PROCESO DIRECCIÓN DE FORMACIÓN PROFESIONAL INTEGRAL
FORMATO GUÍA DE APRENDIZAJE

1. Identificación de la guía de aprendizaje

- **Denominación del programa de formación:** Apropiación de los conceptos en ciberseguridad
- **Código del programa de formación**: 23310008
- **Nombre del proyecto (si es formación titulada):** N/A
- **Fase del proyecto (si es formación titulada):** N/A
- **Actividad de proyecto (si es formación titulada):** N/A
- **Competencia**: 220501108. Diagnosticar la seguridad de la información de acuerdo con métodos de análisis y normativa técnica.
- **Resultados de aprendizaje a alcanzar**:
    - 220501108-01. Valorar activos de información de acuerdo con métodos y criterios técnicos de evaluación.
    - 220501108-02. Implementar el mapa de amenazas de acuerdo con métodos de análisis, criterios técnicos y marcos de referencia.
    - 220501108-03. Estructurar el mapa de riesgos de ciberseguridad de acuerdo con los activos de información de la organización, la normativa y los estándares técnicos.
    - 220501108-04. Gestionar los procesos críticos de ciberseguridad de acuerdo con criterios técnicos y los objetivos de la organización.

- **Duración de la guía**: 48 horas.

2. Presentación

Estimado aprendiz en esta guía se describen las actividades de aprendizaje del programa denominado "**Apropiación de los conceptos en ciberseguridad"**, en las cuales puede conocer los conceptos iniciales de la seguridad de la información, clasificación, análisis y valuación de activos y riesgos informáticos a través de la construcción de la matriz de riesgos, el plan de tratamiento de los peligros identificados y la información general de los sistemas de gestión de seguridad de la información de acuerdo con el estándar internacional ISO 27001:2017.

Para el desarrollo de las actividades planteadas cuenta con el acompañamiento del instructor asignado al programa, que de forma continua y permanente lo orienta con las pautas necesarias para el logro de las actividades de aprendizaje, brindando herramientas básicas de tipo conceptual y metodológico.

El instructor programa encuentros de asesoría virtual para brindar orientaciones específicas relacionadas con las temáticas a desarrollar en las actividades.

Es importante que organice su tiempo con un promedio de trabajo diario de dos horas, dada la exigencia que demanda la realización de las actividades mencionadas en esta guía de aprendizaje. No olvide revisar y explorar los materiales de estudio del programa.

Downloaded by william sepulveda (sepul204@gmail.com)

3. Formulación de las actividades de aprendizaje

Como requisito para el desarrollo del presente curso es importante que reconozca el espacio de trabajo, junto con las posibilidades que tiene para interactuar, comunicar, visualizar y poder utilizar las herramientas necesarias en el LMS desde su rol de aprendiz. Además, la invitación es a que realice las siguientes acciones:

- Inicie la socialización con los participantes de la formación a través del "Foro social". Participe de forma activa, dando respuesta a las preguntas planteadas y compartiendo un poco de su quehacer diario con sus demás compañeros.
- Consulte el apartado "Información general", en este espacio se muestra la metodología y el diseño curricular del programa de formación en curso, esto le permite entender los objetivos, las actividades y la metodología a desarrollar durante el proceso.
- Tenga en cuenta entender los pasos y reconocer las actividades a realizar, lo cual le permite tener un estimado del tiempo de dedicación y así, planear el cumplimiento de los requisitos de acuerdo con su tiempo disponible.

3.1. Actividad de aprendizaje 1. Realizar la valuación de los activos de la organización

Reflexión inicial

Parte fundamental de la seguridad de la información y la ciberseguridad empieza por entender y reconocer el funcionamiento de las empresas y organizaciones; lo que implica hacer un análisis de los recursos tecnológicos y demás dispositivos que permiten que la empresa logre cumplir con los objetivos empresariales.

Es de suma importancia entender los lineamientos básicos que deben ser utilizados por los responsables de la seguridad de la información para poner en marcha la gestión y clasificación de activos que son manejados por la entidad, con el fin de determinar qué activos posee, cómo deben ser utilizados, los roles y responsabilidades que tienen los usuarios sobre los mismos, y reconociendo adicionalmente el nivel de clasificación de la información que a cada activo debe dársele.

Duración: 12 horas.

Materiales de formación: para el desarrollo de esta actividad es importante la lectura y análisis del componente formativo "Ciberseguridad y seguridad de la información."

Evidencia: a continuación, se describe la acción y la correspondiente evidencia que conforma la actividad de aprendizaje.

