



PROCESO DIRECCIÓN DE FORMACIÓN PROFESIONAL INTEGRAL FORMATO GUÍA DE APRENDIZAJE

1. Identificación de la guía 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

Estimado aprendiz esta guía pretende orientarlo para que pueda adquirir 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 realizarán 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/o aplicaciones de sistemas de información que puedan comprometer la integridad de los datos, clasificar, analizar y valorar los activos, así como los 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.

Es importante que organice su tiempo con un promedio de trabajo diario de dos horas adicionales por fuera de la formación para esta competencia, 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 propuestos para esta competencia de aprendizaje.



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 tanto en el ambiente de aprendizaje como en el LMS Zajuna en su rol de aprendiz. Además, la invitación es a que realice las siguientes acciones:

- Tenga en cuenta entender los pasos y reconocer las actividades a realizar previamente impartidas y propuestas por su instructor(a), lo cual le permite tener un estimado del tiempo de dedicación y así planear el cumplimiento de los requisitos de acuerdo con las actividades a entregar.

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?



- 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:

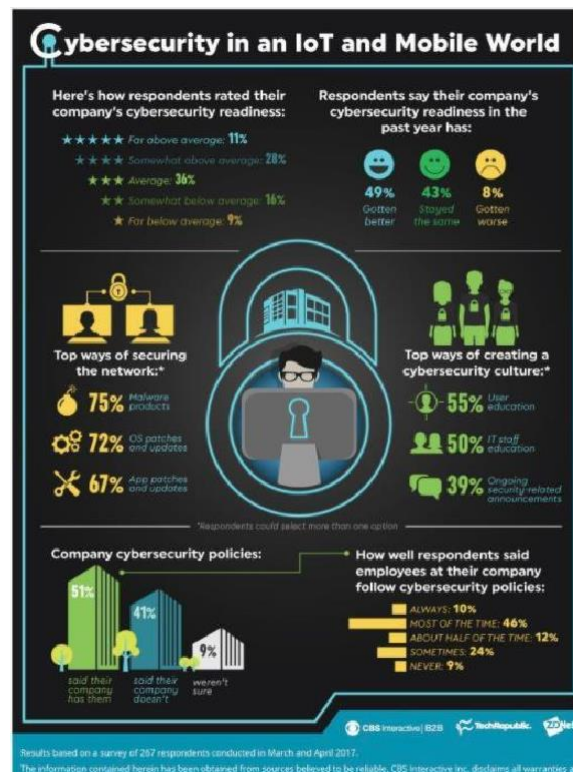
- Elija el tema de la infografía.
- Identifique las fuentes de información.
- Organice las ideas.
- Diseñe la infografía. Realice un bosquejo o borrador de cómo quiere presentar la información.
- Puede utilizar herramientas web para crear infografías como Canva, Adobe Spark, Visme.co, Venngage.com, PiktoChart,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



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.



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.

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**.

3.5. Actividad de aprendizaje 5. Análisis Forense Inyección de Código

A partir de esta actividad se realizarán actividades enfocadas al análisis forense. El análisis forense es la aplicación de técnicas científicas y analíticas especializadas a infraestructuras tecnológicas que permiten identificar, preservar, analizar y presentar datos válidos que puede usarse en un proceso legal.

Dichas técnicas incluyen reconstruir elementos informáticos, examinar datos residuales, autenticar datos y explicar las características técnicas del uso de datos y bienes informáticos.

Esta disciplina no sólo hace uso de tecnologías de punta para mantener la integridad de los datos y del procesamiento de los mismos; sino que también requiere de una especialización y/o formación y conocimientos avanzados de informática y sistemas para identificar lo que ha ocurrido dentro de cualquier dispositivo electrónico. La formación de un informático forense o técnico en análisis forense abarca no sólo el conocimiento del software, sino también de hardware, redes, seguridad, piratería, hackeo y recuperación de información.

La informática forense ayuda a detectar pistas sobre ataques informáticos, robos de información, conversaciones o para recolectar evidencias en correos electrónicos y chats.

