PROCESO DE GESTIÓN DE FORMACIÓN PROFESIONAL INTEGRAL

FORMATO GUÍA DE APRENDIZAJE

1. 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** Aplicación y documentacion de controles deseguridad digital en entornos Empresariales
- **Fase del Proyecto** Ejecución
- **Actividad de Proyecto:** Caracterizar los incidentes de seguridad
- **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.
- **Duración de la Guía** 96 horas

2. PRESENTACIÓN



La recopilación de información de incidentes de seguridad digital es un proceso crítico para cualquier organización que busque proteger sus activos digitales y garantizar la continuidad de sus operaciones.

Para llevar a cabo esta tarea de manera efectiva, es esencial contar con un conjunto de criterios técnicos, marcos de referencia y un modelo de negocio bien definidos.

Los criterios técnicos son las herramientas y técnicas utilizadas para recopilar, analizar y reportar información sobre los incidentes de seguridad digital. Estos pueden incluir sistemas de detección y respuesta de seguridad, herramientas de análisis de registro, y sistemas de monitoreo y análisis de red, entre otros.

Los marcos de referencia, por otro lado, son modelos preestablecidos que proporcionan una estructura y una guía para la recopilación de información de incidentes de seguridad digital. Estos marcos pueden incluir el marco de trabajo de la NIST, el marco de trabajo de CIS, y el marco de trabajo de ISO, entre otros.

Finalmente, el modelo de negocio define la estrategia general de la organización en relación con la seguridad digital y cómo la recopilación de información de incidentes de seguridad digital se integra en esta estrategia. Esto puede incluir la identificación de los activos digitales críticos de la organización, la definición de los objetivos de seguridad y la asignación de recursos para la seguridad digital.

En conjunto, estos tres elementos proporcionan una base sólida para la recopilación de información de incidentes de seguridad digital, lo que permite a las organizaciones identificar, investigar y responder a los incidentes de seguridad digital de manera efectiva.

3. FORMULACIÓN DE LAS ACTIVIDADES DE APRENDIZAJE

3.1 Actividad de Reflexión inicial : Reconocer la importancia de que las organizaciones tengan planes y medidas de seguridad sólidos para prevenir y detectar estos incidentes de seguridad digital

Es fundamental que las organizaciones tengan planes y medidas de seguridad sólidos para prevenir y detectar los incidentes de seguridad digital, ya que estos incidentes pueden tener graves consecuencias tanto para la organización como para sus clientes o usuarios.

En esta actividad los aprendices deberán observar el vídeo ”Metodología de Gestion e Incidentes de la Seguridad”, posteriormente harán uso de la herramienta mentimeter donde escriban los beneficios de la implementación de planes de gestión de incidentes de la seguridad.

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

Duración: 3 horas.

Evidencia: Uso de la herramienta mentimeter.

Modalidad de trabajo: Individual

Ambiente requerido: Ambiente de aprendizaje, Computador, Internet.

Materiales: Computadores, Internet, Video Beam o Televisor.

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

Cada aprendiz realizará la actividad ingresando al siguiente enlace EDUCAPLAY donde deberá contestar un cuestionario acerca de unos conocimeintos básicos en el área de seguridad digital.

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

Duración: 3 horas.

Evidencia: Uso de la herramienta Educaplay.

Modalidad de trabajo: Individual

Ambiente requerido: Ambiente de aprendizaje, Computador, Internet.

Materiales: Computadores, Internet, Video Beam o Televisor.

3.3 Actividades de apropiación del conocimiento (Conceptualización y Teorización): Identificar los criterios técnicos relevantes sobre incidentes de seguridad digital:

Es fundamental comprender algunos conceptos básicos sobre los incidentes de seguridad digital y sus varios tipos, así como los sistemas y aplicaciones que deben monitorearse, los indicadores de compromiso (IOC), los patrones de ataque conocidos y otros factores relevantes para el monitoreo de seguridad.

Se organizarán en parejas para investigar los temas planteados y se realizarán exposiciones para socializar los diferentes conceptos a todo el grupo.

