PROCESO DE GESTIÓN DE FORMACIÓN PROFESIONAL INTEGRAL

FORMATO GUÍA DE APRENDIZAJE

GUÍA 9 - SEGURIDAD DE LA INFORMACIÓN

1. IDENTIFICACIÓN DE LA GUIA DE APRENDIZAJE N° 9

- **Denominación del Programa de Formación**: Técnico en Sistemas Teleinformáticos
- **Código del Programa de Formación**: 233108 V1
- **Nombre del Proyecto Formativo**: Implementación de estrategias para las operaciones teleinformáticas de las organizaciones desde la infraestructura de la red de datos. (2903490)
- **Fase del Proyecto: Evaluación**
- **Actividad de Proyecto Formativo** : Documentar los resultados de las acciones de mantenimiento preventivo y correctivo sobre los sistemas teleinformáticos de la organización.
- **Competencia**: Operar herramientas informáticas.
- **Resultados de Aprendizaje**: Planificar la información según criterios de ciberseguridad
- **Duración de la Guía de Aprendizaje** (horas): 60 horas (48 horas presenciales – 12 horas desescolarizadas)

2. PRESENTACIÓN



Fuente: https://acortar.link/sT24SA

El auge de las Tecnologías de la Información y las Comunicaciones (TIC) ha permitido a distintas actividades humanas la generación y manipulación de grandes volúmenes de datos, desde múltiples plataformas y desde cualquier lugar, lo que juega un papel fundamental en el desarrollo de las actividades cotidianas de empresas y en general del ámbito productivo. Este crecimiento en la información que gestionan las organizaciones actuales ha planteado grandes retos en materia de administración, en los cuales tiene un papel importante lo relacionado con la seguridad de la misma.

En los últimos años se ha notado un creciente número de incidentes de seguridad que afectan a las redes de datos, infraestructura tecnológica y aplicaciones informáticas, convirtiéndose en un problema crítico dentro de los procesos de negocio. Por tanto, la anticipación a este fenómeno es esencial y debe ser comprendido para poder administrar y gestionar los activos de información e infraestructura. De acuerdo al informe IT Trends 2019 (IT Research) que muestra las tendencias para la seguridad y los riesgos de información, cada vez crecen las dificultades para este ámbito, lo que motiva entonces a tener una comprensión profunda de las herramientas que permitan la protección de las organizaciones, y en esta línea, a tener un talento humano cualificado para la utilización de las mismas.

3. FORMULACIÓN DE LAS ACTIVIDADES DE APRENDIZAJE

- La guía 9 “Seguridad de la información” contiene concepto de seguridad de la información,actividades de acceso a la información, Monitorear el almacenamiento de los activos de la información,mejora del tratamiento de la información,copia de seguridad y restablecimiento, Habeas data y derechos de autor,copias de seguridad, Introducción a ISO 27001.

3.1 Actividades de reflexión inicial: Identificar y comprender la importancia que tiene la seguridad de la información en nuestra vida diaria.

Descripción de la actividad 1:

A continuación ver el siguiente video

https://www.youtube.com/watch?v=OC8x73OfV6s

Mire el video y conteste las siguientes preguntas:

1.Qué entiende por seguridad de la información

2.Por qué es importante la seguridad de la información en Colombia

3.Cuáles son las principales amenazas a la seguridad de la información en Colombia

4.Qué medidas conoce para proteger la información

5.En qué nivel considera que una empresa o entidad cumple con las normas de seguridad de la información.

Discutan las siguientes preguntas

6.Cuáles fueron las respuestas más comunes

7.Qué diferencias o similitudes encontraron en sus respuestas

8.Qué aprendieron de la actividad

9.Qué expectativas tienen sobre la guía

Ambiente requerido: fuera de centro

Estrategias o técnicas didácticas activas: Video, discusión acerca del video,enfocado en la vida cotidiana

Materiales de formación

- 1.Video de reflexión acerca de la seguridad de la información

Material de apoyo: No aplica

Duración de la actividad: (5) horas.

