



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 LA SEGURIDAD DIGITAL
- **Código del Programa de Formación:** 233103
- **Nombre del Proyecto:** ASEGURAR LOS PROCESOS DE SEGURIDAD DE LA INFORMACIÓN TANTO LÓGICOS Y FÍSICOS EN LAS INSTITUCIONES EDUCATIVAS Y EMPRESAS DEL DEPARTAMENTO DE CAUCA
- **Fase del Proyecto:** Fase I - PLANEACIÓN
- **Actividad de Proyecto:** ELABORAR UN PLAN PARA LA GESTIÓN DE CONTROLES DE SEGURIDAD DIGITAL PARA MONITORIZAR, CONTROLAR Y DOCUMENTAR PROCESOS DE SEGURIDAD DIGITAL SEGÚN TECNOLOGÍAS Y MODELO DE
- **Competencia:** Controlar sistema de seguridad de la información de acuerdo con los procedimientos y normativa técnica
- **Resultados de Aprendizaje Alcanzar:**
 - Recopilar información de incidentes de seguridad digital según criterios técnicos, marcos de referencia y modelo del negocio.
 - Documentar incidentes de seguridad digital según criterios técnicos y marco de referencia.
 - Operar herramientas de control de la seguridad digital para mitigar los riesgos según procedimientos técnicos de la política de seguridad digital.
 - Validar el impacto de incidentes de seguridad con base en criterios técnicos y herramientas de monitoreo de acuerdo con el modelo del negocio.



- Duración de la Guía: 96 horas

2. PRESENTACION

La seguridad digital requiere de un conjunto de operaciones, métodos y herramientas destinados a proteger activos de información. Todo activo de información es un recurso que representa valor para la entidad, y por lo tanto se debe mantener un inventario detallado sobre el estado, las características y la función que cumplen dentro de la infraestructura que soporta las operaciones del negocio. Así, los activos son todos aquellos recursos que facilitan, en gran medida, el funcionamiento mismo de la entidad manteniendo la información disponible, confiable y confidencial dándole valor al proceso de la seguridad digital. Dentro de los activos de la información también se encuentran las personas las cuales deben ser informadas y capacitadas sobre la importancia de mantener un “buen” comportamiento al tratar la información que se comparte en la red.

Dentro de la normativa interna de las organizaciones se debe contar con políticas de seguridad digital que estén enfocadas en indicar cómo se realizan los procesos para el tratamiento de incidentes de seguridad informática, también se debe especificar las normas internas sobre las configuraciones que se deben realizar a los equipos involucrados en el tratamiento de la información en cualquier nivel y área de la empresa; en términos generales, las compañías deben contar con políticas en las cuales se especifique de manera detallada como se debe tratar la información cuando se procesa, almacena y transporta por la red de datos.

El técnico en **control de la seguridad digital** debe conocer a fondo la política de seguridad digital de la organización y allí identificar su función dentro este proceso de manera que se apropie de la política y modelo de seguridad digital de la organización y realice todas sus actividades de acuerdo a su rol dentro del proceso.

En esta fase de proyecto y a través de esta guía de aprendizaje el aprendiz va a adquirir conocimientos indispensables para su función como técnico en control de la seguridad digital, conocerá y aplicará las técnicas e instrumentos para realizar inventario de activos de información y desarrollará las habilidades necesarias para identificar políticas de seguridad digital y la aplicabilidad y pertinencia dentro de la organización y su modelo de negocio.



