1. IDENTIFICACIÓN DE LA GUÍA DE APRENDIZAJE

- **Denominación del Programa de Formación:** Redes y Seguridad.
- **Código del Programa de Formación:** 83240071.
- **Nombre del Proyecto:** N/A.
- **Fase del Proyecto:** N/A.
- **Actividad de Proyecto:** N/A.
- **Competencia:**

  220501014: Instalar y administrar *hardware* y *software* de seguridad en la red a partir de normas internacionales.

- **Resultados de Aprendizaje a alcanzar:**

  220501014-04: Desarrollar un plan de acción para implantar las políticas de seguridad informática en diversas jerarquías de la empresa.

- **Duración de la guía:** 10 horas.

2. PRESENTACIÓN

Estimado aprendiz, el SENA le da la bienvenida a la última actividad de aprendizaje del programa de formación **Redes y Seguridad,** en la cual se aplicarán todos los contenidos estudiado durante este programa. También se elaborará un plan de acción

de seguridad informática o Políticas de Seguridad Informática (PSI). Para esto se recordarán los temas de redes de tecnología, el concepto de seguridad informática y también a lo referente a la vulnerabilidad de la red tecnológica frente a los ataques informáticos que ponen en riesgo la información de la empresa.

Para el desarrollo de las actividades planteadas en esta guía, contará con el acompañamiento del instructor asignado al programa, quien de forma continua y permanente lo orientará con las pautas necesarias para el logro de las actividades de aprendizaje, brindando herramientas básicas de tipo conceptual y metodológico, enmarcadas en las políticas de ética y calidad.

De igual manera, el instructor programará una asesoría virtual a través de la plataforma, para brindar orientaciones específicas relacionadas con las temáticas a desarrollar en las actividades. La fecha y el horario para este encuentro virtual serán indicados oportunamente.

Es importante que organice su tiempo con un promedio de trabajo diario de dos horas, dada la exigencia que demanda la realización de las actividades que se mencionan en esta guía de aprendizaje. También es necesario revisar los materiales del programa, realizar consultas en internet y explorar los siguientes materiales complementarios:

- ¿Cómo crear un plan de seguridad informática?

- Importancia de la seguridad informática en las empresas.

3. FORMULACIÓN DE LAS ACTIVIDADES DE APRENDIZAJE

3.1 Actividad de aprendizaje 4: Elaborar un plan de acción para evitar la pérdida de información de acuerdo con las políticas de seguridad establecidas en la empresa.

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

Destacar la responsabilidad del administrador de la red informática de la empresa

Lea detenidamente el siguiente texto y reflexione sobre el contenido a partir de la pregunta formulada.

> El administrador de la red de información es el único responsable de la seguridad de la información en una empresa.

¿Está de acuerdo o no en que el administrador de la red de información de una empresa es el único responsable de la seguridad de la información? Argumente su respuesta.

Nota: la actividad descrita de reflexión y conocimientos previos, tiene como finalidad encaminarlo en el desarrollo de los temas de la actividad de aprendizaje, por lo tanto, no es calificable; sin embargo, es importante su realización, ya que puede ser solicitada más adelante en esta guía de aprendizaje.

Reconocer la importancia de las políticas de seguridad informática en una empresa

Las políticas de seguridad informática de una empresa son los procedimientos que se redactan en un documento para ser impartidos a todos los funcionarios de la empresa. Este plan de acción de seguridad informática está encaminado a proteger la base de datos de la red tecnológica. Y es por eso que este plan es único y exclusivo para cada empresa, ya que el inventario tecnológico y el tipo de información dependen de la misma.

Con base en la anterior información, en el material de formación Conceptos de políticas de seguridad informática y en el material complementario correspondiente a la actividad de aprendizaje 4, participe en el foro temático Reconocer la importancia de las políticas de seguridad informática en una empresa, respondiendo a los siguientes interrogantes. Justifique sus respuestas.

1. ¿Cuál es la importancia de establecer políticas de seguridad en una empresa?

2. ¿Qué proceso se debe tener en cuenta después que un usuario permite que otras personas tengan acceso al equipo, sin tener en cuenta las políticas de seguridad implantadas en la empresa?

3. Como administrador de una red tecnológica, ¿qué controles se deben establecer para proteger el *software* de una empresa?

4. Desde el mismo rol, ¿qué controles establece usted para asegurar que los usuarios de la empresa protejan la información?

