PROCESO DE GESTIÓN DE FORMACIÓN PROFESIONAL INTEGRAL

FORMATO GUÍA DE APRENDIZAJE

IDENTIFICACIÓN DE LA GUIA DE APRENDIZAJE

- Denominación del Programa de Formación: Técnico en control de seguridad digital V1
- Código del Programa de Formación: 233103
- Nombre del Proyecto: Aplicación y documentación de controles de seguridad digital en entornos empresariales
- Fase del Proyecto: Ejecución
- Actividad del proyecto: Operar plataformas de gestión de seguridad digital
- Competencia: Controlar sistema de seguridad de la información de acuerdo con los procedimientos y normativa técnica
- Resultados de Aprendizaje Alcanzar: Operar herramientas de control de la seguridad digital para mitigar los riesgos según procedimientos técnicos de la política de seguridad digital.
- Duración de la Guía: 144 horas

2. PRESENTACIÓN



Figura 1. Tríada SGSI. Fuente: https://n9.cl/5y212

Esta guía de aprendizaje pretende orientar al aprendiz para que adquiera la competencia, que le permitirá aplicar e implementar controles, políticas y procedimientos definidos en el sistema de gestión de seguridad de la información (SGSI), durante el desarrollo de las actividades planteadas se realizaran prácticas basadas

en la fundamentación teórica con el fin de identificar amenazas y vulnerabilidades que puedan generar incidentes que afecten la infraestructura de las redes de datos y comprometer la integridad de los datos.

3. FORMULACIÓN DE LAS ACTIVIDADES DE APRENDIZAJE

3.1. Actividades de reflexión inicial

Reconocer la importancia de la implementación de planes de seguridad en redes de datos acuerdo estándares y normativas vigentes

Con la implementaciones de controles en la seguridad de datos en redes de telecomunicaciones, el administrador de redes implementa políticas que permitan asegurar y gestionar la seguridad de la información, de los sistemas que la procesan.

En esta actividad los aprendices deberán observar el vídeo "SGSI - 01 Conceptos Básicos sobre la Seguridad de la Información", posteriormente harán uso de la herramienta mentimeter donde escriban los beneficios de la implementación de planes de seguridad en las redes de datos.

Finalmente se realizará una reflexión donde cada aprendiz interpreta la información obtenida y el instructor aclara dudas e inquietudes.

Duración de la actividad: 1 hora

Modalidad de trabajo: Individual

Ambiente requerido: Ambiente de aprendizaje presencial

Materiales: Computadores, Internet, Video Beam.

3.2 Actividades de contextualización e identificación de conocimientos necesarios para el aprendizaje.

3.2.1 Relacionar las dimensiones de los controles en sistemas de seguridad según ISO 27000.

Cada aprendiz realizará la actividad ingresando al siguiente enlace EDUCAPLAY donde deberá relacionar la descripción de cada una de las palabras relacionadas.

Luego el instructor realizará las conclusiones de las respuestas de cada aprendiz y hará la respectiva retroalimentación, aclarando las dudas.

Duración de la actividad: 1 hora

Tipo de actividad: Individual

Evidencia: No aplica

Ambiente requerido: Ambiente de aprendizaje presencial

Materiales: Computadores, Internet

3.3. Actividades de apropiación del conocimiento (Conceptualización y Teorización).

3.3.1. Reconocer los parámetros básicos de control aplicados a un sistema de gestión de seguridad de la información a través de la la realización de laboratorios prácticos.

Laboratorio 1 de control de plataforma en sistemas operativos

El instructor socializa el documento de apoyo " Lab 1", posteriormente los aprendices harán la lectura del documento entregado por el instructor y seguirán el paso a paso establecido en el laboratorio, durante la ejecución de esta actividad el instructor supervisara el desarrollo realizado por los aprendices y aclara dudas; el aprendiz debe generar como evidencia un informe que contenga; captura de pantalla con la descripción del proceso realizado, el cual se cargara en la plataforma LMS Territorium

Al finalizar la actividad se hará el cierre donde se mencionarán aspectos relevantes en la ejecución del laboratorio, se citarán ejemplos de posibles aplicaciones en entornos de producción.