3. FORMULACION DE LAS ACTIVIDADES DE APRENDIZAJE

Actividades de Reflexión Inicial:

Analice y reflexione el siguiente caso:

La empresa “SENAdmins” se dedica a la Administración de las constructoras de obras civiles en la ciudad, esta cuenta con 5 departamentos que son: arquitectura, ingeniería, contabilidad, ventas y gerencia. La infraestructura tecnológica está conformada por enrutadores, firewalls, switches, Access Point, servidor proxy, servidor con servicios de directorio, equipos de escritorio, portátiles que permanecen dentro de las instalaciones, portátiles que son utilizados desde lugares externos a la empresa, tabletas y celulares. Se ha notado que durante el último año los usuarios han reportado alertas por posible infección de virus, los correos se van a la bandeja de SPAM, lentitud en la navegación de internet, lentitud al acceder a la información compartida en la red interna, incluso pérdida de información por ataque de ransomware.

El equipo de soporte técnico del área de sistemas realizó auditoria de software a todos los equipos de cómputo, revisó los registros de los equipos activos y reportó los siguientes hallazgos:

- Registros de acceso a páginas Web con contenido pornográfico.
- Instalación de programas (software), sin la debida autorización del área de Tecnología, tales como: Shareware, software de evaluación, los cuales en su mayoría traen código oculto que daña los navegadores.
- Uso de redes sociales durante todo el tiempo desde cualquier departamento de la empresa.
- Ingreso a sitios de compras que no están relacionadas con el “core” del negocio.
- Dentro de la empresa se ha utilizado el internet con fines comerciales y políticos.
- Se ha registrado acceso a internet para acceder, crear, copiar, distribuir material o enviar mensajes obscenos, pornográficos, etc, o mensajes que instiguen violencia o, incluso, amenazas



- Los usuarios que tienen acceso a Internet a través de los recursos de la entidad no conocen sobre la existencia de las políticas y prácticas de uso de Internet.
- El equipo de soporte técnico se ha enterado de que los usuarios están enviando información confidencial a través de plataformas de correo electrónico con dominio diferente al de la empresa.
- Se ha utilizado el correo institucional para el desarrollo de actividades políticas, comerciales o de entretenimiento o para la transmisión de mensajes vulgares u obscenos.
- Se han identificado equipos de cómputo ajenos a la empresa accediendo al servicio de red inalámbrica corporativo.
- Se ha utilizado el correo electrónico para participar en la propagación de cartas encadenadas o participar en esquemas piramidales o temas similares.
- Se han encontrado claves, de acceso a los equipos de cómputo, escritas en papeles sobre el escritorio de los usuarios, en correos y en chats. Desde el punto de vista del **control de la seguridad digital** y en su rol como técnico encargado del proceso, responda las siguientes preguntas:
- ¿Cuál es su opinión, desde el punto de vista técnico, sobre la situación que se presenta en la empresa?
- ¿Cuáles de los hallazgos afectan la confidencialidad, cuales la integridad y cuales la disponibilidad de la información?
- ¿Cuáles personas deben estar involucradas en el proceso de la seguridad digital para lograr mejorar el rendimiento y el funcionamiento de la infraestructura informática? Justifique
- Haga una lista de recomendaciones que usted le haría al departamento de sistemas y al departamento administrativo de la empresa.

Actividades de Conocimientos Previos:

De acuerdo a su experiencia con las redes de datos, con las nuevas tecnologías, el uso de dispositivos móviles, redes sociales, sistemas de información y todo lo que involucre el uso de tecnologías en sus tareas cotidianas, responda lo siguiente:

1. ¿Cuáles son las acciones que realizan los usuarios, de forma cotidiana, que ponen en peligro la seguridad digital en entornos corporativos? Enumérelas y justifique.
2. Defina con sus propias palabras:
 - a. ¿Qué es una recomendación?
 - b. ¿Qué es una norma?
 - c. ¿Qué es seguridad digital?
 - d. ¿Qué es un marco de referencia?



- e. ¿Qué es la infraestructura informática de una organización?
 - f. ¿Qué es una vulnerabilidad?
 - g. ¿Qué es un riesgo?
3. Enumere los componentes, activos y pasivos, que forman una red de datos. Diga la función de cada uno.

