PROCESO DE GESTIÓN DE FORMACIÓN PROFESIONAL INTEGRAL
FORMATO GUÍA DE APRENDIZAJE

IDENTIFICACIÓN DE LA GUIA DE APRENDIZAJE

- **Denominación del Programa de Formación**: Técnico en Sistemas Tele informáticos.
- **Código del Programa de Formación**: 233101 V1.
- **Nombre del Proyecto**: Gestión de los servicios solicitados por los clientes para el soporte técnico de software, hardware y redes.
- **Fase del Proyecto**: Evaluación
- **Actividad de Proyecto**: Validar los procedimientos realizados en los sistemas teleinformáticos.
- **Competencia**: Operar herramientas informáticas y digitales de acuerdo con protocolos y manuales técnicos**.**
- **Resultados de Aprendizaje**: Documentar la gestión de la información de acuerdo a protocolos establecidos
- **Duración de la Guía**: 80 horas

2. PRESENTACIÓN

"En la era digital en la que vivimos, la digitalización de documentos se ha convertido en una práctica fundamental para empresas y organizaciones de todo tipo. La transformación de documentos físicos en formatos digitales ofrece innumerables beneficios, como el ahorro de espacio, la eficiencia en la búsqueda de información y la facilidad de acceso. Sin embargo, a medida que más información confidencial y valiosa se almacena en formato digital, la seguridad en la digitalización de documentos se convierte en una preocupación esencial.



Figura 1 https://acortar.link/AWK7US

La seguridad en la digitalización de documentos se refiere a la protección de la información digitalizada contra accesos no autorizados, pérdida de datos, daño o manipulación. Garantizar la seguridad de los documentos digitales es crucial para proteger la privacidad de los clientes, la propiedad intelectual y la información confidencial de la empresa".
(Tomado de: https://acortar.link/uV5B3z)

Estimado aprendiz en esta guía se describen las actividades de aprendizaje del programa denominado "Operar herramientas informáticas y digitales de acuerdo con protocolos y manuales técnicos", 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: *"norma dedicada a Sistemas de Gestión de la Seguridad de la Información. que recoge todos los requisitos necesarios con los que una organización debe contar para poder garantizar que su gestión de datos e información sea segura".*
(Tomado de: https://acortar.link/WtHq8C)

3. FORMULACIÓN DE LAS ACTIVIDADES DE APRENDIZAJE

3.1 Actividades de Reflexión inicial.

3.3.1 Identificar los riesgos y controles de la seguridad de la información a través del diseño de una matriz de riesgos.

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.

En equipos de trabajo los aprendices a partir de la observación del video **"Análisis y valoración de riesgos de la información"**, diseñaran una matriz de riesgos en la aplicación Excel, de acuerdo con las orientaciones proporcionadas durante la sesión de clase, que será socializada en una mesa redonda, dirigida por el Instructor quien aclarará las dudas que se presenten.

- **Ambiente requerido:** Ambiente de aprendizaje presencial.
- **Estrategias o técnicas didácticas activas**: Mesa redonda.
- **Materiales de formación:** Computador funcionales de escritorio o portátiles con memoria RAM 16 GB, procesador 3.0 GHz o Superior, Disco Duro de 1 TB, Software ofimático, Red internet operativa para consultas – Video Beam, marcadores borrables, Tablero.
- **Material de apoyo:** video **"Análisis y valoración de riesgos de la información"**
- **Duración de la actividad:** 5 horas**.**

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

3.2.1. Identificar saberes previos mediante la clasificación y evaluación de las amenazas y vulnerabilidades de la seguridad de la información en un escenario empresarial.

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.

Actividad 1: Los aprendices en equipos de trabajo darán respuesta a un **taller sobre sus conocimientos previos** acerca de las amenazas y vulnerabilidades en la seguridad de la información.

Actividad 2: Estudio de caso: Los aprendices deberán formar equipos de trabajo y resolver los diferentes casos de estudio asignados por el instructor que evidencien la diferentes vulnerabilidades y amenazas observables de acuerdo con cada contexto, que serán socializadas en plenaria.

