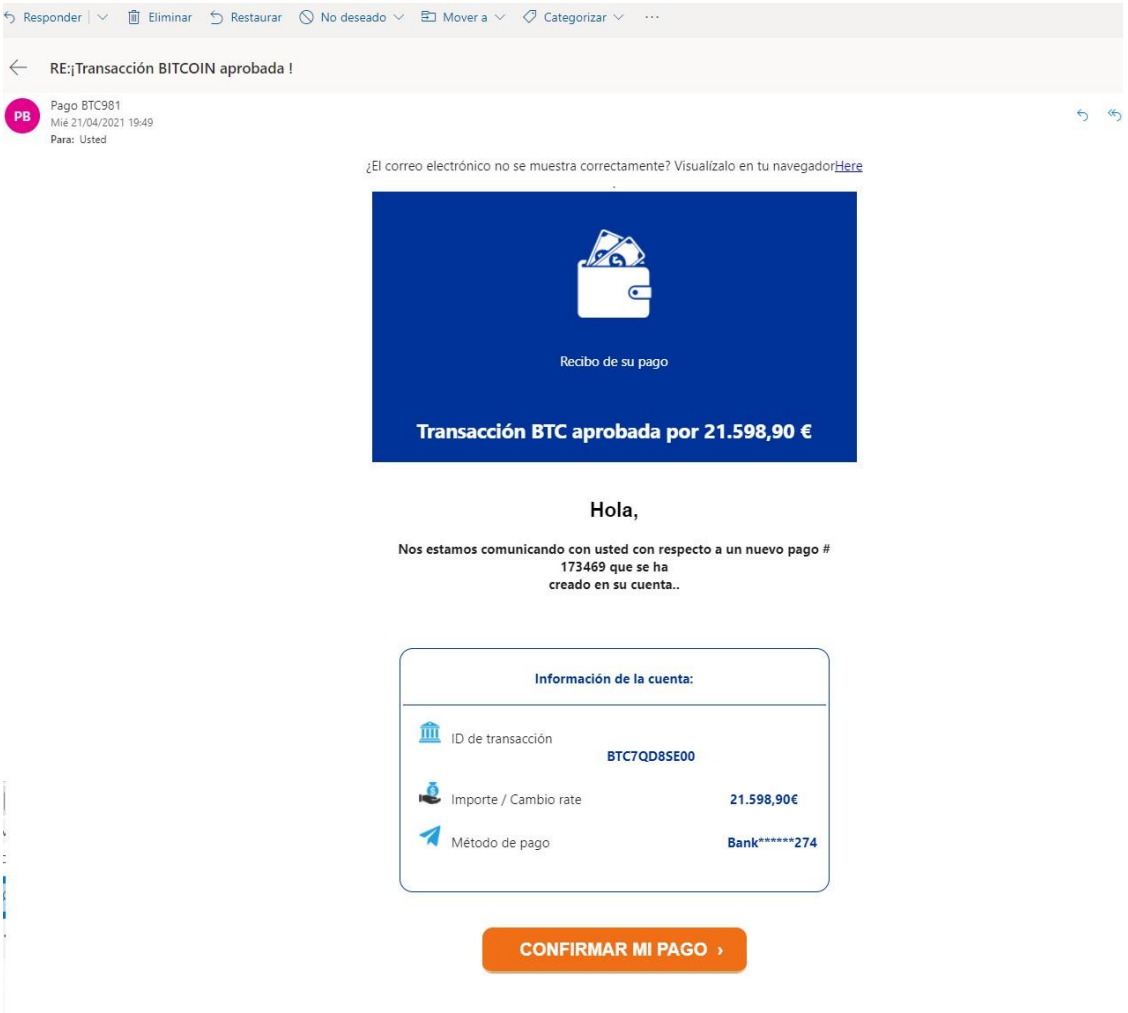


Fig. 1: Ejemplo de correo de phishing

Taller:

Teniendo en cuenta la lectura anterior conteste:

1. *¿Porque es tan importante la seguridad de la información?*

2. *¿Si fuera contratado en una empresa como técnico en seguridad informática que sería lo más importante que usted considere desde su rol debe de hacer?*

3. *¿Cuál considera es el problema mas grande de seguridad en una empresa y como haría para mitigar esa amenaza?*

4. *¿Usted como técnico cuales serían sus principales herramientas a utilizar para poder desempeñar bien su trabajo?*