Actividades de Apropiación:

Actividad – Fundamentos de redes

Resolver la actividad propuesta en el LMS dispuesta para este objetivo, en ella se va a desarrollar todo lo relacionado con fundamentos de redes, direccionamiento IPv4, IPv6, modelos de referencia OSI, TCP/IP, servicios de red, conectividad, topologías y seguridad digital.

Actividad – infraestructura de hardware y software

Resolver la actividad propuesta en el LMS correspondiente a herramientas de análisis de red, herramientas de escaneo de red, herramientas de escaneo de servicios de red, fundamentos de firewall, tipos de firewall, fichas técnicas de los equipos de conectividad y tipos de licencia

Actividad de seguridad digital

En la plataforma LMS se dispone de la actividad correspondiente a seguridad digital, allí se van a tocar temas como las vulnerabilidades y sus clasificaciones, amenazas, riesgos, mitigación del riesgo y riesgo asumible, contramedidas técnicas y administrativas, manejo de incidentes y equipo de respuesta a incidentes, técnicas de diagnóstico para determinar el nivel de daño que puede llegar a tener un incidente que atenta contra la **seguridad digital**.

Actividad de seguridad de la información

En esta actividad se abordará la introducción al análisis de riesgos, políticas de seguridad de la información y la importancia que tienen para garantizar la **seguridad digital**, todo esto con base a estándares



internacionales y aplicados al entorno laboral actual. La actividad se encuentra en el LMS.

Actividades de Transferencia:

Esta actividad deberá resolverla con base en el conocimiento adquirido al desarrollar el caso de estudio y las actividades de apropiación desarrolladas anteriormente.

El instructor le va a entregar un documento llamado "**Políticas Internas de seguridad digital**". Este documento es propiedad de la empresa "**SENAdmins**" Por lo tanto se debe mantener la confidencialidad y la integridad del mismo.

Sus tareas van a ser la siguientes:

1. Identificar las tareas operativas dentro del manual de políticas internas de seguridad digital
2. ¿Cuáles de las tareas operativas le corresponden al "técnico en control de seguridad digital"
3. Diseñar un plan de ejecución para realizar las tareas operativas en la infraestructura de red.

Ambiente Requerido

AMBIENTES DE APRENDIZAJE TIPIFICADOS
ESCENARIO (Aula, Laboratorio, taller, unidad productiva) y elementos y condiciones de seguridad industrial, salud ocupacional y medio ambiente
Ambiente de aproximadamente 48 mts ² con capacidad para 35 aprendices, dotado de sillas, mesas, conexiones eléctricas, pantalla para proyectar, buena iluminación y aire acondicionado.



- Materiales

Materiales de formación devolutivos: (Equipos/Herramientas)		Materiales de formación (consumibles)	
Descripción	Cantidad	Descripción	Cantidad
Computadores portátiles o de escritorio, con las siguientes características mínimas: <ul style="list-style-type: none"> • 4 GB de RAM • 500 GB de disco duro • Procesador cuatro núcleos de 2 GHz en adelante 	18	<ul style="list-style-type: none"> • Licencias para Sistemas operativos. • Software de ofimática 	18
<ul style="list-style-type: none"> • Conectividad a internet 	100 Mbps /ambiente		

4. ACTIVIDADES DE EVALUACIÓN

Evidencias de Aprendizaje	Criterios de Evaluación	Técnicas e Instrumentos de Evaluación
<p>Evidencias de Conocimiento:</p> <p>Prueba de conocimientos correspondiente a la "política de seguridad digital"</p>	<p>Interpreta la normativa y política de seguridad digital propia de la organización según marco de referencia.</p>	<p>Técnica: Cuestionario</p>
<p>Evidencias de Desempeño:</p> <p>Solución al caso de estudio propuesto en el cual debe</p>	<p>Reconoce y asume las funciones y responsabilidades propias de su rol dentro de la estructura</p>	<p>Solución de caso de estudio</p>



<p>asumir su rol como técnico en control de la seguridad digital</p> <p>Evidencias de Producto:</p> <p>Evidencias en documento escrito para la solución a las actividades de apropiación del conocimiento.</p>	<p>del equipo de seguridad digital.</p> <p>Interpreta la normativa de seguridad digital de acuerdo con normas interna de la organización.</p>	<p>ensayo, mapa conceptual, preguntas, foro, taller</p>
---	---	--

5. GLOSARIO DE TERMINOS

Activos: Son todo elemento que compone el proceso de la comunicación, la cual la componen: la información, el emisor, el medio que la transporta y finalmente el receptor.