- **Ambiente requerido:** Ambiente de aprendizaje presencial.
- **Estrategias o técnicas didácticas activas**: cuestionario y caso de estudio.
- **Materiales de formación:** Computador funcionales de escritorio o portátiles con memoria RAM 16 GB, procesador 3.0 GHz o Superior, Disco Duro de 1 TB, Software ofimático, Red internet operativa para consultas – Video Beam, marcadores borrables, Tablero.
- **Material de apoyo: Cuestionario y casos de estudio en documento Word.**
- **Duración de la actividad:** 5 horas**.**

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

3.3.1 Identificar y valorar en un escenario empresarial, los activos de información de acuerdo con métodos y criterios técnicos de evaluación.

Realizar la valuación de los activos de la organización de acuerdo con métodos y criterios técnicos de evaluación.

La valuación de activos es el proceso mediante el cual se determina el valor monetario de los recursos y propiedades que posee una organización. Este proceso es crucial para una variedad de propósitos financieros y estratégicos, incluyendo la elaboración de informes financieros, la toma de decisiones de inversión, la gestión de riesgos y la planificación estratégica.

En equipos de trabajo los aprendices a partir de la lectura del documento "Ciberseguridad y seguridad de la información", elaboraran un informe detallado en el que describan:

- ¿Cuáles son los activos tangibles o intangibles informáticos con que cuenta una empresa o entidad, que están relacionados o requeridos para el cumplimiento de sus objetivos o metas? y ¿Cómo debe ser la clasificación de esto en la empresa o entidad?
- ¿Qué metodologías o estándares puede utilizar para realizar el proceso de valuación de activos?

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

Estudio de campo: (documento o formato) se asignarán por dependencias un grupo de aprendices para realizar la actividad propuesta, la cual consiste en verificar los activos de información en cada una de las dependencias asignadas que serán consignadas en un informe.

- **Ambiente requerido:** Ambiente de aprendizaje presencial.
- **Estrategias o técnicas didácticas activas**: Estudio de campo.
- **Evidencia:** documento escrito con el informe del análisis y valuación de activos para el caso propuesto.
- **Instrumento de evaluación:** Evaluación de desempeño. (Lista de chequeo)
- **Materiales de formación:** Computador funcionales de escritorio o portátiles con memoria RAM 16 GB, procesador 3.0 GHz o Superior, Disco Duro de 1 TB, Software

ofimático, Red internet operativa para consultas – Video Beam, marcadores borrables, Tablero.

- **Material de apoyo: Documento con lectura sobre:** "Ciberseguridad y seguridad de la información"
- **Duración de la actividad:** 15 horas**.**

3.3.2 Crear la matriz de riesgos de ciberseguridad de la organización, de acuerdo con los activos de información, la normativa y los estándares técnicos.

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.**

Para el desarrollo de esta actividad los aprendices deberán tener en cuenta la importante de la lectura y análisis del material de apoyo "Formato matriz de riesgo" y retomar el estudio de campo propuesto en la actividad: **"Ciberseguridad y seguridad de la información".**

De acuerdo con lo anterior el aprendiz tendrá 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**.

Para crear la matriz de riesgos, se debe utilizar como insumo para el proceso el estudio de campo y la aplicación Excel para automatizar el documento.

- **Ambiente requerido:** Ambiente de aprendizaje presencial.
- **Estrategias o técnicas didácticas activas**: Cuadro comparativo.
- **Evidencia:** Documento con matriz de riesgos automatizada en Excel.
- **Instrumento de evaluación:** Evaluación de desempeño. (Lista de chequeo)
- **Materiales de formación:** Computador funcionales de escritorio o portátiles con memoria RAM 16 GB, procesador 3.0 GHz o Superior, Disco Duro de 1 TB, Software ofimático, Red internet operativa para consultas – Video Beam, marcadores borrables, Tablero.
- **Material de apoyo:** Documento**:** "Formato matriz de riesgo" - Tutor en matriz de riesgo en Excel.
- **Duración de la actividad:** 15 horas**.**

3.3.3. Implementar el mapa de amenazas de acuerdo con métodos de análisis, criterios técnicos y marcos de referencia.

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.