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

Descripción de la actividad: 2

Clasificar privilegios de acceso y seguridad a la información implica organizar los permisos de acceso a los recursos según los roles y necesidades específicas de los usuarios en una organización. Este proceso se asegura de que solo las personas autorizadas tengan acceso a la información adecuada, protegiendo así los datos sensibles y minimizando riesgos**.**

Actividad: 2.Simulación de clasificación de acceso

Haciendo uso de la lectura denominada Clasificar privilegios de acceso y seguridad a la información los cuales se encuentran en material de formacion y analizando la lectura realice

Lista ficticia de empleados, perfiles de usuario (administrador, usuario estándar, invitado), datos sensibles y públicos,

En grupos de 2 estudiantes realizaran el análisis a la lista ficticia de empleados para implementar controles de acceso, utilizar un software de gestión puede ser Active Directory o equivalente.

Ambiente requerido: Aula de sistemas Fuera de Centro
Estrategias o técnicas didácticas activas: Aprendizaje Basado lectura critica, videos
Materiales de formación:

- Clasificar privilegios de acceso y seguridad a la información

Material de apoyo:

- Videos(**Clasificar privilegios de acceso y seguridad a la información)**

Duración de la actividad: (5) horas.

3.3 Actividades de apropiación: Monitorear el almacenamiento de los activos de la información

Descripción de la actividad: 3 Auditoría de almacenamiento

Los datos creados o utilizados **por** un proceso de la organización en medio digital, en papel o en otros medios. El hardware y el software utilizado para el procesamiento, transporte o almacenamiento de **información**.

Actividad: Auditoría de almacenamiento

Una empresa requiere realizar el almacenamiento de los activos de la información para lo cual la entidad delega al jefe de seguridad de la información,el cual debe realizar una autoría de todos los activos de la entidad, para realizar la actividad mencionada se recomienda utilizar TreeSize o WinDirStat para analizar el uso del espacio de almacenamiento y categorizar los activos.

Para realizar la actividad solicitada y con la orientación del instructor los aprendices deben Remitirse al material de formación y consultar el documento denominado Guía para la Gestión y Clasificaciónde Activos de Información de igual manera podrá apoyarse en los siguientes videos denominados **2.Video activos de información.**

Ambiente requerido: Aula de sistemas Fuera de Centro
Estrategias o técnicas didácticas activas: Aprendizaje basado en problemas, trabajo colaborativo, aprendizaje por descubrimiento, uso de recursos multimedia, evaluación formativa.
Materiales de formación

- Guía para la Gestión y Clasificaciónde Activos de Información

Material de apoyo:

- **Video activos de información.**

Evidencias de aprendizaje:

1.El aprendiz estará en la capacidad de realizar auditoria de almacenamiento a activos de información de la entidad**.**

Instrumentos de evaluación:Lista de chequeo

Duración de la actividad: (5) horas.

Descripción de la actividad 4: Identificar procesos de mejora para el tratamiento de la información

Actividad: Propuesta de mejora para un flujo de trabajó

En el colegio nuestra señora milagrosa desean mejorar los procesos de cartera,para ello deben mejorar y llevar un orden en la base de datos de los padres de familia para dar respuesta inmediata al proceso de pago de pensión.

Con base en el material de formación el aprendiz debe realizar una mejora en la base de datos de los padres de familia Simplificar un proceso de verificación de pago de pensión.

Para la solución de la actividad, se puede apoyar en el documento modelo de gestión de tratamiento de la información y en el video de diagrama de flujos, para realizar la propuesta de mejora en el tratamientode la información.

Ambiente requerido: Aula de sistemas Fuera de Centro
Estrategias o técnicas didácticas activas: Aprendizaje basado en problemas, trabajo colaborativo, aprendizaje por descubrimiento, uso de recursos multimedia, simulación práctica, evaluación formativa
Materiales de formación:

- 4.Modelo de gestión de tratamiento de la información

Material de apoyo

- Diagrama de flujo (https://www.youtube.com/watch?v=hTz4YzvtjrM)

Evidencias de aprendizaje:

2.Propuesta de mejora del flujo de trabajó

Instrumentos de evaluación:Lista de chequeo

Duración de la actividad: (5) horas.

Descripción de la actividad 4: Gestionar copias de seguridad y restablecimiento

Actividad: Taller de respaldo y recuperación

- La empresa ficticia **"DataSafe S.A."** tiene archivos de clientes y reportes financieros. Durante el taller, configurarás un plan de respaldo diario de estos datos y probarás restaurarlos tras una eliminación accidental.