Duración de la actividad: 15 horas

Tipo de actividad: Grupal – individual

Evidencia: Informe laboratorio 1 cargado en plataforma LMS Territorium

Ambiente requerido: Ambiente de aprendizaje virtual

Materiales: Computadores, Internet

Laboratorio 2 de gestión y monitoreo de la red en equipos de red

Para el desarrollo de esta actividad el instructor asigna los siguientes temas de exposición:

- ✓ Incidentes de seguridad.
- ✓ Etapas de detección, contención, erradicación, recuperación.
- ✓ Gestión de eventos de incidentes: CIRTS, CERTS.
- ✓ Centros de seguridad, ciclos de gestión de incidentes (preparación, detección y análisis, notificación, documentación y gestión del conocimiento)

Los aprendices harán uso de las bases de datos SENA y repositorios de universidades, con el fin de preparar sus presentaciones en la herramienta de presentación acordada, durante el proceso de consultas de los aprendices el instructor aclara dudas e inquietudes, finalmente se realizará la socialización de los temas asignados donde el instructor hará la retroalimentación final.

Para fortalecer el proceso teórico, los aprendices realizan prácticas sobre procesos de configuración de dispositivos de red, monitorear la red con herramientas de monitoreo de datos y recopilar incidentes de seguridad, al finalizar la actividad los aprendices realizan el taller de buenas prácticas de seguridad en la nube.

Duración de la actividad: 50 horas
Tipo de actividad: Grupal
Evidencia: Taller de buenas prácticas
Ambiente requerido: Ambiente de aprendizaje virtual
Materiales: Computadores, Internet

Laboratorio 3 de buenas prácticas de seguridad para la computación en la nube

En esta actividad de aprendizaje el instructor socializa el laboratorio 3, donde los aprendices deberán realizar el paso a paso según el documento de apoyo suministrado, sobre los conceptos de: Tipo de nube, almacenamiento en la nube, servicios en la nube, medidas esenciales en seguridad, el instructor hará preguntas y validara la realización de las actividades propuestas con el fin de evidenciar la apropiación de conceptos y configuraciones, para el cierre de la actividad el aprendiz presenta el informe de acuerdo a las instrucciones brindadas por el instructor.

Duración de la actividad: 15 horas
Tipo de actividad: Grupal
Evidencia: Informe laboratorio 3 cargado en plataforma LMS territorium
Ambiente requerido: Ambiente de aprendizaje virtual
Materiales: Computadores, Internet

Laboratorio 4 herramientas y controles básicos de seguridad digital

En esta actividad de aprendizaje "Implementar herramientas y controles básicos de seguridad digital según procedimientos técnicos de la política de seguridad de la organización, uso de contraseñas seguras, backup de datos, recuperación de información" los aprendices realizaran copias de seguridad de datos, apoyados en el material de apoyo suministrado por el instructor. Para el cierre de la actividad los aprendices presentaran un informe siguiendo las instrucciones del aprendiz.

Duración de la actividad: 15 horas
Tipo de actividad: Grupal
Evidencia: Informe laboratorio 4 cargado en plataforma LMS territorium
Ambiente requerido: Ambiente de aprendizaje virtual
Materiales: Computadores, Internet

3.4 Actividades de transferencia del conocimiento.

3.4.1 Implementar un sistema de control de seguridad de la información para una empresa

Los aprendices conformarán equipos de trabajo y resolverán el siguiente caso de estudio:

La empresa GECOMTEC S.A.S. ha sido víctima de una serie de ataques a sus sistemas, entre los que se destacan la elevación de privilegios, denegación de servicio, la presencia de ransomware. Esto evidencia debilidades en la seguridad informática de la empresa, Por tal motivo se decide contratar a la empresa TCSD.SAS para que realice el monitoreo a la red de datos con el fin de identificar vulnerabilidades y amenazas; finalmente deberán elaborar un informe técnico de fallas detectadas que puedan generar incidentes, el instructor estará presto atender dudas aclarar inquietudes y hacer acompañamiento durante todo el trabajo práctico de los aprendices.

