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. **Análisis**

Estimado aprendiz este instrumento esta diseñado con fin de evaluar sus conocimientos de cada una de las actividades desarrolladas en le ambiente de formación. Apropiación de los conceptos sobre grandes avances tecnológicos, las empresas u organizaciones deben estar a la vanguardia en sus procesos informáticos, por lo cual deben asegurar su infraestructura computacional a través de todo su sistema de procesamiento y almacenamiento de datos de tal manera que se garantice la confidencialidad, integridad y disponibilidad de los mismos en el momento en que se requiera. La seguridad física y lógica de la información cada vez más está siendo amenazada por el incremento en los delitos informáticos y el terrorismo computacional, es por eso que las organizaciones se deben encontrar preparadas para no dejar ninguna vulnerabilidad en su sistemas y utilizar todos los recursos a su alcance para proteger todos los recursos computacionales y de información

3. Actividades de evaluación

1. ¿Qué es la seguridad informática y por qué es importante?
2. ¿Cuáles son las principales amenazas a la seguridad informática?
3. ¿Cuáles son las diferencias entre un virus, un gusano y un troyano?
4. ¿Qué es un ataque de fuerza bruta y cómo se puede prevenir?
5. ¿Qué es un ataque de phishing y cómo se puede detectar?
6. ¿Qué es el malware y cuáles son sus tipos más comunes?
7. ¿Cuáles son las mejores prácticas para crear contraseñas seguras?
8. ¿Qué es la autenticación de dos factores y cómo puede ayudar a mejorar la seguridad?
9. ¿Qué es una vulnerabilidad de día cero y cómo se puede abordar?
10. ¿Cuál es la importancia de mantener el software y los sistemas operativos actualizados?
11. ¿Qué es el cifrado y cómo se utiliza para proteger los datos?
12. ¿Cuál es la diferencia entre seguridad física y seguridad lógica?
13. ¿Qué es una política de seguridad de la información y por qué es necesaria?
14. ¿Cuáles son las medidas de seguridad que se pueden implementar en una red empresarial?
15. ¿Cómo se puede detectar si un dispositivo ha sido comprometido?
16. ¿Cuáles son los pasos que se deben seguir para responder a un incidente de seguridad informática?

17. ¿Qué es un cortafuegos (firewall) y cuál es su función principal?

18. ¿Cuál es la importancia de realizar copias de seguridad de los datos y cómo se pueden hacer de manera efectiva?

19. ¿Qué es un análisis de vulnerabilidades y cómo se puede llevar a cabo?

20. ¿Cuáles son las mejores prácticas para educar a los empleados sobre seguridad informática en una organización?

3. 1 Actividad de desempeño de conocimientos

Textos escritos:

❖ Ensayos que es la ingeniería Social

3.2 Actividad de desempeño de Desempeño

Esquemas, gráficos, mapas

3.3 Actividad de Producto

Lista de chequeo			
Criterio o actividad	Cumple	No Cumple	No aplica
¿Se entrega los ensayos de respuesta con respeto al termino ingeniera social?			
¿explica los conceptos básicos de ingeniería social			
¿Relaciona adecuadamente la consecuencias seguridad informática?			
¿Completa adecuadamente el organigrama de gestión de la información?			
¿ Completa adecuadamente el mapa conceptual de sistemas informáticos?			
¿Con le video seguridad de la información completa el cuadro según lo indicado en la guía?			
¿ Completa adecuadamente el diagrama Administración de la seguridad de la información?			

5. GLOSARIO DE TERMINOS

Activo (Asset): Un recurso, procedimiento, sistema u otra cosa que tenga un valor para una organización y por lo tanto deba de ser protegida, los Activos pueden ser

bienes físicos tales como equipos de cómputo y maquinaria, también puede ser la Información y propiedad intelectual.
Adware: Software legitimo pero molesto, es una característica que tienen algunos programas gratuitos o en fase de prueba que muestran publicidad, mensajes de activación o de compra, comúnmente el creador cobra por la publicidad que se muestra, los mensajes se muestran cuando esta en funcionamiento el software asociado.
Antivirus: Software diseñado para la detección, prevención y eliminación de Software mal intencionado o dañino para los sistemas.
Ataques de Diccionario: Es un tipo de ataque de fuerza bruta enfocado en el que se utiliza una lista predefinida de palabras. GFPI-F-019 V03
Ataque de Fuerza Bruta: Es un tipo de ataque que consiste en que el atacante intenta con todas las posibles combinaciones de letras, números y caracteres para acertar la contraseña, PIN o phassphrace.
Auditoría: La verificación independiente de cualquier actividad o proceso.
Autenticación: El procedimiento de verificar la identidad que reclama un sujeto mediante una validación en un sistema de control de acceso**.**
Autorización: Es el proceso de definir los derechos o permisos asignados a un sujeto (que puede hacer).
Baja de Voltaje (Brownout): Voltaje bajo de manera prolongada de una fuente de energía eléctrica, tal como la energía eléctrica del servicio público.
Biometría: Cualquiera de varios métodos utilizados como parte de un mecanismo de autenticación, para verificar la identidad de una persona. Los tipos de biometría utilizada incluye las huellas dactilares, impresiones de la palma de la mano, firmas, escaneos de retina, escaneos de voz y patrones de escritura en teclados.
Certificado Digital: Es un certificado que liga una identidad a una llave de cifrado pública.
Cifrado: El proceso de transformar texto plano a texto cifrado**.**
Cifrar: Una transformación criptográfica de texto claro a mensaje cifrado.
Confidencialidad: Previene del uso no autorizado o revelación de información, asegurándose que la información es accesible únicamente para aquellos que tengan autorizado su uso**.**
Controles Detectivos: Controles que identifican violaciones e incidentes.
Controles Disuasivos: Controles que desalientas la realización de violaciones.
Criptoanálisis: Es la ciencia de descifrar texto cifrado sin el uso de la llave criptográfica.
Criptografía: La ciencia de cifrar o descifrar información, tal como puede ser un mensaje privado para proteger su confidencialidad, integridad y / o autenticidad.
Criptología: La ciencia que abarca Criptografía y Criptoanálisis.
DDoS (Ataque distribuido de negación de Servicios): Es un tipo de ataque en el que el atacante inicia ataques de negación de servicio simultáneamente desde muchos sistemas. GFPI-F-019 V03
Defensa en profundidad (o en capas): Es el principio de proteger los activos (información, bienes físicos de la empresa, etc) por medio de utilizar varias capas de protección diferentes.
Descifrado: Es el proceso de transformar texto cifrado en texto plano.