A partir de la reflexión descrita y con base en lo consultado en el componente formativo elabore un informe detallado en el que describa:

- ¿Cuáles son los activos tangibles o intangibles informáticos con que cuenta su organización que están relacionados o requeridos para el cumplimiento de los objetivos empresariales?
- ¿Cómo debe ser la clasificación de la organización?
- ¿Qué metodologías o estándares puede utilizar para realizar el proceso de valuación de activos?

Downloaded by william sepulveda (sepul204@gmail.com)

- 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.

- **Producto a entregar:** documento escrito con el informe del análisis y valuación de activos para el caso propuesto.

- **Formato**: crear un documento y exportarlo a PDF, el cual debe contener portada, informe y bibliografía enmarcada bajo las normas APA.

- Para hacer el envío del producto remítase al área de la actividad correspondiente y acceda al espacio para el envío de la evidencia **AA1_EV01_Informe del análisis y valuación de activos**

3.2. Actividad de aprendizaje 2. Clasificar y evaluar las amenazas y vulnerabilidades

Posterior al análisis y valuación de activos se debe realizar la tarea de identificar, caracterizar, clasificar y evaluar las amenazas y vulnerabilidades que pueden afectar en algún momento el correcto funcionamiento de los activos informáticos importantes y/o necesarios para el cumplimiento de los objetivos empresariales.

Esto nos lleva a la necesidad del estudio de diferentes metodologías de análisis y valuación de activos, dentro de las más utilizadas y de mayor popularidad es la definición e implementación de los sistemas de gestión de seguridad de la información a través la aplicación del estándar NIST SP 830.

Duración: 12 horas.

Materiales de formación: para el desarrollo de esta actividad es importante la lectura y análisis del componente formativo “Metodologías de análisis y evaluación de riesgos”.

Evidencia: a continuación, se describe la acción y la correspondiente evidencia que conforma la actividad de aprendizaje.

Realice una infografía en la que represente los tres tipos de categorías (naturales, humanas y entorno) que muestre los aspectos principales sobre la aplicación de dicha metodología de análisis y evaluación de riesgos en la situación planteada.

Lineamientos para la entrega de la evidencia:

A continuación, algunas recomendaciones para realizar la infografía:

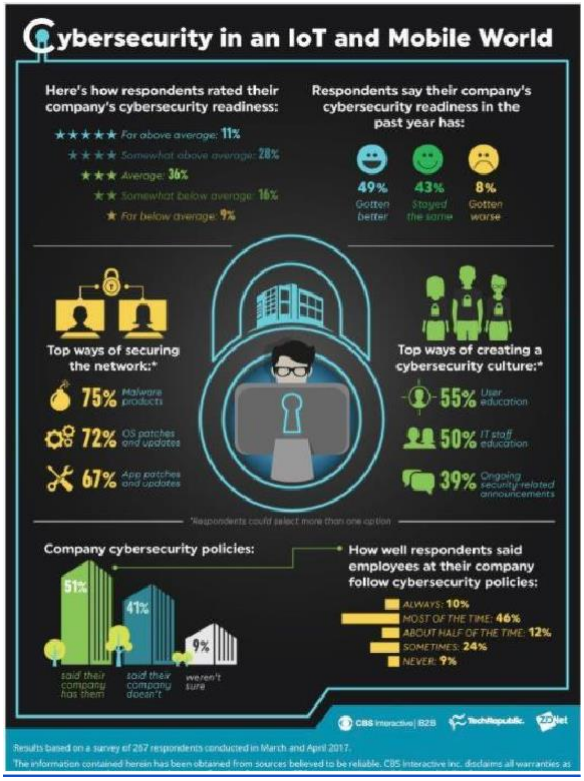
- Elija el tema de la infografía.
- Identifique las fuentes de información.
- Organice las ideas.
- Diseñe la infografía. Realice un bosquejo o borrador de cómo quiere presentar la información.
- Puede utilizar herramientas web para crear infografías como Canva, Adobe Spark, Visme.co, Venngage.com, PiktoChart, Easel.ly, Nubedepalabras.es e incluso el presentador de diapositivas PowerPoint.

Downloaded by william sepulveda (sepul204@gmail.com)

Revise a través de Internet ejemplos de infografías que le permitan realizar una pieza gráfica visualmente estructurada y consecuente con lo requerido en la evidencia:

Figura 1

Infografía – Ciberseguridad en un mundo IoT y Móvil



Nota. IoT World Online. (2017, noviembre 14). Infografía – Ciberseguridad en un mundo IoT y Móvil. [Web log post]. *Blog de Internet de las cosas (IoT)*. https://www.iotworldonline.es/infografia-ciberseguridad-mundo-iot-movil/

- **Producto a entregar:** una infografía de la aplicación de una metodología de análisis y evaluación de riesgos.
- **Formato:** archivo en formato PDF.
- Para hacer el envío del producto remítase al área de la actividad correspondiente y acceda al espacio para el envío de la evidencia **AA2_EV01_Infografía**

3.3. Actividad de aprendizaje 3. Crear la matriz de riesgos de la organización

Es fundamental a partir de seguridad de la información y ciberseguridad la identificación de riesgos informáticos, siendo el insumo fundamental que permite evaluar y planear un conjunto de acciones que determinen el plan de tratamiento de los riesgos obtenidos, de tal manera que se puedan mitigar o controlar.