Duración de la actividad: 37 horas
Tipo de actividad: Grupal
Evidencia: Informe técnico implementación SGSI caso de estudio cargado en plataforma LMS territorium
Ambiente requerido: Ambiente de aprendizaje virtual
Materiales: Computadores, Internet

4. ACTIVIDADES DE EVALUACIÓN

Evidencias de Aprendizaje	Criterios de Evaluación	Técnicas e Instrumentos de Evaluación
Evidencias de Conocimiento: Taller de buenas prácticas de seguridad en la nube. **Evidencias de Desempeño:** Exposiciones de gestión de monitoreo. **Evidencias de Producto:** Informe de laboratorios. Informe técnico de incidencias.	Configura los parámetros básicos de los equipos de protección y control como plataforma de actualizaciones, servicios de directorio, plataforma antivirus y antimalware en servidores y clientes acorde con los manuales y política de seguridad digital Configura parámetros básicos de gestión de red en equipos tecnológicos según procedimientos técnicos de la política de seguridad de la organización. Opera herramientas de monitoreo y gestión de red de datos de acuerdo con	**Técnica: Preguntas** **Instrumento**: Rúbrica **Técnica:** Cuestionario Lista de chequeo Técnica: Observación. Lista de chequeo Técnica: valoración de producto

	procedimiento interno establecido por la organización. Opera herramientas de protección y control de activos tecnológicos según procedimientos técnicos de la política de seguridad de la organización. Implementa herramientas y controles básicos de seguridad digital según procedimientos técnicos de la política de seguridad de la organización Opera herramientas de monitoreo y gestión de incidentes de seguridad digital según procedimientos técnicos de la política de seguridad de la organización. Seguridad perimetral: parametrizar firewalls, next generation firewall (ngf), appliance aplicación, firma de conexiones, identificadores de aplicaciones. Valida la funcionalidad de los controles de seguridad digital según los requerimientos funcionales y política interna de la organización. Verifica el cumplimiento de la cadena de custodia del incidente según los procedimientos técnicos	

	establecidos por equipo de respuesta a incidentes.	

5. GLOSARIO DE TÉRMINOS

- Canal de control y comando: Un canal de mando y control es el medio por el cual un atacante se comunica y controla los equipos infectados con malware, lo que conforma un botnet.
- Carga destructiva: Una carga destructiva es la actividad maliciosa que realiza el malware. Una carga destructiva es independiente de las acciones de instalación y propagación que realiza el malware. Crimeware: Software que realiza acciones ilegales no previstas por un usuario que ejecuta el software. Estas acciones buscan producir beneficios económicos al distribuidor del software.
- Ciberdelito: El ciberdelito es un delito que se comete usando una computadora, red o hardware. La computadora o dispositivo puede ser el agente, el facilitador o el objeto del delito. El delito puede ocurrir en la computadora o en otros lugares.
- Definiciones de virus: Una definición de virus es un archivo que proporciona información al software antivirus, para identificar los riesgos de seguridad. Los archivos de definición tienen protección contra todos los virus, gusanos, troyanos y otros riesgos de seguridad más recientes. Las definiciones de virus también se denominan firmas antivirus.
- Descarga inadvertida: Una descarga inadvertida es una descarga de malware mediante el ataque a una vulnerabilidad de un navegador Web, equipo cliente de correo electrónico o plug-in de navegador sin intervención alguna del usuario. Las descargas inadvertidas pueden ocurrir al visitar un sitio Web, visualizar un mensaje de correo electrónico o pulsar clic en una ventana emergente engañosa.
- Encriptación: La encriptación es un método de cifrado o codificación de datos para evitar que los usuarios no autorizados lean o manipulen los datos. Sólo los individuos con acceso a una contraseña o clave pueden descifrar y utilizar los datos. A veces, el malware utiliza la encriptación para ocultarse del software de seguridad. Es decir, el malware cifrado revuelve el código del programa para que sea difícil detectarlo Exploits o Programas intrusos: Los programas intrusos son técnicas que aprovechan las vulnerabilidades del software y que pueden utilizarse para evadir la seguridad o atacar un equipo en la red.
- Firewall: Un firewall es una aplicación de seguridad diseñada para bloquear las conexiones en determinados puertos del sistema, independientemente de si el tráfico es benigno o maligno. Un firewall debería formar parte de una estrategia de seguridad estándar de múltiples niveles.
- Firma antivirus: Una firma antivirus es un archivo que proporciona información al software antivirus para encontrar y reparar los riesgos. Las firmas antivirus proporcionan protección contra todos los virus, gusanos, troyanos y otros riesgos de seguridad más recientes. Las firmas antivirus también se denominan definiciones de virus.