La evidencia digital o electrónica es sumamente frágil, de ahí la importancia de mantener su integridad; por ejemplo, el simple hecho de pulsar dos veces en un archivo modificaría la última fecha de acceso del mismo.



Dentro del proceso del cómputo forense, un examinador forense digital puede llegar a recuperar información que haya sido borrada y/o secuestrada desde el sistema operativo. El Técnico en Control de Seguridad Digital debe tener muy presente principios básicos como el principio de intercambio de Locard por su importancia en el análisis criminalístico, así como el estándar de Daubert para hacer admisibles en juicio las pruebas presentadas por el experto forense entre otros.

Es muy importante mencionar que la informática o el cómputo forense no tiene como objetivo prevenir delitos, por lo que resulta imprescindible tener claros los distintos marcos de actuación de la informática forense, la seguridad y la auditoría informáticas, es decir ya se centra en entrar a analizar lo sucedido después de la comisión del delito informático y esto permitirá a futuro poder prevenir y/o asegurar con mejores herramientas la preservación de la información.

Uno de los delitos informáticos mas comunes es la inyección de código, el cual por ejemplo puede extraer información de bases de datos destruirla o secuestrarla para posteriormente el ciberdelincuente pedir rescate o usar esta información confidencial de manera ilegal.

Duración: 20 horas.

Materiales de formación: para el desarrollo de esta actividad es importante atender de manera clara y concisa las indicaciones del instructor y las recomendaciones que se dan en el material de estudio “Prevención en la inyección de código y como combatirlo”.

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

Realice una pequeña aplicación de un sistema de información el cual evite el envío de caracteres especiales o caracteres ASCII especiales a un sistema que negocie con una base de datos.

Lineamientos para la entrega de la evidencia:

A continuación, algunas recomendaciones para realizar la actividad:

- Elija el lenguaje de programación de su preferencia
- Escoja la base de datos de su preferencia.
- Determine la seguridad que implementara en el código.
- Pruebe mediante ensayo error la aplicación en un hosting.
- Puede utilizar herramientas Apache.
- Debe entregar un link donde el instructor verificara la seguridad de la aplicación.
- Para hacer el envío del producto remítase al área de la actividad correspondiente y acceda al espacio para el envío de la evidencia **AA5_EV01_Aplicacion con seguridad anti inyección de código.**

3.6. Actividad de aprendizaje 6. Análisis Forense Ataque por Ingeniería Social

Los ataques de ingeniería social manipulan a las personas para que compartan información que no deberían compartir, descarguen software que no deberían descargar, visiten sitios web que no deberían visitar, envíen dinero a delincuentes o cometan otros errores que comprometan su seguridad personal u organizacional.

Dado que la ingeniería social utiliza la manipulación psicológica y explota los errores o debilidades humanas en

GFPI-F-135 V04



lugar de las vulnerabilidades técnicas o digitales de los sistemas, a veces se la denomina «hackeo humano».

Los ciberdelincuentes utilizan con frecuencia tácticas de ingeniería social para obtener datos personales o información financiera, incluidas credenciales de inicio de sesión, números de tarjetas de crédito, números de cuentas bancarias y números de Seguro Social. Utilizan la información que han robado para el robo de identidad, lo que les permite realizar compras utilizando el dinero o crédito de otras personas, solicitar préstamos en nombre de otra persona, solicitar beneficios de desempleo de otras personas y más. Pero un ataque de ingeniería social también puede ser la primera fase de un ciberataque a gran escala. Por ejemplo, un ciberdelincuente podría engañar a una víctima para que comparta un nombre de usuario y una contraseña. Luego, utilice esas credenciales para plantar ransomware en la red del empleador de la víctima.

Duración: 12 horas.

Materiales de formación: para el desarrollo de esta actividad es importante atender de manera clara y concisa las indicaciones del instructor y las recomendaciones que se dan en el material de estudio “Prevención en el ataque por Ingeniería Social y como combatirlo”.

