PROCESO DE GESTIÓN DE FORMACIÓN PROFESIONAL INTEGRAL

1. IDENTIFICACIÓN DE LA GUÍA DE APRENDIZAJE

- Denominación del Programa de Formación: SISTEMAS TELEINFORMÁTICOS
- Código del Programa de Formación: 233108

Competencia: OPERACIÓN DE HERRAMIENTAS INFORMTICAS

- Resultados de aprendizaje a alcanzar:
  - o PLANIFICAR LA INFORMACIÓN SEGÚN CRITERIOS DE CIBERSEGURIDAD
- Duración de la Guía: Setenta (80) horas

2. PRESENTACIÓN

Estimados aprendices, esta guía sobre Políticas de Seguridad de la Información en Colombia te ofrece una completa formación para comprender, implementar y gestionar las mejores prácticas en este ámbito.
A lo largo de 80 horas, profundizarás en:

* Marco legal colombiano: Ley de Habeas Data, Ley de Protección de Datos Personales y otras normas relevantes.
* Gestión de riesgos: identificación, análisis y tratamiento de riesgos para la información.
* Controles de seguridad: físicos, técnicos y administrativos para proteger la información.
* Políticas de seguridad de la información: elaboración, implementación y seguimiento de políticas.
* Buenas prácticas: para la gestión de accesos, contraseñas, correo electrónico, dispositivos móviles, etc.
* Incidentes de seguridad: prevención, detección, respuesta y recuperación.

3. FORMULACIÓN DE LAS ACTIVIDADES DE APRENDIZAJE

3.1 Actividades de reflexión inicial

3.1.1 Objetivo:

* Concientizar sobre la importancia de la seguridad de la información en el contexto Colombiano.

* Evaluar los conocimientos previos sobre el tema.

* Motivar la participación en la guía.

Instrucciones:

3.1.1.1. Mire el video:

https://www.youtube.com/watch?v=7UPe_fxOz8M

3.1.1.2. Responda individualmente las siguientes preguntas:

* ¿Qué entiende por seguridad de la información?

* ¿Por qué es importante la seguridad de la información en Colombia?

* ¿Cuáles son las principales amenazas a la seguridad de la información en Colombia?

* ¿Qué medidas conoce para proteger la información?

* ¿En qué nivel considera que una empresa o entidad cumple con las normas de seguridad de la información?

3.1.1.3. Comparta sus respuestas con un compañero y grupo de clase.

3.1.1.4. Discutan las siguientes preguntas:

* ¿Cuáles fueron las respuestas más comunes?

* ¿Qué diferencias o similitudes encontraron en sus respuestas?

* ¿Qué aprendieron de la actividad?

* ¿Qué expectativas tienen sobre la guía?

Recursos:

* Ley de Habeas Data: https://acortar.link/ntlazT

* Ley de Protección de Datos Personales: https://www.youtube.com/watch?v=Z1MAFgf6KoQ

* Marco normativo de seguridad de la información en Colombia: https://acortar.link/EKXJ40

3.2 Actividades de contextualización

3.2.1 Objetivo:

* Brindar a los participantes una comprensión del contexto actual de la seguridad de la información en Colombia.

* Sensibilizar sobre los riesgos y amenazas que enfrentan las empresas y entidades.

* Motivar la participación en la guía.

3.2.2 Actividades

3.2.2.1. Análisis de noticias:

* Seleccionar una noticia reciente sobre un caso de seguridad de la información en Colombia.

* Leer la noticia en detalle y responder las siguientes preguntas:

  * ¿Qué tipo de incidente de seguridad se produjo?

  * ¿Cuál fue la empresa o entidad afectada?

  * ¿Cuáles fueron las consecuencias del incidente?

  * ¿Qué medidas se podrían haber tomado para prevenir el incidente?

3.2.2.2 ¿Que es un incidente de seguridad de la información?:

Definición:

Un incidente de seguridad de la información es un evento que viola la confidencialidad, integridad o disponibilidad de la información.