- Greylisting o Lista Gris: La lista gris es un método de defensa para proteger a los usuarios de correo electrónico contra el spam. Los mensajes de correo electrónico son rechazados temporalmente de un remitente que no es reconocido por el agente de transferencia de correos. Si el correo es legítimo, el servidor de origen tratará de nuevo y se aceptará el correo electrónico. Si el correo es de un remitente de spam, probablemente no se reintentará su envío y por lo tanto, no logrará pasar el agente de transferencia de correos.

- Gusanos: Los gusanos son programas maliciosos que se reproducen de un sistema a otro sin usar un archivo anfitrión, lo que contrasta con los virus, puesto que requieren la propagación de un archivo anfitrión infectado.

- Ingeniería Social: Método utilizado por los atacantes para engañar a los usuarios informáticos, para que realicen una acción que normalmente producirá consecuencias negativas, como la descarga de malware o la divulgación de información personal. Los ataques de phishing con frecuencia aprovechan las tácticas de ingeniería social.

- Lista blanca o Whitelisting: La lista blanca es un método utilizado normalmente por programas de bloqueo de spam, que permite a los correos electrónicos de direcciones de correo electrónicos o nombres de dominio autorizados o conocidos pasar por el software de seguridad.

- Keystroke Logger o Programa de captura de teclado (Keylogger): Es un tipo de malware diseñado para capturar las pulsaciones, movimientos y clics del teclado y del ratón, generalmente de forma encubierta, para intentar robar información personal, como las cuentas y contraseñas de las tarjetas de crédito. Malware: El malware es la descripción general de un programa informático que tiene efectos no deseados o maliciosos. Incluye virus, gusanos, troyanos y puertas traseras. El malware a menudo utiliza herramientas de comunicación populares, como el correo electrónico y la mensajería instantánea, y medios magnéticos extraíbles, como dispositivos USB, para difundirse. También se propaga a través de descargas inadvertidas y ataques a las vulnerabilidades de seguridad en el software. La mayoría del malware peligroso actualmente busca robar información personal que pueda ser utilizada por los atacantes para cometer fechorías.

- Negación de servicio (DoS): La negación de servicio es un ataque en el que el delincuente intenta deshabilitar los recursos de una computadora o lugar en una red para los usuarios. Un ataque distribuido de negación de servicio (DDoS) es aquel en que el atacante aprovecha una red de computadoras distribuidas, como por ejemplo una botnet, para perpetrar el ataque.

- Pharming: Método de ataque que tiene como objetivo redirigir el tráfico de un sitio Web a otro sitio falso, generalmente diseñado para imitar el sitio legítimo. El objetivo es que los usuarios permanezcan ignorantes del redireccionamiento e ingresen información personal, como la información bancaria en línea, en el sitio fraudulento. Se puede cometer pharming cambiando el archivo de los equipos anfitriones en la computadora de la víctima o atacando una vulnerabilidad en el software del servidor DNS.

- Phishing: A diferencia de la heurística o los exploradores de huella digital, el software de seguridad de bloqueo de comportamiento se integra al sistema operativo de un equipo anfitrión y supervisa el comportamiento de los programas en tiempo real en busca de acciones maliciosas. El software de bloqueo de comportamiento bloquea acciones potencialmente dañinas, antes de que tengan

oportunidad de afectar el sistema. La protección contra el comportamiento peligroso debe ser parte de una estrategia de seguridad estándar de múltiples niveles.