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

Identificará una aplicación de un sistema de información que pueda ser potencialmente usado para un ataque ciber social ya sea este spam o virus, el cual determinará como menguar, disminuir o prevenir un futuro ataque con este tipo de aplicación.

Lineamientos para la entrega de la evidencia:

A continuación, algunas recomendaciones para realizar la actividad:

- Elija la aplicación y/o sistema de información tipo spam o virus que usted crea es potencialmente peligrosa en seguridad
- Realice un análisis de esta aplicación aplicando una técnica forense.
- Determine la seguridad que implementará y/o técnica de prevención en el potencial ataque.
- Pruebe mediante ensayo error su técnica de prevención.
- Debe entregar un link donde el instructor verifique la medida tomada con la aplicación.
- Para hacer el envío del producto remítase al área de la actividad correspondiente y acceda al espacio para el envío de la evidencia **AA6_EV01_Análisis forense de spam para ciberataques.**



3.7. Actividad de aprendizaje 7. Sistemas Operativos Forenses



Los sistemas operativos forenses se utilizan para poder determinar en sitio o en laboratorios forenses la ocurrencia de ataques a equipos informáticos, los cuales han sido víctimas de hurto de información o usados para actividades delincuenciales.

Estos sistemas operativos están disponibles de manera gratuita, también hay otras que no son gratuitas y son costosas lo que las hace casi que de uso exclusivo de entidades gubernamentales o de uso de peritos forenses que trabajan para entidades como la policía de delitos informáticos, la fiscalía etc.

También se usan para poder recuperar o hallar información en equipos informáticos destruidos o dispositivos de almacenamiento destruidos o defectuosos mediante una técnica forense llamada autopsia informática.

IMAGENES FORENSES

Una imagen forense es una copia digital de la información y estructura lógica de un dispositivo de almacenamiento como puede ser un disco duro, memoria USB, DVD, Micro SD, etc. el cual es utilizado por un investigador forense digital para analizar la información capturada.

Las imágenes digitales forenses son la huella digital que guarda información valiosa que puede ser relevante para la investigación que se realiza.

Para la generación de imágenes digitales forenses se debe tomar en consideración el orden de volatilidad de la información a recuperar, considerando que es la información alojada en memoria RAM la más propensa a desaparecer si el equipo de computo o dispositivo a investigar se apaga de forma accidental.

Duración: 18 horas.

Materiales de formación: para el desarrollo de esta actividad es importante atender de manera clara y concisa las indicaciones del instructor y las recomendaciones que se dan en el material de estudio “Sistema



Operativo Forense Bento” y “ACCESSDATA FTK”

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

Usando el programa Bento o **ACCESSDATA FTK** el cual previamente ha sido contextualizado por el instructor(a), así como un caso de estudio propuesto, realizará un análisis forense de un equipo informático.

Lineamientos para la entrega de la evidencia:

A continuación, algunas recomendaciones para realizar la actividad:

- Elija un equipo y/o dispositivo informático para realizar la práctica
- Realice el análisis de la información obtenida.
- Obtenga la Imagen Forense
- Obtenga el volcado de memoria
- Haga un análisis forense del volcado de memoria.
- Debe entregar en formato PDF el análisis forense realizado.
- Para hacer el envío del producto remítase al área de la actividad correspondiente y acceda al espacio para el envío de la evidencia **AA7_EV01_Análisis forense con sistema operativo forense.**
-

3.8. Actividad de aprendizaje 8. Sistemas Operativos Forenses

Herramienta para análisis forense digital Autopsy



Autopsy es una herramienta digital usada para la recuperación de información en dispositivos de almacenamiento como lo es USBs formateadas, discos duros formateados, equipo de almacenamiento dañado etc.

Permite obtener y/o recuperar información en volcado de memoria donde se puede verificar también acceso a paginas para fines delictivos.

Es ampliamente usada por peritos forenses y/o entidades gubernamentales dedicadas a la investigación forense donde se deben recopilar evidencias para casos de investigación en delitos informáticos.