Tipos:

Tipos:

Categoría	Subcategorías	Ejemplos
Acceso no autorizado	Intercepción, acceso o uso indebido de la información	Robo de datos, acceso a sistemas sin autorización, espionaje
Malware	Infección por software malicioso	Virus, troyanos, ransomware, spyware
Denegación de servicio (DoS)	Interrumpción o degradación del servicio de un sistema	Ataques de inundación SYN, ataques ping de la muerte
Errores humanos	Acciones involuntarias que afectan la seguridad	Borrado accidental de datos, configuración incorrecta de sistemas
Desastres naturales	Eventos que afectan la infraestructura física	Inundaciones, terremotos, incendios
Fallos técnicos	Fallas en el hardware o software	Daños en el disco duro, errores en el sistema operativo

Consecuencias:

* Pérdida de datos
* Daño a la reputación
* Interrupción del negocio
* Pérdidas económicas
* Sanciones legales

Prevención:

* Implementar políticas y procedimientos de seguridad

* Capacitar a los usuarios

* Utilizar tecnología de seguridad

* Realizar copias de seguridad

* Implementar un plan de respuesta a incidentes

- Comparta las respuestas con el grupo y discuta las lecciones aprendidas del caso.

3.2.2.3 Mapa de riesgos Informáticos:

* En grupos de trabajo, identificar los principales riesgos y amenazas a la seguridad de la información en Colombia.

* Clasificar los riesgos por tipo (físicos, técnicos, administrativos) y por nivel de impacto (bajo, medio, alto).

* Graficar los riesgos en un mapa de riesgos, utilizando diferentes colores para cada categoría.

* Presentar el mapa de riesgos al resto del grupo y discutir las estrategias para mitigar los riesgos identificados.

3.2.2.3.1 Riesgos Informáticos: Tabla Resumen

Objetivo:

Un mapa de riesgos informáticos es una herramienta que permite identificar, evaluar y mitigar los riesgos que pueden afectar la seguridad de la información de una organización.

Tabla:

Amenaza	Vulnerabilidad	Impacto	Probabilidad	Riesgo	Control	Riesgo residual
Acceso no autorizado	Contraseñas débiles	Pérdida de datos confidenciales	Alta	Alto	Implementar políticas de contraseñas seguras	Medio
Malware	Software desactualizado	Interrupción del servicio	Alta	Medio	Implementar un programa de actualización de software	Bajo
Denegación de servicio	Ancho de banda limitado	Pérdida de disponibilidad	Media	Medio	Implementar soluciones de protección DDoS	Bajo
Errores humanos	Falta de capacitación	Borrado accidental de datos	Media	Bajo	Implementar programas de capacitación en seguridad	Bajo
Desastres naturales	Inundaciones	Daño a la infraestructura	Baja	Bajo	Implementar un plan de recuperación ante desastres	Bajo
Fallos técnicos	Fallas en el hardware	Pérdida de datos	Media	Bajo	Implementar un plan de mantenimiento preventivo	Bajo

Explicación de las columnas:

- **Amenaza:** Evento o acción que puede poner en riesgo la seguridad de la información.
- **Vulnerabilidad:** Debilidad en el sistema o proceso que permite que se concrete la amenaza.
- **Impacto:** Consecuencia negativa que puede tener el incidente de seguridad.
- **Probabilidad:** Posibilidad de que ocurra el incidente de seguridad.
- **Riesgo:** Producto del impacto y la probabilidad.
- **Control:** Medida que se puede tomar para mitigar el riesgo.
- **Riesgo residual:** Riesgo que queda después de implementar el control.

Ejemplo:

Una empresa tiene contraseñas débiles en sus sistemas informáticos. Esto representa una vulnerabilidad que puede ser explotada por un atacante para acceder sin autorización a la información confidencial de la empresa. El impacto de este incidente podría ser la pérdida de datos confidenciales, lo que podría dañar la reputación de la empresa y generar pérdidas económicas. La probabilidad de que ocurra este incidente es alta, ya que las contraseñas débiles son una vulnerabilidad común. El riesgo asociado a este incidente es alto, ya que el impacto es alto y la probabilidad es alta.

Para mitigar este riesgo, la empresa puede implementar políticas de contraseñas seguras. Estas políticas deben incluir requisitos de longitud, complejidad y cambio periódico de las contraseñas.

Conclusión:

Un mapa de riesgos informáticos es una herramienta útil para la gestión de la seguridad de la información. Al identificar, evaluar y mitigar los riesgos, las organizaciones pueden proteger sus activos de información y reducir el impacto de los incidentes de seguridad.

3.2.2.3.1 Estudio de caso:

* Seleccionar una empresa o entidad colombiana con una buena gestión de la seguridad de la información.

* Investigar las políticas y prácticas que la empresa implementa para proteger la información.

* Identificar los factores clave del éxito de la empresa en la gestión de la seguridad de la información.