Es el estándar internacional para la seguridad de la información que establece la especificación para un sistema de gestión de seguridad de la información (SGSI). El enfoque de mejores prácticas del estándar del sistema de gestión de seguridad de la información ayuda a las organizaciones a gestionar su seguridad de la información dirigiéndose a las personas y los procesos, así como a la tecnología.

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. Para el desarrollo de esta actividad en grupos deben diseñar 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. Se les facilitará el documento "**El sistema de gestión de seguridad de la información**" en el material de apoyo. Esta actividad será socializada durante la sesión de clase, donde el instructor aclarará inquietudes.

Para la entrega de la evidencia el aprendiz deberá tener en cuenta:

- ✓ El mapa mental dará respuesta a las indicaciones señaladas para su elaboración.
- ✓ El mapa mental debe integrar el uso de convenciones, ramificaciones, colores, imágenes e íconos que permitan su organización y comprensión.
- ✓ Podrá 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.
- ✓ Debe generar un documento y entregar en formato PDF.

- **Ambiente requerido:** Ambiente de aprendizaje presencial.
- **Estrategias o técnicas didácticas activas**: Mapa mental.
- **Evidencia:** Documento con diagrama tipo mapa mental formato pdf.
- **Instrumento de evaluación:** Evaluación de producto. (Lista de chequeo)
- **Materiales de formación:** Computador funcionales de escritorio o portátiles con memoria RAM 16 GB, procesador 3.0 GHz o Superior, Disco Duro de 1 TB, Software ofimático, Red internet operativa para consultas – Video Beam, marcadores borrables, Tablero.
- **Material de apoyo:** Documento**:** "**El sistema de gestión de seguridad de la información**"
- **Duración de la actividad:** 15 horas**.**

3.4 Actividades de transferencia del conocimiento.

3.4.1 Identificar los procesos críticos de ciberseguridad en un escenario empresarial de acuerdo con criterios técnicos y los objetivos de la organización.

Cuando se habla de ciberseguridad, el análisis de riesgos informáticos es la evaluación de los **distintos peligros que afectan a nivel informático** y que pueden producir situaciones de amenaza a las empresas, como robos o intrusiones que comprometan los datos o ataques externos que impidan el funcionamiento de los sistemas propiciando periodos de inactividad críticos. La sociedad actual vive en un camino constante hacia la digitalización, con el uso masivo de los smartphones, la comunicación diaria a través de internet, el uso de la inteligencia artificial, el Big Data, e incluso el IoT, donde los electrodomésticos también se vuelven inteligentes y se conectan a la red. Todas estas ventajas que aporta esta transformación digital vienen acompañadas de una serie de amenazas que ponen en riesgo la seguridad de los sistemas y comprometen la privacidad de la información.

En este sentido, las empresas deben analizar los riesgos informáticos y tomar medidas para evitar que se produzcan, o para mitigar sus efectos negativos. (Tomado de: https://acortar.link/BxKLWg)

En equipos de trabajo asignados por el instructor, los aprendices diseñaran un manual de procedimientos para Identificar los procesos críticos de ciberseguridad, a partir del análisis e investigación, cuyo punto de partida será un estudio de caso en un escenario empresarial.

El manual de procedimiento deberá documentarlo con suficiencia y diseñar el diagrama de flujo de los procesos referenciados.

- ✓ **Documentación y Cumplimiento Normativo:** Asegurar que la documentación cumpla con las normativas legales y de seguridad.
- ✓ **Gestión de Incidentes y Documentación:** Documentar correctamente los incidentes de seguridad y sus respuestas
- ✓ **Evaluación de la Documentación:** Evaluar la efectividad de la documentación y su impacto en la gestión de la información

Cada equipo de trabajo deberá socializar el diagrama de flujo según el estudio de caso asignado. En plenaria el instructor ampliará la información.