- Protección heurística (Heuristics-Based Protection): Forma de tecnología antivirus que detecta las infecciones mediante el escrutinio de la estructura general de un programa, las instrucciones de sus computadoras y otros datos contenidos en el archivo. Una exploración heurística hace una evaluación sobre la probabilidad de que el programa sea malicioso con base en la aparente intención de la lógica. Este plan puede detectar infecciones desconocidas, ya que busca lógica generalmente sospechosa, en lugar de huellas específicas de malware, tales como los métodos tradicionales de antivirus de firmas. La protección heurística debería hacer parte de una estrategia de seguridad estándar de múltiples niveles Rootkits: Componente de malware que utiliza la clandestinidad para mantener una presencia persistente e indetectable en un equipo. Las acciones realizadas por un rootkit, como la instalación y diversas formas de ejecución de códigos, se realizan sin el conocimiento o consentimiento del usuario final. Los rootkits no infectan las máquinas por sí mismos como lo hacen los virus o gusanos, sino que tratan de proporcionar un entorno indetectable para ejecutar códigos maliciosos. Los atacantes normalmente aprovechan las vulnerabilidades en el equipo seleccionado o utilizan técnicas de ingeniería social para instalar manualmente los rootkits. O, en algunos casos, los rootkits pueden instalarse automáticamente al ejecutarse un virus o gusano o incluso simplemente al navegar en un sitio Web malicioso. Una vez instalados, el atacante puede realizar prácticamente cualquier función en el sistema, incluyendo acceso remoto, intercepción de comunicaciones, así como procesos de ocultamiento, archivos, claves de registro y canales de comunicación.

- Seguridad basada en la reputación: La seguridad basada en la reputación es una estrategia de identificación de amenazas que clasifica las aplicaciones con base en ciertos criterios o atributos para determinar si son probablemente malignas o benignas. Estos atributos pueden incluir diversos aspectos como la edad de los archivos, la fuente de descarga de los archivos y la prevalencia de firmas y archivos digitales. Luego, se combinan los atributos para determinar la reputación de seguridad de un archivo. Las calificaciones de reputación son utilizadas después por los usuarios informáticos para determinar mejor lo que es seguro y permitirlo en sus sistemas. La seguridad basada en la reputación debe ser parte de una estrategia de seguridad estándar de múltiples niveles.

- Sistema de detección de intrusos: Un sistema de detección de intrusos es un servicio que monitorea y analiza los eventos del sistema para encontrar y proporcionar en tiempo real o casi real advertencias de intentos de acceso a los recursos del sistema de manera no autorizada. Es la detección de ataques o intentos de intrusión, que consiste en revisar registros u otra información disponible en la red. Un sistema de detección de intrusos debe ser parte de una estrategia de seguridad estándar de múltiples niveles. Sistema de prevención de intrusos: Un sistema de prevención de intrusos es un dispositivo (hardware o software) que supervisa las actividades de la red o del sistema en busca de comportamiento no deseado o malicioso y puede reaccionar en tiempo real para bloquear o evitar esas actividades. Un sistema de prevención de intrusos debe ser parte de una estrategia de seguridad estándar de múltiples niveles.

- Software de seguridad fraudulento (rogue): Un programa de software de seguridad rogue es un tipo de aplicación engañosa que finge ser software de seguridad legítimo, como un limpiador de registros o detector antivirus, aunque realmente proporciona al usuario poca o ninguna protección y, en algunos casos, puede de hecho facilitar la instalación de códigos maliciosos contra los que busca protegerse.

- Spam: También conocido como correo basura, el spam es correo electrónico que involucra mensajes casi idénticos enviados a numerosos destinatarios. Un sinónimo común de spam es correo electrónico comercial no solicitado (UCE). El malware se utiliza a menudo para propagar mensajes de spam al infectar un equipo, buscar direcciones de correo electrónico y luego utilizar esa máquina para enviar mensajes de spam. Los mensajes de spam generalmente se utilizan como un método de propagación de los ataques de phishing

- Spyware: Paquete de software que realiza un seguimiento y envía información de identificación personal o información confidencial a otras personas. La información de identificación personal es la información que puede atribuirse a una persona específica, como un nombre completo. La información confidencial incluye datos que la mayoría de las personas no estaría dispuesta a compartir con nadie e incluye datos bancarios, números de cuentas de tarjeta de crédito y contraseñas. Los receptores de esta información pueden ser sistemas o partes remotas con acceso local.