* Presentar el caso al grupo y discutir las lecciones aprendidas que se pueden aplicar en otras organizaciones.

3.2.2.3.2 Encuesta.

* Realizar una encuesta a los participantes sobre sus conocimientos y prácticas en materia de seguridad de la información.

* Incluir preguntas sobre:

  * Nivel de conocimiento sobre la Ley de Habeas Data y la Ley de Protección de Datos Personales.

  * Prácticas para proteger las contraseñas y la información personal.

  * Percepción del riesgo de sufrir un ataque informático.

  * Expectativas sobre la guía.

* Analizar los resultados de la encuesta y discutir las áreas de mejora en materia de seguridad de la información.

3.2.2.3.3 Debate

* Organizar un debate sobre un tema controversial relacionado con la seguridad de la información en Colombia, como el uso de las redes sociales o el almacenamiento de datos en la nube.

* Dividir al grupo en dos equipos que defenderán diferentes posiciones sobre el tema.

* Brindar al grupo tiempo para investigar y preparar sus argumentos.

* Moderar el debate y garantizar que se mantenga un ambiente de respeto y diálogo.

* Al final del debate, realizar una síntesis de los argumentos presentados y las conclusiones alcanzadas.

3.2.2.3.3 Recursos:

* Ley de Habeas Data: https://www.sic.gov.co/manejo-de-informacion-personal

* Ley de Protección de Datos Personales: https://www.minambiente.gov.co/politica-de-proteccion-de-datos-personales/

* Marco normativo de seguridad de la información en Colombia: http://seguridadinformacioncolombia.blogspot.com/2010/02/marco-legal-de-seguridad-de-la.html

* Cartilla de seguridad de la información para ciudadanos: https://www.itrc.gov.co/observatorio/wp-content/uploads/2018/03/CARTILLA-INFORMATICA-ilovepdf-compressed.pdf

3.4 Actividades de Transferencia:

3.4.1 Estudio de Caso

Objetivo:

Analizar un caso real de una empresa o entidad que haya enfrentado un incidente de seguridad de la información.

Identificar las causas del incidente.

Proponer medidas para prevenirlo en el futuro.

Caso de estudio:

Empresa: Equifax

Incidente: Fuga de datos en 2017

Descripción:

En septiembre de 2017, Equifax, una de las empresas de información crediticia más grandes del mundo, sufrió una fuga de datos que afectó a más de 145 millones de personas. Los atacantes explotaron una vulnerabilidad en la aplicación web de la empresa para acceder a información confidencial, incluyendo nombres, direcciones, números de la Seguridad Social y fechas de nacimiento.

Causas:

Vulnerabilidad en la aplicación web: La aplicación web de Equifax tenía una vulnerabilidad conocida como "Apache Struts 2 Remote Code Execution" que permitía a los atacantes ejecutar código arbitrario en el servidor.

Falta de medidas de seguridad: Equifax no tenía implementadas medidas de seguridad básicas como un firewall de aplicaciones web o un sistema de detección de intrusiones.

Falta de respuesta adecuada: Equifax tardó más de un mes en notificar a los clientes afectados sobre la fuga de datos.

Medidas para prevenirlo:

Implementar medidas de seguridad: Implementar un firewall de aplicaciones web, un sistema de detección de intrusiones y otras medidas de seguridad para proteger las aplicaciones web.

Realizar pruebas de seguridad: Realizar pruebas de seguridad periódicas para identificar y corregir vulnerabilidades en las aplicaciones web.

Contar con un plan de respuesta a incidentes: Desarrollar un plan de respuesta a incidentes que defina las acciones a tomar en caso de un ataque informático.

Actividad:

Divida a los participantes en grupos de 3 a 5 personas.

Entregue a cada grupo una copia del caso de estudio.

Pida a los grupos que analicen el caso de estudio y respondan las siguientes preguntas:

¿Cuáles fueron las causas del incidente?

¿Qué medidas se podrían haber tomado para prevenirlo?

¿Qué medidas debería tomar Equifax ahora para mejorar su seguridad informática?

Cada grupo presenta sus conclusiones al resto del grupo.

Se realiza una discusión general sobre el caso de estudio.

Evaluación:

Se evaluará la participación de los participantes en la actividad, la calidad de sus respuestas y análisis, y su capacidad para trabajar en equipo.