El aprendiz deberá Configurar un respaldo incremental diario y uno completo semanal en el software elegido. Simula la pérdida de datos el día viernes y realiza una recuperación total.

- Para resolver la actividad tomara como apoyo el videos dispuestos en el material de formación denominados **5.** "Cómo realizar copias de seguridad y restaurar datos con Veeam Backup".

Ambiente requerido: Aula de sistemas Fuera de Centro
Estrategias o técnicas didácticas activas: Aprendizaje basado en proyectos, simulación práctica, uso de recursos multimedia, trabajo colaborativo, aprendizaje autónomo, resolución de problemas
Materiales de formación:

- 5.Cómo realizar copias de seguridad y restaurar datos con Veeam Backup
- 6.Veeam Software. (2024). *Best Practices for Backup and Recovery*. Recuperado de https://www.veeam.com

Material de apoyo:

- Acronis. (2024). *Guía práctica para soluciones de respaldo empresarial*. 1.Recuperado de https://www.acronis.com
- Microsoft. (2024). *Planificación y configuración de copias de seguridad en sistemas Windows*. Recuperado de https://support.microsoft.com

Evidencias de aprendizaje:
3.Realizacion de copia de seguridad de datos
Instrumentos de evaluación: Lista de chequeo
Duración de la actividad: 10 horas.

Descripción de la actividad 5: Habeas data y derechos de autor

- Caso: Una universidad comparte datos de contacto de sus estudiantes con empresas de mercadeo sin su consentimiento. También utiliza música protegida por derechos de autor en sus eventos sin licencias adecuadas.

- Para realizar está actividad el aprendiz debe Identifica las infracciones en el caso anterior y elabora un plan de acción para evitar futuras violaciones.

- Con base en este video el aprediz podrá realizar lo solicitado

- 1.Introducción al Habeas Data y su aplicación en Colombia":

- 2.https://www.youtube.com/watch?v=uQy1zl4E2tw

Ambiente requerido: Aula de sistemas Fuera de Centro
Estrategias o técnicas didácticas activas: Video herramientas tecnológicas.

- **Materiales de formación:**

- **7**Introducción al Habeas Data y su aplicación en Colombia":

- 8.https://www.youtube.com/watch?v=uQy1zl4E2tw

- 9.Congreso de la República de Colombia. (2012). *Ley 1581 de 2012: Protección de datos personales*. Recuperado de https://www.sic.gov.co
- 10.Superintendencia de Industria y Comercio. (2024). *Guía para la protección de datos personales en Colombia*. Recuperado de https://www.sic.gov.co/proteccion-de-datos-personales
- **Material de apoyo:**
  Organización Mundial de la Propiedad Intelectual. (2024). *Derechos de Autor y Propiedad Intelectual: Conceptos clave*. Recuperado de https://www.wipo.int

Evidencias de aprendizaje:
4.Identificación de habias data

Instrumentos de evaluación: Lista de chequeo

Duración de la actividad: (10) hora

Descripción de la actividad 6: Copias de seguridad

Actividad: Comparativa de métodos de respaldo

- Empresa ficticia: **"Tech Solutions"** gestiona bases de datos de clientes y documentos internos. ¿Qué esquema de respaldo recomendarías considerando un presupuesto limitado y la necesidad de recuperación rápida?

- Diseña un esquema que combine respaldos completos mensuales e incrementales diarios. Justifica tu decisión con base en costos y tiempo de recuperación.

- Remitase al documento denominado "Tipos de respaldo explicados": https://www.youtube.com/watch?v=D1Lwod_1bqg,realice lo que se indique allí, para posteriormente hacer entrega en su portafolio.

Ambiente requerido: Aula de sistemas Fuera de Centro
Estrategias o técnicas didácticas activas: Aprendizaje basado caso, práctica guiada, resolución de problemas reales, uso de herramientas prácticas

- **Materiales de formación:**
- Beal, V. (2024). *Diferencias entre copias de seguridad completas, incrementales y diferenciales*. *TechTarget*. Recuperado de https://www.techtarget.com

- **Material de apoyo:**
- IBM. (2024). *Estrategias de respaldo para empresas modernas*. Recuperado de https://www.ibm.com

Evidencias de aprendizaje:
- 5.Diseña un esquema que combine respaldos completos mensuales e incrementales

Instrumentos de evaluación: Lista de chequeo
Duración de la actividad: 10 horas.