Los temas son:

- **Incidentes de seguridad digital y sus varios tipos:** Cualquier incidente que comprometa la seguridad de la información de una organización se denomina incidente de seguridad digital. Estos eventos pueden tener una variedad de formas y pueden ser causados por una variedad de factores, como errores humanos, malware, ataques externos, desastres naturales y fallas técnicas.

- **Los diversos tipos de amenazas:** Hay una variedad de amenazas a la seguridad digital, incluidos el malware, los ataques de phishing, los ataques DDoS y la ingeniería social. Es fundamental comprender las características de cada una de estas amenazas y cómo pueden afectar a la empresa.

- **Identificar los sistemas y aplicaciones críticos:** es crucial identificar los sistemas y aplicaciones críticos del negocio y asegurarse de que estén debidamente protegidos. Estos sistemas y aplicaciones deben monitorearse continuamente para detectar cualquier anomalía.

- **Los Indicadores de Compromiso (IOCs):** las señales de que un sistema puede estar comprometido o haber sido atacado se denominan IOCs. Es fundamental tener conocimiento de los diversos tipos de IOC, incluidas direcciones IP maliciosas, archivos sospechosos y cadenas de texto específicas, para poder detectar y responder rápidamente a los ataques.

- **Los patrones de ataque conocidos:** la comunidad de seguridad ha identificado técnicas de ataque que se conocen como patrones de ataque conocidos. Para identificarlos rápidamente, es fundamental estar al tanto de estos patrones de ataque.

- **Sistema de monitoreo de seguridad:** la implementación de un sistema de monitoreo de seguridad es crucial. Este sistema debe tener la capacidad de recopilar y analizar datos sobre los sistemas y aplicaciones importantes de la organización. Las herramientas de detección y respuesta de seguridad, las herramientas de análisis de registro y los sistemas de monitoreo y análisis de red pueden ser parte de estos sistemas.

Deben crear un diagrama de tipo mapa mental que describa los conceptos técnicos de seguridad que se le dieron. Para su elaboración, este esquema gráfico de tipo mapa mental debe responder a las indicaciones señaladas y incorporar convenciones, ramificaciones, colores, imágenes e íconos que permitan su organización y comprensión.

Puede investigar la estructura de un mapa mental utilizando Internet si lo desea. Teniendo en cuenta la mejor opción que se adecue a sus estilos de aprendizaje, puede realizarlo en una herramienta digital como Goconqr, Draw.io, Mindomo, incluso en el procesador de palabras Word o el presentador de diapositivas PowerPoint.

Debe crearse y enviarse en formato PDF.

Duración: 25 horas.

Evidencia: Mapa mental, en formato PDF.

Ambiente requerido: Ambiente de aprendizaje, Computador, Internet.

Materiales: Computadores, Internet, Video Beam o Televisor.

3.3.1. Conocer los marcos de referencia disponibles para la gestión de la seguridad de la información y el control de los sistemas de información:

Hay varios marcos de referencia disponibles para la administración de la seguridad de la información y el control de los sistemas de información. Algunos de los más conocidos son:

- **NIST:** El Instituto Nacional de Estándares y Tecnología (NIST) es una agencia gubernamental de los Estados Unidos que ha desarrollado un marco de referencia de ciberseguridad ampliamente utilizado. El marco se enfoca en la administración de riesgos y está diseñado para ayudar a las organizaciones a proteger sus sistemas de información y activos críticos.

- **ISO 27001:** La norma ISO 27001 es un marco de referencia de seguridad de la información reconocido internacionalmente. Se enfoca en la administración de riesgos y proporciona un conjunto de controles de seguridad que se pueden implementar para proteger los activos de información de una organización.

- **COBIT:** El marco de referencia de COBIT (Control Objectives for Information and Related Technology) es un conjunto de prácticas y principios para la gobernanza y administración de los sistemas de información de una organización. Está diseñado para ayudar a las empresas a alcanzar sus objetivos estratégicos y operativos mediante el uso efectivo de la tecnología de la información.

- **CIS Controls:** Los CIS Controls son un conjunto de 20 controles críticos de seguridad de la información que se han desarrollado a partir de una revisión exhaustiva de los ataques cibernéticos más comunes. Estos controles están diseñados para ayudar a las organizaciones a proteger sus sistemas de información contra las amenazas más comunes.