Directrices (Guidelines): Documentos similares a Estándares, pero considerados recomendaciones, en lugar de un requisito forzosos.
Disponibilidad: El proceso de asegurar que los sistemas e información sean accesibles para usuarios autorizados cuando ellos lo requieran.
Due Care (Cuidado Necesario): Los pasos que toma una organización para implementar mejores prácticas de seguridad.
Due Diligence (Diligencia Debida): La prudente administración y ejecución de "Due Care".
Dumpster Diving (Buceo de Contenedores): El proceso de examinar basura con la intención de encontrar bienes valiosos o información.
Espionaje: La práctica de espiar o utilizar espías para obtener información propietaria o confidencial.
Firewall: Dispositivo o programa que controla el flujo de tráfico entre redes.
Firewall de Aplicaciones: Un Firewall que inspecciona la capa 7 del Modelo OSI (aplicación) con el objetivo de bloquear contenido malicioso antes de que alcancé o abandone el Servidor de Aplicaciones (portal web, base de datos, etc).
Forense (Informática Forense): La ciencia de conducir una investigación criminal computacional para poder determinar que sucedió o quien es el responsable por lo ocurrido.
Función Hash: Una función matemática que crea una representación única de un grupo grande de datos. Las funciones Hash son frecuentemente utilizadas en algoritmos criptográficos y para producir resúmenes de mensajes (Checksums and message digest).
Gateway: Un sistema conectado a una red de computadoras, el cual ejecuta cualquier traducción en tiempo real o funcionalidad de interfaz.
Honeypot: Un sistema señuelo instalado por un administrador de seguridad para descubrir los métodos de ataque de hackers potenciales. GFPI-F-019 V03
Hot Site: Una ubicación alterna a la de uso diario, con recursos computacionales totalmente funcionales que tiene servicios de electricidad, aire acondicionado, servidores de impresión, servidores de archivos y estaciones de trabajo, en resumen todos los servicios brindados en la ubicación primaria.
Identificación: Los medios por los cuales un usuario reclama una identidad especifica sin validación a un sistema.
Integridad: Garantiza la exactitud y completitud de la información y los métodos de procesamiento.
Negación de Servicios (DoS): Es un ataque a sistemas o redes con la intención de hacer que el sistema o red no este disponible para su uso.
Propiedad Intelectual: Incluye patentes, marcas registradas, derechos de autor y secretos comerciales.
Pruebas de Caja Negra:Es un tipo de prueba de seguridad donde el sujeto que realiza la prueba no tiene ningún conocimiento previo de los sistemas que están siendo puestos a prueba.
Texto Cifrado (Ciphertext): Es un texto plano que ha sido transformado (cifrado) en un mensaje mezclado que es ininteligible.

6. REFERENTES BILBIOGRAFICOS

Pruebas de penetración en Ingenieria social: https://searchdatacenter.techtarget.com/es/consejo/Pruebas-de-penetracion-en-ingenieria-social-cuatro-tecnicas-efectivas
Qué es Kali linx y qué puedo hacer con el?: https://computerhoy.com/paso-a-paso/software/que-es-kali-linux-que-puedes-hacer-41671
Instalar Kali Linux en Virtual box: http://www.cursodehackers.com/VirtualBox.html
25 ataques informáticos y como prevenirlos: https://ciberseguridad.blog/25-tipos-de-ataques-informaticos-y-como-prevenirlos/
Ciberataques: https://www.eitb.eus/es/tag/ciberataques/
Glosario de tecnología: https://www.onasystems.net/glosario-terminos-seguridad/

Autor (es)	Nombre	Cargo	Dependencia	Fecha
	Sandra Yineth Macias	Instructores	Regional Cauca, Centro de Comercio y Servicios	2024