Descripción de la actividad 7: Introducción a ISO 27001

Actividad: Simulación de auditoría inicial

Explicar como realizar una auditoria inicial
Caso ficticio: **"SecureCorp"** carece de políticas claras de gestión de contraseñas y no realiza copias de seguridad regulares. Además, su personal no ha recibido capacitación en seguridad informática.

- Elabora un informe identificando 3 deficiencias principales y proponiendo 3 medidas correctivas priorizadas.

- Para realizar este informe remitase al material de apoyo

- "Introducción práctica a la ISO 27001": https://www.youtube.com/watch?v=zV2sfyvfqik

Ambiente requerido: Aula de sistemas Fuera de Centro
Estrategias o técnicas didácticas activas: Aprendizaje basado en proyectos, uso de simuladores y herramientas de análisis de red, resolución de problemas reales.

- **1.Materiales de formación:** "Introducción práctica a la ISO 27001": https://www.youtube.com/watch?v=zV2sfyvfqik

- **2.Material de apoyo:**

- https://www.youtube.com/watch?v=FSYYOlm2zOA

Evidencias de aprendizaje:
6.Informe de la norma ISO 2701
Instrumentos de evaluación: No Aplica
Duración de la actividad: (20)hora.

Descripción de la actividad 8 Prueba de conocimiento

Realizar el cuestionario correspondiente a la guía 7 que se encuentra en la plataforma Zajuna.

Ambiente requerido: Aula de sistemas Fuera de Centro
Estrategias o técnicas didácticas activas: Prueba de conocimiento
Materiales de formación: No aplica
Material de apoyo: No aplica
Evidencias de aprendizaje:
- 7. Prueba de conocimiento Guía 9

Instrumentos de evaluación: No Aplica
Duración de la actividad: 1 hora.

3.4 Actividades de Transferencia el Conocimiento:

Carta de satisfacción, debe diligenciarla con su cliente, recuerde presentar firma manuscrita, la carta se encuentra en el material de formación.

Indicadores y resultados diligenciar las encuestas, entrevistas y presentar el informe en google forms.

Video recopilatorio, en este video debe presentar el historial fotográfico y documental de todo su proyecto (cuatro fases del proyecto), con una duración de 3 a 5 minutos.

Cargue su actividad en su portafolio con el nombre **Video resumen proyecto, Resultados encuestas y Carta de satisfacción del cliente**.

Ambiente requerido: Aula de sistemas Fuera de Centro
Estrategias o técnicas didácticas activas: Estrategias o técnicas didácticas activas:

Materiales de formación
- Carta de satisfacción
- 13.Video Como crear encuestas y formularios

Material de apoyo: No aplica
Evidencias de aprendizaje:
- 11. Video resumen proyecto
- 12. Resultados encuestas
- 13. Carta de satisfacción del cliente

Instrumentos de evaluación:
Duración de la actividad: 22 horas.
-

4. PLANTEAMIENTO DE EVIDENCIAS DE APRENDIZAJE PARA LA EVALUACIÓN EN EL PROCESO FORMATIVO.

Fase del proyecto formativo	Actividad del proyecto formativo	Actividad de Aprendizaje	Evidencias de Aprendizaje	Criterios de Evaluación	Técnicas e Instrumentos de Evaluación
Evaluación	Documentar los resultados de las acciones de mantenimiento preventivo y correctivo sobre los sistemas teleinformáticos de la organización	Simulación de clasificación de acceso	El aprendiz estará en la capacidad de realizar auditoria de almacenamiento a activos de información de la entidad. Propuesta de mejora del flujo de trabajó El aprendiz estará en la capacidad de realizar auditoria de almacenamiento a activos de información de la entidad. Realizacion de copia de seguridad de datos. Diseña un esquema que combine respaldos completos mensuales e incrementales	Aplica controles de seguridad según normativa, necesidades y restricciones de acceso a la información. Propone procesos de mejora en el manejo de la información con base a la normativa vigente. gestiona las copias de seguridad y recuperación, según lineamientos establecidos por la empresa	Lista de chequeo • Desempeño • Producto Prueba de conociento

			Realizacion de copias de seguridad Informde la norma ISO 2701.		

5. GLOSARIO DE TÉRMINOS

Acceso: Permiso de un usuario para entrar a un sistema, red o aplicación.