- **ITIL:** La Biblioteca de Infraestructura de Tecnología de la Información (ITIL) es un marco de referencia para la administración de servicios de TI que incluye una serie de mejores prácticas para la administración

de la seguridad de la información. ITIL se enfoca en la prestación de servicios de TI efectivos y eficientes, lo cual incluye la protección de los activos de información de una organización.

Existen numerosos marcos de referencia disponibles, cada uno con su propio enfoque y conjunto de prácticas recomendadas. Es fundamental evaluar minuciosamente cada marco de referencia y determinar cuál es el más apropiado para las necesidades y objetivos específicos de su organización.

Se agruparán en parejas, con el fin de crear una infografía que represente los distintos marcos de referencia disponibles y que muestre los aspectos principales para seleccionar el más adecuado para la organización.

A continuación, se presentan algunas sugerencias para crear la infografía:

• Seleccione el tema de la infografía.

- Identifique las fuentes de información.
- Organice las ideas.
- Diseñe la infografía.
- Realice un boceto o borrador de cómo desea presentar la información.
- Puede utilizar herramientas en línea para crear infografías como Canva, Adobe Spark, Visme.co, Venngage.com, PiktoChart, Easel.ly, Nubedepalabras.es e incluso el programa de presentaciones PowerPoint.

Busque en Internet ejemplos de infografías que le permitan crear un diseño visualmente estructurado y coherente con lo solicitado en la evidencia. El formato de entrega debe ser en PDF.

Duración: 25 horas.

Evidencia: Infografía en formato PDF

Ambiente requerido: Ambiente de aprendizaje, Computador, Internet.

Materiales: Computadores, Internet, Video Beam o Televisor.

3.3.2. Analizar el modelo de negocio e Identificar los activos críticos en una organización.

Parte esencial de la seguridad de la información y la ciberseguridad comienza por comprender y reconocer el funcionamiento de las empresas y organizaciones; lo que implica realizar un análisis de los recursos tecnológicos y otros dispositivos que permiten que la empresa logre alcanzar los objetivos empresariales.

Es de suma importancia entender los principios básicos que deben ser utilizados por los responsables de la seguridad de la información para implementar la gestión y clasificación de activos que son manejados por la entidad, con el objetivo de determinar qué activos posee, cómo deben ser utilizados, los roles y responsabilidades que tienen los usuarios sobre ellos, y reconociendo además el nivel de clasificación de la información que a cada activo debe asignársele. También poder Identificar los activos críticos, los riesgos asociados y los controles de seguridad necesarios para proteger los activos.

Para el desarrollo de esta actividad es importante la lectura y análisis del material adjunto "Ciberseguridad y seguridad de la información". A partir de la reflexión descrita y con base en lo consultado elabore un informe detallado en el que describa:

- ¿Cuáles son los activos físicos o intangibles informáticos con que cuenta su organización que están relacionados o requeridos para el cumplimiento de los objetivos empresariales? o ¿Cómo debe ser la clasificación de la organización?

- ¿Qué metodologías o estándares puede utilizar para llevar a cabo el proceso de valoración de activos?

- Por otro lado, teniendo en cuenta el caso de estudio definido en el material de formación, plantee la identificación y clasificación de los activos.

- Defina el estándar o el marco de referencia que más se ajusta al estudio de caso.

Se organizarán en parejas, para entregar un documento escrito con el informe del análisis y valoración de activos para el caso propuesto, el cual debe contener portada, informe y bibliografía enmarcada bajo las normas APA.

Duración: 20 horas.

Evidencia: Informe con normas APA en formato PDF.

Ambiente requerido: Ambiente de aprendizaje, Computador, Internet.

Materiales: Computadores, Internet, Video Beam o Televisor.

3.4. Actividad de transferencia del conocimiento: Crear la matriz de riesgos informáticos de la organización.

Es esencial en términos de seguridad de la información y ciberseguridad la identificación de riesgos informáticos, siendo el insumo esencial que permite evaluar y planificar un conjunto de acciones que determinen el plan de tratamiento de los riesgos obtenidos, de manera que se puedan mitigar o controlar.