- Toolkit: Paquete de software diseñado para ayudar a los hackers a crear y propagar códigos maliciosos. Los toolkits frecuentemente automatizan la creación y propagación de malware al punto que, incluso los principiantes delincuentes cibernéticos son capaces de utilizar amenazas complejas. También pueden utilizarse toolkits para lanzar ataques web, enviar spam y crear sitios de phishing y mensajes de correo electrónico.

- Variantes: Las variantes son nuevas cepas de malware que piden prestados códigos, en diversos grados, directamente a otros virus conocidos. Normalmente se identifican con una letra o letras, seguido del apellido del malware; por ejemplo, W32.Downadup.A, W32.Downadup.B y así sucesivamente. Muchos de los virus actuales están programados para operar sigilosamente la computadora del usuario con el fin de robar información personal y utilizarla para cometer delitos. Otros menoscaban el equipo dañando los programas, eliminando archivos o volviendo a formatear el disco duro. Aún existen otros que no están diseñados para causar daño, aunque simplemente se reproducen y hacen manifiestan su presencia presentando mensajes de texto, video y audio, aunque este tipo de ataques de notoriedad no son tan comunes, puesto que los autores de virus y demás malware tiene como fin obtener ganancias ilegales. Vulnerabilidad: Una vulnerabilidad es un estado viciado en un sistema informático (conjunto de sistemas) que afecta las propiedades de confidencialidad, integridad y disponibilidad (CIA) de los sistemas.

6. REFERENTES BILBIOGRÁFICOS

Bibliografía SENA

- http://biblioteca.sena.edu.co/paginas/bases.html
- Díaz Orueta, G. Alzórriz Armendáriz, I. y Sancristóbal Ruiz, E. (2014). Procesos y herramientas para la seguridad de redes. UNED - Universidad Nacional de Educación a Distancia. https://elibro-net.bdigital.sena.edu.co/es/lc/senavirtual/titulos/48736

- Gómez Vieites, Á. (2015). Gestión de incidentes de seguridad informática. RA-MA Editorial. https://elibro-net.bdigital.sena.edu.co/es/lc/senavirtual/titulos/62467

Alegsa (2011), Definición de Seguridad Informática. http://www.alegsa.com.ar/Dic/seguridad%20informatica.php , (Descargado el 30 de julio del 2018)

Arango, Jhon (2010), El atacante informático.http://www.itforensic-la.com/revistas/El-Atacante-Informatico-Cp1-3.pdf ,(Descargado el el 21 de octubre del 2021)

Briones, Ignacio(S.F),definición métricas de seguridad, rediris, http://www.rediris.es/difusion/publicaciones/boletin/85-86/ponencias85-1.pdf , (Consultado el 10 de octubre del 2021)

Manual de políticas de seguridad informática, Universidad Nacional para la Gestión del riesgo de Desastres. P.

Saavedra Lopez, Esteban. Seguridad Perimetral en Redes GNU/Linux. Esteban Saavedra Slideshare. Fecha de Consulta: 1 de Febrero de 2017.URL: https://es.slideshare.net/estebansaavedra/introduccin-a-la-seguridad-perimetral-presentation

Software ISO Riesgos y seguridad https://www.isotools.org/normas/riesgos-y-seguridad/iso-27001/ (consultado 21 octubre del 2021)

Vaquero,Miguel(2010), software libre y software propietario, webmaster, http://www.deciencias.net/simulaciones/paginas/libre.htm , (Consultado el 15 de octubre del 2021)

7. CONTROL DEL DOCUMENTO

	Nombre	Cargo	Dependencia	Fecha
Autor (es)	Diego Fernando Rodriguez Mapallo Juan Pablo Agredo Castaño Sandra Galíndez	Instructor Instructor Formadora Instructores	CEAI	02-05-2022

8. CONTROL DE CAMBIOS (diligenciar únicamente si realiza ajustes a la guía)

	Nombre	Cargo	Dependencia	Fecha	Razón del Cambio
Autor (es)					