De ahí la importancia de adquirir los conocimientos referentes a la construcción de una matriz de riesgos informáticos mediante la aplicación de un formato ya preestablecido, siguiendo las recomendaciones hechas por la Norma ISO 27001.

Downloaded by william sepulveda (sepul204@gmail.com)

Duración: 12 horas.

Materiales de formación: para el desarrollo de esta actividad es importante la lectura y análisis del componente formativo “Formato matriz de riesgo” y retomar el caso de estudio propuesto en el punto 6 de “Ciberseguridad y seguridad de la información”.

Evidencia: a continuación, se describe la acción y la correspondiente evidencia que conforma la actividad de aprendizaje.

Para el desarrollo de esta actividad tenga en cuenta el caso planteado en el punto 6 del componente formativo denominado “Ciberseguridad y seguridad de la información”, en la actividad debe aplicar el formato “**Anexo 1. Matriz_Riesgo.xls”** anexo a esta guía.

De acuerdo con lo anterior tenga en cuenta:

- La clasificación según el análisis previo a los tipos de criterios que podría ver afectado el activo.
- El formato debe mostrar los tipos de riesgos encontrados en el caso.
- En el formato se debe ver la valuación de las posibles amenazas que podrían surtir algún efecto sobre los **activos**.

Lineamientos para la entrega de la evidencia:

- **Producto a entregar:** matriz de riesgos diligenciada, utilizando como insumo para el proceso el caso de estudio propuesto en el punto 6 del material de formación denominado “Ciberseguridad y seguridad de la información”.

- **Formato**: archivo en hoja de cálculo con los datos del aprendiz.

- Para hacer el envío del producto remítase al área de la actividad correspondiente y acceda al espacio para el envío de la evidencia **AA3_EV01_Formato matriz de riesgo**

3.4 Actividad de aprendizaje 4. Conocer la Norma ISO 27001

Los sistemas de gestión de seguridad de la información o SGSI es un término que se utiliza en la Norma Internacional ISO 27001 para referirse al conjunto de políticas, normas y controles que se aplican en una organización para garantizar el cumplimiento de los pilares de la seguridad de la información como lo son la integridad, la disponibilidad y la confidencialidad.

Con esta actividad se logra hacer una introducción general a los sistemas de gestión de seguridad de la información según la Norma ISO 27001, sus fases, actividades y las recomendaciones según la Norma ISO.

Duración: 12 horas.

Materiales de formación: para el desarrollo de esta actividad es importante la lectura y análisis del componente formativo “El sistema de gestión de seguridad de la información”.

Evidencia: a continuación, se describe la acción y la correspondiente evidencia que conforma la actividad de aprendizaje.

Downloaded by william sepulveda (sepul204@gmail.com)

Diseñe un diagrama de tipo mapa mental en el que especifique las fases y las actividades más importantes de cada una de ellas en la implementación de un SGSI.

Lineamientos para la entrega de la evidencia:

- **Producto a entregar:**

- Esquema gráfico tipo mapa mental que dé respuesta a las indicaciones señaladas para su elaboración. Considere las referencias en el material de formación, además de contener los elementos necesarios para la elaboración, integre el uso de convenciones, ramificaciones, colores, imágenes e íconos que permitan su organización y comprensión.
- Si desea puede indagar a través de la Web sobre la estructura de un mapa mental.
- Puede realizarlo en una herramienta digital como Goconqr, Draw.io, Mindomo incluso en el procesador de palabras Word o el presentador de diapositivas PowerPoint, teniendo en cuenta la mejor opción que se adecue a su estilo de aprendizaje.

- Se debe generar y entregar en formato PDF.

- Para hacer el envío del producto remítase al área de la actividad correspondiente y acceda al espacio para el envío de la evidencia **AA4_EV01_Mapa mental**

Total horas actividad de aprendizaje: 48 horas; 12 directas (D), 36 independientes (I).