Reflexión final:

La seguridad de la información es un tema fundamental para cualquier empresa o entidad en la actualidad. Esta actividad le ha permitido reflexionar sobre la importancia del tema y su conocimiento actual. A lo largo de la guía, profundizará en estos conceptos y adquirirá las herramientas necesarias para implementar una gestión eficaz de la seguridad de la información en su organización.

¡Esperamos que esta actividad haya sido de provecho!

4. ACTIVIDADES DE EVALUACIÓN

Evidencias de Aprendizaje	Criterios de Evaluación	Técnicas e Instrumentos de Evaluación
Evidencias de Desempeño: Participación crítica y propositiva frente a las actividades de aprendizaje. **Evidencias de Producto:** Ejemplos de Aplicaciones de las políticas de seguridad y privacidad de la información aplicadas en Colombia.	**1. Conocimiento teórico:** Los aprendices deben ser capaces de definir los conceptos básicos de la seguridad de la información. Deben comprender las principales amenazas y vulnerabilidades a las que están expuestas las empresas y entidades. Deben conocer las diferentes medidas que se pueden tomar para proteger la información. **2. Habilidades prácticas:** Los aprendices deben ser capaces de aplicar los conocimientos adquiridos en la guía para resolver problemas reales de seguridad de la información. Deben ser capaces de analizar riesgos, implementar medidas de seguridad y gestionar incidentes de seguridad. 3**. Actitud:** Los aprendices deben mostrar una actitud proactiva y responsable frente a la seguridad de la información. Deben ser conscientes de la importancia de proteger la	Observación

	información y estar dispuestos a tomar medidas para hacerlo.	

5. GLOSARIO DE TÉRMINOS

- **Acceso:** Permiso para obtener información o utilizar un recurso.
- **Amenaza:** Evento o acción que puede poner en riesgo la seguridad de la información.
- **Autenticación:** Proceso de verificar la identidad de un usuario.
- **Autorización:** Permiso para realizar una acción sobre un recurso.
- **Confidencialidad:** Propiedad de la información que solo debe ser conocida por las personas autorizadas.
- **Copia de seguridad:** Duplicado de la información que se utiliza para restaurarla en caso de pérdida o daño.

- **Cifrado:** Proceso de convertir la información en un formato que solo puede ser leído por las personas autorizadas.

- **Contraseña:** Secuencia de caracteres 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 y a los recursos.

- **Datos personales:** Cualquier información que pueda ser utilizada para identificar a una persona.

- **Desastre natural:** Evento natural que puede causar daños a la infraestructura y a la información.

- **Encriptación:** Término sinónimo de cifrado.

- **Error humano:** Acción involuntaria que puede poner en riesgo la seguridad de la información.

- **Evaluación de riesgos:** Proceso de identificar, analizar y evaluar los riesgos que pueden afectar la seguridad de la información.

- **Gestión de riesgos:** Proceso de implementar medidas para controlar y mitigar los riesgos que pueden afectar la seguridad de la información.

- **Incidente de seguridad:** Evento que viola la confidencialidad, integridad o disponibilidad de la información.

- **Integridad:** Propiedad de la información que debe ser completa, precisa y confiable.

- **Malware:** Software malicioso que puede infectar un sistema informático y causar daños.

- **Política de seguridad:** Conjunto de reglas y procedimientos que se utilizan para proteger la información.

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

- **Respaldo:** Término sinónimo de copia de seguridad.

- **Riesgo:** Probabilidad de que ocurra un evento que pueda afectar la seguridad de la información.

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

- **Vulnerabilidad:** Debilidad en un sistema o proceso que puede ser explotada por una amenaza.

REFERENTES BILBIOGRÁFICOS

Libros:

- "Seguridad informática: un enfoque práctico" de William Stallings (2017)
- "Gestión de riesgos de seguridad de la información" de James H. Graham (2018)
- "Ciberseguridad para todos: cómo protegerte en el mundo digital" de Daniel J. Solove (2020)

Normas:

- ISO/IEC 27001:2013 (https://www.iso.org/isoiec-27001-information-security.html)
    - Ley 1266 de 2008: https://acortar.link/ntlazT

Sitios web:

Centro Cibernético Policial (CECIP):https://caivirtual.policia.gov.co/

Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC) (https://www.mintic.gov.co/)

6. CONTROL DEL DOCUMENTO

	Nombre	Cargo	Dependencia	Fecha
Autor (es)	Wilman Jesus Peña Guzman	Instructor	Centro de Biotecnología Agropecuaria	Abril de 2024