- **Ambiente requerido:** Ambiente de aprendizaje presencial.
- **Estrategias o técnicas didácticas activas**: Estudio de caso.
- **Evidencia:** Documento Manual de procedimiento. formato Pdf.
- **Instrumento de evaluación:** Evaluación de producto. (Lista de chequeo)
- **Materiales de formación:** Computador funcionales de escritorio o portátiles con memoria RAM 16 GB, procesador 3.0 GHz o Superior, Disco Duro de 1 TB, Software ofimático, Red internet operativa para consultas – Video Beam, marcadores borrables, Tablero.
- **Material de apoyo:**
  - ✓ **https://www.ambit-bst.com/blog/ciberseguridad-10-tipos-de-amenazas**
  - ✓ **https://cncs.gob.do/wp-content/uploads/2020/07/Guia-de-Controles-Criticos-de-Ciberseguridad-Controles-CIS-V7.pdf**

- ✓ **https://www.asobancaria.com/wp-content/uploads/2022/06/Guia_de_Buenas_Practicas_para_Auditar_la_Ciberseguridad_2022_V1.pdf**

- **Duración de la actividad:** 25 horas**.**

4. ACTIVIDADES DE EVALUACIÓN

Fase del proyecto formativo	Actividad del proyecto formativo	Actividad de Aprendizaje	Evidencias de Aprendizaje	Criterios de Evaluación	Técnicas e Instrumentos de Evaluación
Evaluación	Validar los procedimientos realizados en los sistemas teleinformáticos.	3.1.1 Actividad de Reflexión. 3.2.1 Actividad de contextualización. 3.3.1. Identificar y valorar en un escenario empresarial, los activos de información de acuerdo con métodos y criterios técnicos de evaluación. 3.3.2 Crear la matriz de riesgos de ciberseguridad de la organización, de acuerdo con los activos de información, la normativa y los estándares técnicos. 3.3.3. Implementar el mapa de amenazas de acuerdo con métodos de análisis, criterios técnicos y marcos de referencia. 3.4.1 Documentar los procedimientos de mantenimiento preventivo y correctivo de computadores, según las especificaciones técnicas y recomendaciones del fabricante, utilizando	No aplica para evidencia de aprendizaje. No aplica para evidencia de aprendizaje. **Desempeño:** documento escrito con el informe del análisis y valuación de activos para el caso propuesto. **Desempeño y producto:** Documento con matriz de riesgos automatizada en Excel. **Producto**: Documento con diagrama tipo mapa mental formato Pdf. **Producto**: Manual de procedimientos	No aplica criterio de evaluación. No aplica criterio de evaluación. Mantiene la documentación según manual técnico.	**Técnica:** Observación **Instrumento de evaluación de desempeño:** Lista de chequeo . **Técnica:** Observación **Instrumento de evaluación de desempeño:** Lista de chequeo **Técnica:** Observación **Instrumento de evaluación de producto:** Lista de chequeo **Técnica:** Observación **Instrumento de evaluación de producto:** Lista de chequeo

5. GLOSARIO DE TÉRMINOS

- **Activo: E**l 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.
- **Activo Informático:** todo elemento tecnológico o relacionado con la tecnología necesario para que la organización cumpla con su misión y logre sus objetivos empresariales.
- **Activo Tecnológico:** todo equipo tecnológico o relacionado con la tecnología requerido para que la organización cumpla con su función o misión.

- **Amenaza: C**ualquier evento que puede afectar los activos de información y se relaciona, principalmente, con recursos humanos, eventos naturales o fallas técnicas.
- **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.
- **Valuar:** determinar o atribuir un valor a una cosa o persona.
- **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 BILBIOGRÁFICOS

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.

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

OEA, AWS. (2019). Ciberseguridad marco NIST. Un abordaje integral de la ciberseguridad. Organización de Estados Americanos, AWS.

7. CONTROL DEL DOCUMENTO

	Nombre	Cargo	Dependencia	Fecha
Autor (es)	Adriana Salazar, Jaime Saucedo	Instructores	CEAI	02/09/2024

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

	Nombre	Cargo	Dependencia	Fecha	Razón del Cambio