PROCESO DE GESTIÓN DE FORMACIÓN PROFESIONAL INTEGRAL
GUÍA DE APRENDIZAJE 4

IDENTIFICACIÓN DE LA GUIA DE APRENDIZAJE

- **Denominación del Programa de Formación:** Controles y seguridad informática.
- **Código del Programa de Formación:** 21730025.
- **Competencia:** 220501019. Verificar la vulnerabilidad de la red contra ataques de acuerdo con las políticas de seguridad de la empresa.
- **Resultados de Aprendizaje Alcanzar:** 220501019_03. Identificar los conceptos básicos sobre seguridad informática y delitos informáticos.
- **Duración de la Guía:** 10 horas.

2. PRESENTACIÓN

Bienvenido a la actividad de aprendizaje 4 del programa de formación Controles y Seguridad Informática.

Uno de los bienes más preciados en la empresa es la información, esta se encuentra expuesta a muchos riesgos a lo largo de todo su manejo, desde que es generada, hasta que es almacenada. Es por eso que las empresas deben establecer políticas de seguridad de tipo lógico y físico. Ambas de la misma importancia para conservar a la información segura.

La seguridad física y lógica de la información cada vez más está siendo amenazada por el incremento en los delitos informáticos y el terrorismo computacional, es por eso que las organizaciones se deben encontrar preparadas para no dejar ninguna vulnerabilidad en su sistemas y utilizar todos los recursos a su alcance para proteger todos los recursos computacionales y de información estratégicos para el negocio.

Para realizar las evidencias correspondientes de esta actividad de aprendizaje, es necesario revisar los materiales del programa de formación, explorar los documentos de apoyo y realizar consultas en internet.

Con la actividad de aprendizaje propuesta en esta guía usted podrá “Identificar los conceptos básicos sobre seguridad informática y delitos informáticos”.

¡Éxitos en su proceso de formación!

3. FORMULACIÓN DE LAS ACTIVIDADES DE APRENDIZAJE

3.1 Actividad de aprendizaje 4: Reconocer las posibles amenazas, riesgos, delitos, a los que está expuesta la información de una empresa.

A continuación, se describen las evidencias que conforman la actividad de aprendizaje 4:

- **Actividades de Reflexión inicial.**

  Es importante conocer e identificar los conceptos de seguridad física y lógica, así como las diferentes formas en que se puede proteger la información y todos los recursos computacionales de los delitos informáticos y el terrorismo computacional. Se le invita a que reflexione sobre las siguientes preguntas:

  ¿Qué entiende por seguridad informática?
  ¿Qué decisiones se deben tomar, si en la empresa donde labora se presentan delitos informáticos?

  Nota: esta actividad tiene como finalidad encaminarlo y motivarlo en el desarrollo de los temas de esta guía de aprendizaje, por tal motivo no es calificable.

- **Actividades de apropiación del conocimiento (Conceptualización y Teorización).**

  Cuestionario: seguridad informática

  Para el desarrollo de esta actividad y la apropiación del conocimiento que esta sugiere, deberá consultar los recursos para el aprendizaje y en específico el material de formación 4.

  El desarrollo del resultado de aprendizaje “Identificar los conceptos básicos sobre seguridad informática y delitos informáticos.”, hace necesario que usted como aprendiz apropie conocimientos basados en los siguientes conceptos:

  - Generalidades
  - Seguridad lógica - física
  - Políticas de seguridad informática
  - Delitos informaticos
  - Terrorismo computacional

  Una vez revisado el material mencionado y resuelto las inquietudes con su instructor, se le solicita responder la evaluación de conocimientos sobre seguridad informática.

  Para acceder a la evidencia remítase a la ***Actividad 4 / Evidencias / Cuestionario: seguridad informatica.***

  Nota: esta actividad es calificable.

- **Actividades de transferencia de conocimiento.**

  Informe: delitos informáticos y terrorismo computacional

Actualmente los delitos informáticos son algo que se encuentra en aumento, un campo que tiene gran crecimiento son los medios electrónicos, pero igualmente es uno de los puntos más vulnerables, y hasta ahora las legislaciones de los países se están preparando para combatirlos.