Duración: 12 horas.

Materiales de formación: para el desarrollo de esta actividad es importante atender de manera clara y concisa las indicaciones del instructor y las recomendaciones que se dan en el material de estudio “Sistema Operativo Forense Autopsy”

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



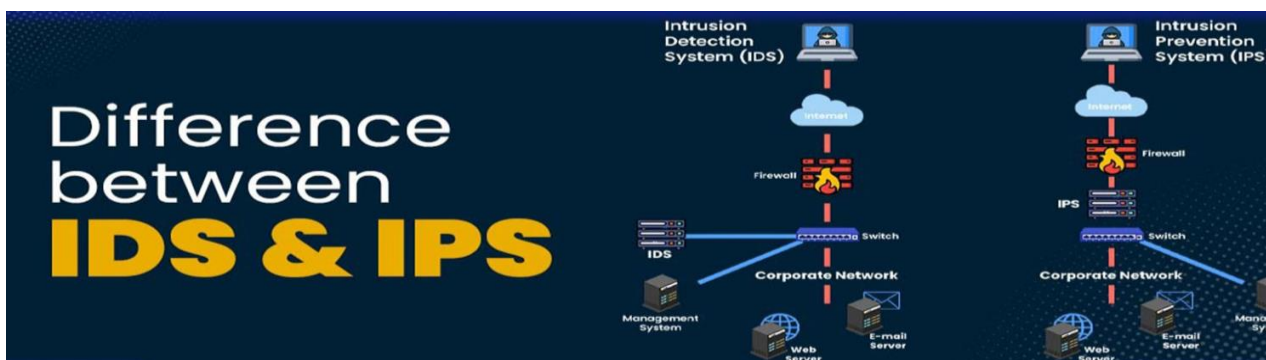
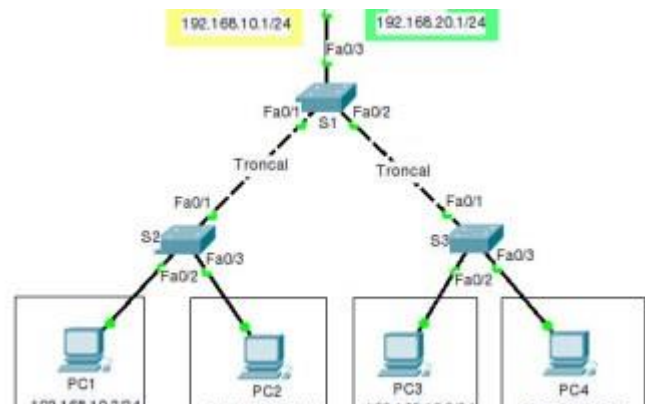
Usando el programa Autopsy el cual previamente ha sido contextualizado por el instructor(a), así como un caso de estudio propuesto, realizara un análisis forense de un equipo informático.

Lineamientos para la entrega de la evidencia:

A continuación, algunas recomendaciones para realizar la actividad:

- Elija un equipo y/o dispositivo informático para realizar la practica
- Realice el análisis de la información obtenida.
- Obtenga la Imagen Forense
- Obtenga el volcado de memoria
- Haga un análisis forense del volcado de memoria.
- Debe entregar en formato PDF el análisis forense realizado.
- Para hacer el envío del producto remítase al área de la actividad correspondiente y acceda al espacio para el envío de la evidencia **AA8_EV01_Analisis forense con sistema operativo Autopsy.**

3.9. Actividad de aprendizaje 9. Seguridad en puertos de redes



A partir de esta actividad se realizarán actividades enfocadas en seguridad en redes de datos.

La seguridad de red es cualquier actividad diseñada para proteger el acceso, el uso y la integridad de la red y los datos corporativos.

- Incluye tecnologías de hardware y software.



- Está orientada a diversas amenazas.
- Evita que ingresen o se propaguen por la red ataques.
- La seguridad de red eficaz administra el acceso a la red.