Activo de información: Cualquier información o elemento relacionado con su tratamiento (sistemas, soportes, edificios, personas...) que tenga valor para la organización.

Amenaza: Posibilidad de que ocurra un evento que pueda afectar negativamente a la seguridad de la información.

Autenticación: Proceso de verificar la identidad de un usuario.

Autorización: Permiso de un usuario para realizar una acción específica en un sistema, red o aplicación.

Copia de seguridad: Duplicado de la información que se realiza para protegerla en caso de pérdida o daño.

Cifrado: Conversión de la información en un código que solo puede ser leído por personas autorizadas.

Confidencialidad: Propiedad de la información que solo puede ser conocida por personas autorizadas.

Contraseña: Clave secreta que se utiliza para autenticar a un usuario.

Control de acceso: Conjunto de medidas que se utilizan para controlar quién tiene acceso a la información.

Cultura de seguridad: Conjunto de valores, creencias y comportamientos que se comparten en una organización con respecto a la seguridad de la información.

Dato: Unidad de información que tiene un significado.

Encriptación: Cifrado de la información.

Gestión de riesgos: Proceso de identificar, analizar y evaluar los riesgos de seguridad de la información y tomar medidas para mitigarlos.

Información: Cualquier dato o conjunto de datos que tenga un significado.

Integridad: Propiedad de la información que es completa, precisa y confiable.

Malware: Software malicioso que puede dañar un sistema o red.

Phishing: Suplantación de identidad de una persona o empresa para obtener información confidencial de los usuarios.

Política de seguridad de la información: Conjunto de normas y procedimientos que se establecen para proteger la información.

Privacidad: Derecho de las personas a controlar su información personal.

Respaldo: Copia de seguridad de la información.

Riesgo: Probabilidad de que ocurra un evento que pueda afectar negativamente a la seguridad de la información.

Seguridad de la información: Conjunto de medidas que se utilizan para proteger la información de amenazas, riesgos y vulnerabilidades.

Vulnerabilidad: Debilidad en un sistema o red que puede ser explotada por un atacante.

6. REFERENTES BILBIOGRÁFICOS

Construya o cite documentos de apoyo para el desarrollo de la guía, según lo establecido en la guía de desarrollo curricular. (**BIBLIOGRAFÍA / WEBGRAFÍA).**

Gestión de copias de seguridad y recuperación:

- Veeam Software. (2024). *Best Practices for Backup and Recovery*. Recuperado de https://www.veeam.com
- Acronis. (2024). *Guía práctica para soluciones de respaldo empresarial*. Recuperado de https://www.acronis.com
- Microsoft. (2024). *Planificación y configuración de copias de seguridad en sistemas Windows*. Recuperado de https://support.microsoft.com

Habeas Data y Derechos de Autor:

- Congreso de la República de Colombia. (2012). *Ley 1581 de 2012: Protección de datos personales*. Recuperado de https://www.sic.gov.co
- Superintendencia de Industria y Comercio. (2024). *Guía para la protección de datos personales en Colombia*. Recuperado de https://www.sic.gov.co/proteccion-de-datos-personales

- Organización Mundial de la Propiedad Intelectual. (2024). *Derechos de Autor y Propiedad Intelectual: Conceptos clave*. Recuperado de https://www.wipo.int

Comparativa de métodos de respaldo:

- Beal, V. (2024). *Diferencias entre copias de seguridad completas, incrementales y diferenciales*. *TechTarget*. Recuperado de https://www.techtarget.com
- IBM. (2024). *Estrategias de respaldo para empresas modernas*. Recuperado de https://www.ibm.com

ISO 27001 y seguridad de la información:

- ISO. (2024). *Introducción a la norma ISO/IEC 27001:2022*. Recuperado de https://www.iso.org
- Peltier, T. R. (2016). *Information Security Risk Analysis* (3rd ed.). Auerbach Publications.
- International Organization for Standardization. (2024). *Gestión de Seguridad de la Información*. Recuperado de https://www.iso.org

7. CONTROL DEL DOCUMENTO

	Nombre	Cargo	Dependencia	Fecha
Autor (es)	**Nury Stella Godoy Montaño**	**Instructora**	**Articulación**	**13 /12/ 2024**

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

	Nombre	Cargo	Dependencia	Fecha	Razón del Cambio
Autor (es)					