Al escuchar las palabras terrorismo computacional nos llevan a pensar en actividades que no son del agrado para nadie. Estas actividades se realizan aplicando diferentes tipos de software que puede generar un gran daño a uno de los más importantes recursos de la empresa como lo es la información. Se encuentran en la red gran cantidad de softwares que se clasifican en el área de terrorismo computacional, entre ellos se encuentran: los spywares, falsos virus y spam, entre otros.

Después de revisar el material de estudio y complementario propuesto, desarrolle un informe sobre estos dos temas (delitos informáticos y terrorismo computacional) donde se tenga en cuenta:

1. Indague en Internet y/o en cualquier otra fuente bibliográfica, artículos que presenten información sobre cuáles son los principales delitos informáticos y su definición.
2. Presente ejemplos de situaciones relacionadas con terrorismo computacional.
3. Defina y de ejemplos de: spyware, anti-virus, maleware, hoaxes, etc.

El informe a presentar debe contener la investigación realizada, donde se de respuesta los ítems propuestos, proceda a elaborar el texto en un documento de Word (procesador de texto), tenga en cuenta las normas APA para su elaboración. Importante realizar las referencias bibliográficas correspondientes.

Guarde el documento final y envíelo dentro del plazo señalado por su instructor.

Resuelta la actividad, para entregar la evidencia remítase a la ***Actividad 4 / Evidencias / Informe: delitos informáticos y terrorismo computacional.***

Nota: esta actividad es calificable.

3.2 Ambiente requerido

- Ambiente virtual de aprendizaje (LMS).

3.3 Materiales

- Material de formación 4.
- Material de apoyo 4.

Total horas actividad de aprendizaje: 10 horas; 2 directas (D), 8 independientes (I).

4. ACTIVIDADES DE EVALUACIÓN

Evidencias de Aprendizaje	Criterios de Evaluación	Técnicas e Instrumentos de Evaluación
Evidencia de conocimiento : Cuestionario: seguridad informática.	• Interpreta los principios de la seguridad informática. • Aplica los conceptos de	**Técnica:** Formulación de preguntas. **Instrumento**: Cuestionario .

Evidencia de Producto: Informe: delitos informáticos y terrorismo computacional.	seguridad informática a la administración de sistema de información. • Diseña estrategias en la organización para combatir la seguridad informática.	**Técnica:** Valoración de producto. **Instrumento**: Informe.

5. GLOSARIO DE TÉRMINOS

Activo: recurso necesario para el funcionamiento de la organización y el cumplimiento de objetivos.

Amenaza: evento que al ocurrir ocasionaría un daño sobre los activos.

Impacto: el resultado de que una amenaza ocurra.

Riesgo: posibilidad de que algo suceda sobre uno o más activos de la organización.

Spam: correo electrónico que no ha sido solicitado por quien lo recibe y normalmente es de contenido publicitario y es enviado de forma masiva.

Spyware: software que recopila información de un ordenador y después transmite esta información a una entidad externa sin el conocimiento o el consentimiento del propietario del ordenador.

Vulnerabilidad: posibilidad de que ocurra una amenaza sobre un activo.

6. REFERENTES BILBIOGRÁFICOS

Galdámez P. (s.f). Seguridad informática. Actualidad TIC.

Ley 1273 de 2009. Por medio de la cual se modifica el código penal, se crea un nuevo bien jurídico tutelado – denominado “del a protección de la información y de los datos”- y se preserva integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones.

Manjarrés, I; Jiménez F. (2012) Caracterización de los delitos informáticos en Colombia.

Valdés, M. (s.f). Departamento de sistemas de información. Instituto Tecnológico y de estudios superiores de Monterrey. México.

7. CONTROL DEL DOCUMENTO

	Nombre	Cargo	Dependencia	Fecha
Autor (es)	Elsa Cristina Arenas Martínez.	Experta temática.	SENA Centro Industrial de Mantenimiento Integral. Girón (Santander).	Julio de 2015
	Elsa Cristina Arenas Martínez. Juan José Botello Castellanos.	Asesores pedagógicos.		
	Santiago Lozada Garcés.	Líder línea de producción Santander.		

8. CONTROL DE CAMBIOS

	Nombre	Cargo	Dependencia	Fecha	Razón del Cambio
Autor (es)	María Yaneth Osorio Caro.	Instructora.	Centro de la Industria, la Empresa y los Servicios – Neiva.	Agosto de 2020.	Actualización formato.