4. Actividades de evaluación

Evidencias de aprendizaje	Criterios de evaluación	Técnicas e instrumentos de evaluación
Evidencia de producto AA1_EV01_Informe del análisis y valuación de activos	• Clasifica los activos de información de acuerdo con los criterios técnicos de evaluación y marcos de referencia. • Identifica el ámbito de aplicación de ciberseguridad de acuerdo con los activos de información de la organización, la normativa y los estándares técnicos. • Determina el contexto de los activos de información acorde con las técnicas de análisis y tipo de negocio.	Lista de chequeo
Evidencia de desempeño AA2_EV01_Infografía	• Clasifica las amenazas y vulnerabilidades de ciberseguridad de acuerdo con la	Lista de chequeo

Downloaded by william sepulveda (sepul204@gmail.com)

	normativa y los estándares técnicos. • Evalúa vulnerabilidades acorde con técnicas de análisis y criterios técnicos.	
Evidencia de producto AA3_EV01_Formato matriz de riesgo	• Identifica factores de riesgo de acuerdo con metodologías de análisis y evaluación, y criterios técnicos. • Valora el impacto y la probabilidad de los riesgos de acuerdo con metodologías de análisis y evaluación, criterios técnicos y marcos de referencia. • Infiere las consecuencias de los riesgos de acuerdo con criterios técnicos y los objetivos del negocio.	Lista de chequeo
Evidencia de conocimiento AA4_EV01_mapa mental	• Analiza los objetivos de seguridad de la información de acuerdo con procedimientos técnicos y requisitos de negocio. • Aplica los controles y lineamientos de ciberseguridad de los activos de información de la organización de acuerdo con criterios técnicos y los objetivos del negocio. • Consolida activos de información de acuerdo con criterios técnicos de evaluación.	Lista de chequeo

5. Glosario de términos

Activo: el término de activo de información se relaciona con todos esos elementos tecnológicos o relacionados con la tecnología que la organización utiliza para el cumplimiento de sus metas o *core* del negocio. Según la Norma ISO/IEC 27001 se entiende como activo todo aquello que es importante y que la organización valora, por lo tanto, debe de protegerse.

Amenaza: cualquier evento que puede afectar los activos de información y se relaciona, principalmente, con recursos humanos, eventos naturales o fallas técnicas.

CISO: Chief Information Security Officer (Oficial de seguridad de la información).

Downloaded by william sepulveda (sepul204@gmail.com)

Clasificación de la información: es el ejercicio por medio del cual se determina que la información pertenece a uno de los niveles de clasificación estipulados en la entidad. Tiene como objetivo asegurar que la información recibe el nivel de protección adecuado.

Confidencialidad: propiedad que determina que la información solo esté disponible y sea revelada a individuos, entidades o procesos autorizados.

Disponibilidad: propiedad de que la información sea accesible y utilizable por solicitud de una entidad autorizada, cuando esta así lo requiera.

Integridad: propiedad de salvaguardar la exactitud y estado completo de los activos.

Riesgo: es la posibilidad de que una amenaza se produzca, dando lugar a un ataque sobre un recurso o servicio tecnológico. Esto no es otra cosa que la probabilidad de que ocurra el ataque por parte de la amenaza.

SGSI: Sistema de gestión de seguridad de la información.

SP-830: método de análisis de gestión del riesgo para el aseguramiento de los sistemas de información que almacenan, procesan y transmiten información.

Vulnerabilidad: es una debilidad o fallo en un sistema de información que pone en riesgo la seguridad de la información, en la que se permite que un atacante pueda comprometer la integridad, disponibilidad o confidencialidad de la misma.

6. Referentes bibliográficos

Barrett, M. P. (2018). Framework for improving critical infrastructure cybersecurity. *National Institute of Standards and Technology, Gaithersburg, MD, USA, Tech.* http://isawaterwastewater.com/wp-content/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/TesisDeposito

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.ccn-cert.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.

Downloaded by william sepulveda (sepul204@gmail.com)

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

7. Control del documento

	Nombre	**Cargo**	**Dependencia** *(Para el SENA indicar Regional y Centro de formación)*	**Fecha**
Autor (es)	Henry Eduardo Bastidas Paruma	Instructor	Regional Cauca, Centro de Teleinformática y Producción Industrial	Diciembre 2020
	Carlos Andrés Rodríguez	Diseñador Instruccional	Centro de Diseño y Metrología -– Regional Bogotá	Diciembre 2020
	Oscar Absalón Guevara	Evaluador Instruccional	Centro de Gestión Industrial – Regional Bogotá	Febrero 2021
	Rafel Neftalí Lizcano Reyes	Adecuador Pedagógico Ecosistema RED	Centro Industrial del Diseño y la Manufactura - Regional Santander	
	Julia Isabel Roberto	Diseñadora y evaluadora instruccional	Centro para la Industria de la Comunicación Gráfica – Regional Distrito Capital	Abril 2021

8. Control de cambios

	Nombre	**Cargo**	**Dependencia**	**Fecha**	**Razón del cambio**
Autor (es)					

Downloaded by william sepulveda (sepul204@gmail.com)