Por lo tanto, la importancia de adquirir los conocimientos relacionados con la elaboración de una matriz de riesgos informáticos a través de la aplicación de un formato ya establecido, siguiendo las recomendaciones hechas por la Norma ISO 27001.

Para llevar a cabo esta actividad, es importante leer y analizar el material "Formato matriz de riesgo" y retomar el caso de estudio propuesto. En la actividad, se debe aplicar el formato "Anexo 1. Matriz_Riesgo.xls" adjunto a esta guía. De acuerdo con lo anterior, tenga en cuenta:

- La clasificación según el análisis previo de los tipos de criterios que podrían afectar al activo.
- El formato debe mostrar los tipos de riesgos encontrados en el caso.
- En el formato se debe incluir la evaluación de las posibles amenazas que podrían tener algún efecto sobre los activos.

La evidencia se entregará de manera individual, utilizando como insumo para el proceso el caso de estudio propuesto. Se entregará el archivo en hoja de cálculo con los datos del aprendiz.

Duración: 20 horas.

Evidencia: Matriz de riesgos diligenciada en formato hoja de cálculo.

Ambiente requerido: Ambiente de aprendizaje, Computador, Internet.

Materiales: Computadores, Internet, Video Beam o Televisor.

4. ACTIVIDADES DE EVALUACIÓN

Evidencias de Aprendizaje	Criterios de Evaluación	Técnicas e Instrumentos de Evaluación
Evidencias de Conocimiento : • Mapa mental sobre conceptos técnicos de seguridad. • Infografía sobre marcos de	Recopilar información de incidentes de seguridad digital según criterios técnicos, marcos de referencia y modelo del negocio. Interpreta la normativa de	**Técnica de Evaluación:** Formulación de Preguntas. **Instrumento de Evaluación:** Cuestionario.

referencia disponibles para la gestión de la seguridad de la información y el control de los sistemas de información. **Evidencias de Desempeño** • Exposición sobre los criterios técnicos relevantes sobre incidentes de seguridad digital **Evidencias deProducto:** Informe del análisis y valuación de activos para el caso propuesto,	gestión de incidentes de ciberseguridad según estándares vigentes. Reconoce y asume las funciones y responsabilidadespropias de su rol dentro de la estructura del equipo de respuestas de incidentes deseguridad. Interpreta los procesos de gestión de incidentes de seguridad digital según normativa vigente. Reconoce y aplica procedimientos de reporte y escalada de incidentes de seguridad digital según procesos definidos por el equipo de respuesta aincidentes. Utiliza herramientas de hardware y software de seguridad digital para el monitoreo y gestión de eventos de seguridad segúnlas especificaciones de los manuales técnicos.	**Técnica de Evaluación:** Observación Directa. **Instrumento de Evaluación:** Lista de Chequeo **Técnica de Evaluación:** Valoración del producto. **Instrumento de Evaluación:** Lista de Chequeo.

5. GLOSARIO DE TÉRMINOS

Activo: En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de la misma (sistemas, soportes, edificios, personas, etc.) que tenga valor para la entidad.

Cadena de Custodia: Es un procedimiento documentado y controlado que se le aplica a toda evidencia física o elemento material probatorio desde su recolección hasta su disposición final, en donde se puede observar su descripción e identificación, una línea de tiempo, y las personas que han participado en su custodia.

Evento de Seguridad: Ocurrencia identificada de un estado en un sistema de información, servicio o red de telecomunicaciones, que indica una posible brecha de seguridad, falla de un control o una condición no identificada que puede ser relevante para la seguridad de la información.

ERISI: Equipo de Respuesta a Incidentes de Seguridad de la Información.

Estampa de Tiempo: Certificar mediante una secuencia de caracteres, que un conjunto de datos ha existido y no ha sido modificado en un espacio de tiempo determinado. La secuencia de caracteres está relacionada con la fecha y el momento en que ocurre dicho evento y específicamente cuando fue creado en un sistema de cómputo.

Hardening: (ingles: endurecimiento) es el proceso de asegurar un sistema informático mediante la reducción de vulnerabilidades en el mismo, esto se logra eliminando software, servicios, usuarios innecesarios en el sistema, así como cerrando puertas de acceso que tampoco estén en uso.