Administrador: Es la persona o programa encargado de gestionar, realizar el control, conceder permisos, en un sistema informático o red de ordenadores.

Adware: Los programas de tipo adware muestran publicidad asociada a productos y/o servicios ofrecidos por los propios creadores o por terceros.

Autorización: Es el proceso por el cual se determina qué, cómo y cuándo, un usuario autenticado puede utilizar los recursos de la organización.

Amenaza: Es cualquier actividad que represente posible daño a su información. Las amenazas pueden tomar muchas formas.



Confidencialidad: Es el acceso a los activos del sistema está limitado a usuarios autorizados.

Gusanos: Los gusanos son programas que realizan copias de sí mismos, alojándolas en diferentes ubicaciones del ordenador. El objetivo de este malware suele ser colapsar los ordenadores y las redes. **Integridad:** Los activos del sistema sólo pueden ser borrados o modificados por usuarios autorizados. Interrupción: es un ataque contra la disponibilidad, se da cuando un componente del sistema informático es destruido o se vuelve no disponible.

Intercepción: Es un ataque contra la confiabilidad, se da cuando una entidad (persona, programa u Ordenador) no autorizada consigue acceso a un recurso.

Modificación: Es un ataque contra la integridad , se da cuando una entidad no autorizada no solo accede al recurso , sino que es capaz de modificarlo cambiando en parte o en todo el funcionamiento del sistema. Organización: En este grupo se incluyen los aspectos que componen la estructura física y organizativa de las empresas

Riesgo: Es que la información de tu compañía esté disponible para terceros, lo cual causará pérdidas a la compañía, tiempo, dinero y reputación.

Scams: Es un tipo de correo electrónico fraudulento que pretende estafar económicamente al usuario presentado como donación a recibir, lotería o premio al que se accede previo envío de dinero.

Seguridad informática: Es un conjunto de métodos y herramientas destinados a proteger la información y por ende los sistemas informáticos ante cualquier amenaza, un proceso en el cual participan además personas.

Spyware: El spyware o programas espías son aplicaciones que recopilan información sobre una persona u organización sin su consentimiento ni conocimiento.

Trojanos: El principal objetivo de este tipo de malware es introducir e instalar otras aplicaciones en el equipo infectado, para permitir su control remoto desde otros equipos.

Virus: Es un programa informático diseñado para infectar archivos. Suelen venir dentro del código de otros programas. Los objetivos de los virus suelen ser los programas ejecutables.



Vulnerabilidad: Es una debilidad en la seguridad de la información que puede ser explotada por una amenaza; que podría ser, una debilidad en su sistema de seguridad de red, procesos, y procedimientos.

6. REFERENTES BIBLIOGRAFICOS

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/introduccion-a-la-seguridad-perimetral-presentation>

MANUAL DE POLÍTICAS DE SEGURIDAD INFORMÁTICA, Universidad Nacional para la Gestión del riesgo de Desastres. P.

7. CONTROL DEL DOCUMENTO

	Nombre	Cargo	Dependencia	Fecha
Autor (es)	Alejandro Arias Henry Bastidas Mauricio Ortiz Morales	Instructor	Teleinformática	31 de julio de 2019

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

	Nombre	Cargo	Dependencia	Fecha
	Sandra Yineth Macias	Instructor	Comercio Servicios y	13/08/2024