La seguridad de red combina varias capas de defensa en el perímetro y la red. Cada capa de seguridad de red implementa políticas y controles. Los usuarios autorizados tienen acceso a los recursos de red, mientras que se bloquea a los usuarios maliciosos para evitar que ataquen vulnerabilidades y amenacen la seguridad.

¿En qué me beneficia la seguridad de red?

La digitalización ha transformado al mundo. Ha cambiado nuestra manera de vivir, trabajar, aprender y entretenernos. Todas las organizaciones que quieren prestar los servicios que exigen los clientes y los empleados deben proteger su red. La seguridad de red también ayuda a proteger la información confidencial de los ataques. En última instancia, protege su reputación.

Duración: 25 horas.

Materiales de formación: para el desarrollo de esta actividad es importante atender de manera clara y concisa las indicaciones del instructor y las recomendaciones que se dan en el material de estudio **“Proteccion de puertos en redes Packet Tracer”**

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

Usando el aplicativo **Packet Tracer** el cual previamente ha sido contextualizado por el instructor(a), se implementaran diversas practicas en redes para la protección de puertos.

Lineamientos para la entrega de la evidencia:

A continuación, algunas recomendaciones para realizar la actividad:

- Solicite al instructor un equipo con el aplicativo **Packet Tracer**
- Realice las practicas propuestas por el instructor(a).
- Debe sustentar las implementaciones que ha realizado.
- Para hacer el envío del producto remítase al área de la actividad correspondiente y acceda al espacio para el envío de la evidencia **AA9_EV01_Proteccion de puertos en Packet Tracer**

Total horas actividad de aprendizaje: 144 horas; 120 directas (D), 24 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	<ul style="list-style-type: none">• 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	<ul style="list-style-type: none">• Clasifica las amenazas y vulnerabilidades de ciberseguridad de acuerdo con la	Lista de chequeo



	<p>normativa y los estándares técnicos.</p> <ul style="list-style-type: none">• Evalúa vulnerabilidades acorde con técnicas de análisis y criterios técnicos.	
<p>Evidencia de producto</p> <p>AA3_EV01_Formato matriz de riesgo</p>	<ul style="list-style-type: none">• 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.	<p>Lista de chequeo</p>



<p>Evidencia de conocimiento</p> <p>AA4_EV01_mapa mental</p>	<ul style="list-style-type: none">• 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.	<p>Lista de chequeo</p>
--	--	-------------------------



Evidencia de producto AA5_EV01_Aplicacion con seguridad anti-inyección de código.	<ul style="list-style-type: none">• 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.	Lista de chequeo
Evidencia de producto AA6_EV01_Analisis forense de spam para ciberataques.	Identifica el ámbito de aplicación de ciberseguridad de acuerdo con los activos de información de la organización, la normativa y los estándares técnicos	Lista de chequeo
Evidencia de producto AA7_EV01_Analisis forense con sistema operativo forense.	<ul style="list-style-type: none">• Valora el impacto y la probabilidad de los riesgos de acuerdo con metodologías de análisis y evaluación, criterios técnicos y marcos de referencia.	Lista de chequeo
Evidencia de producto AA8_EV01_Analisis forense con sistema operativo Autopsy.	<ul style="list-style-type: none">• Determina como eliminar el riesgo de acuerdo con metodologías de análisis y evaluación, criterios técnicos y marcos de referencia.	Lista de chequeo
Evidencia de producto AA9_EV01_Proteccion de puertos en Packet Tracer	<ul style="list-style-type: none">• Determina como eliminar el riesgo en redes de información de acuerdo con metodologías de análisis y evaluación, criterios técnicos y marcos de referencia.	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).

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/TesisDepositado

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.

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](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	Fecha
Autor (es)	Fabio Izquierdo	Instructor	Regional Valle, Centro de Electricidad y Automatización Industrial	Julio de 2024

8. Control de cambios

	Nombre	Cargo	Dependencia	Fecha	Razón del cambio
Autor (es)					