Incidente de Seguridad: Evento único o serie de eventos de seguridad de la información inesperados o no deseados, que poseen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información.

Informática Forense: Es la aplicación de técnicas científicas y analíticas especializadas a infraestructura de TIC, que permiten identificar, preservar, analizar, custodiar y presentar datos – Evidencia Digital – de tal manera que sean válidos dentro de un proceso legal y/o administrativo preservando su valor probatorio.

Integridad: Propiedad de la información relativa a su exactitud y completitud.

Imagen Forense: Copia binaria de la información que se encuentra en un medio de almacenamiento, la cual es trasladada a otro, sin que se cambien ninguna de sus características y/o atributos.

Lugar de la Escena: Lugar de ocurrencia de un incidente y/o evento de seguridad. Entiéndase en la investigación como cualquier lugar mueble o inmueble donde se presuma la comisión de un hecho en contra de la norma y el sitio en donde se sospeche la presencia de elementos materia de prueba y evidencia física relacionados con la misma.

Técnicas HASHING o CHECKSUMS: Son funciones matemáticas y algorítmicas que tiene como propósito principal detectar cambios en una secuencia de datos para proteger la integridad de estos, verificando que no haya discrepancias entre los valores obtenidos al hacer una comprobación inicial y otra final tras el tratamiento realizado.

Vulnerabilidad: Debilidad de un activo o control que pueda ser explotado por una o más amenazas.

6. REFERENTES BILBIOGRÁFICOS

- Barrett, M. P. (2018). Framework for improving critical infrastructure cybersecurity. *National Institute of Standards and Technology, Gaithersburg, MD, USA, Tech.* http://isawaterwastewater.com/wpcontent/uploads/2018/08/WWAC-2018-NIST-Barrett_final.pdf

- Matalobos, J. M. (2009). *Análisis de riesgos de seguridad de la información*. [Tesis de grado, Universidad Politécnica de Madrid, Madrid]. Repositorio Institucional UPM. https://www.upm.es/Estudiantes/Estudios_Titulaciones/Estudios_Doctorado/Tesis/TesisDeposit o

- National Institute of Standards and Technology. (2018). *Cybersecurity Framework.* Framework for Improving Critical Infrastructure Cybersecurity, versión 1.1., p. 1-48.

http://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

- Portal de Administración Electrónica. (2012). *MAGERIT – versión 3.0. Metodología de análisis y gestión de riesgos de los sistemas de información. Libro I – Método.* Ministerio de Hacienda y Administraciones Públicas, Secretaría General Técnica Subdirección General de Información, Documentación y Publicaciones Centro de Publicaciones Gobierno de España. https://www.ccncert.cni.es/documentos-publicos/1789-magerit-libro-i-metodo/file.html

- Sena, L. y Tenzer, S. M. (2004). *Introducción a Riesgo informático. Cátedra Introducción a la Computación.* Universidad de la República, Facultad de Ciencias Económicas y de Administración. Montevideo.

- https://www.academia.edu/6410062/FCEA_C%C3%A1tedra_Introducci%C3%B3n_a_la_Computaci%C3%B3n_Introducci%C3%B3n_a_Riesgo_Inform%C3%A1tico

- Soriano, M. (2014). *Seguridad en redes y seguridad de la información*. Improvet. https://www.academia.edu/40156122/Seguridad_en_redes_y_seguridad_de_la_informaci%C3% B3n

- SGSI – 08. (2010). *Análisis y valoración de riesgos. Metodologías*. [Video]. YouTube. https://www.youtube.com/watch?v=g7EPuzN5Awg

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

7. CONTROL DEL DOCUMENTO

	Nombre	Cargo	Dependencia	Fecha
Autor (es)	**Janeth Patricia Chacón**	**Instructora**	**CEAI**	**Noviembre 2022**

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

	Nombre	Cargo	Dependencia	Fecha	Razón del Cambio
Autor (es)	**Janeth Patricia Chacón**	**Instructora**	**CEAI**	**Diciembre 2022**	**Construcción de actividades**