5. Una de las políticas de seguridad informática, recomienda efectuar copias de seguridad a la información (*backup*). Como administrador de una red tecnológica en una empresa, ¿cada cuánto recomendaría efectuar este proceso?, ¿por qué?

6. En la participación del foro, dé respuesta al interrogante planteado en la evidencia de reflexión Destacar la responsabilidad del administrador de la red informática de la empresa.

7. Comente la participación de al menos dos compañeros y argumente el porqué está o no de acuerdo con la opinión plasmada por ellos.

Ambiente Requerido: Ambiente Virtual de Aprendizaje, Foro.

Materiales: computador, internet, material de formación Conceptos de políticas de seguridad informática, material complementario, glosario y biblioteca SENA.

Evidencia: Foro. Reconocer la importancia de las políticas de seguridad informática en una empresa.

Para acceder a la evidencia remítase al menú principal, haciendo clic en el enlace Actividad 4 / Evidencia: Foro. Reconocer la importancia de las políticas de seguridad informática en una empresa.

Implantar las políticas de seguridad informática en una empresa

Es un día especial para Julián, el administrador de la red tecnológica de información de la empresa LPQ S.A, porque recibirá la visita de los aprendices SENA del programa Redes y Seguridad, con ellos recorrerá las oficinas de la empresa, donde de manera

directa podrán verificar las Políticas de Seguridad Informática que Julián ha establecido para proteger la información frente a los ataques informáticos.

Por sus conocimientos en el tema, usted como aprendiz los acompañará en el recorrido, ayudándoles a responder las preguntas que realizará Julián.

Tenga en cuenta que si responde incorrectamente tres o más preguntas perderá la actividad interactiva y el grupo de aprendices desaprovechará la posibilidad de volver pronto a la empresa de Julián.

Ambiente requerido: Ambiente Virtual de Aprendizaje, Actividad interactiva.

Materiales: computador, internet, material de formación Conceptos de políticas de seguridad informática, material complementario, glosario y biblioteca SENA.

Evidencia: Actividad interactiva. Implantar las políticas de seguridad informática en una empresa.

Para acceder a la evidencia, remítase al menú principal, haciendo clic en el enlace Actividad 4 / Evidencia: Actividad interactiva. Implantar las políticas de seguridad informática en una empresa.

Diseñar políticas de seguridad informática para una empresa

Un plan de acción de seguridad informática va dirigido a una empresa. Sin importar su tamaño y su actividad comercial, este se debe identificar con el nombre de la empresa y su ubicación, porque será de uso exclusivo de esta. Se deben definir los elementos informáticos con los que cuenta la empresa para priorizar y establecer los controles para proteger la información.

Los funcionarios de la empresa son de vital importancia para garantizar el cumplimiento de la política de seguridad informática. Ellos son los encargados de poner en ejecución cada una de las acciones establecidas para garantizar que la información de la red tecnológica cumpla con la filosofía de integridad y confiabilidad.

Para cumplir con esta evidencia, diseñe las políticas de seguridad informática para una empresa. Tenga en cuenta los siguientes pasos:

1. Consulte el material de formación Conceptos de políticas de seguridad informática y el material complementario dispuesto para esta actividad de aprendizaje.

2. Identifique una empresa con nombre, actividad comercial y ubicación de la misma.

3. Describa las dependencias de la empresa, defina las funciones de cada una de ellas y el tipo de información que maneja.

4. Identifique los elementos informáticos como *software*, *hardware* y el tipo de red de tecnología con el cual cuenta la empresa.

5. Con la información obtenida anteriormente, diseñe un plan de acción con las políticas de seguridad que regirán la empresa para protegerla de ataques informáticos y así evitar la pérdida de la información de la empresa.

6. Desarrolle esta evidencia con la herramienta ofimática de su preferencia y envíela al instructor a través de la plataforma virtual de aprendizaje.

Ambiente requerido: Ambiente Virtual de Aprendizaje.

Materiales: computador, internet, material de formación Conceptos de Políticas de Seguridad Informática, material complementario, glosario y biblioteca SENA.

Evidencia: Plan de acción. Diseñar políticas de seguridad informática para una empresa.

Para acceder a la evidencia remítase al menú principal, haciendo clic en el enlace Actividad 4 / Evidencia: Plan de acción. Diseñar políticas de seguridad informática para una empresa.

Nota: si al momento de enviar un archivo (evidencia) el sistema genera el error "archivo inválido", tenga en cuenta que una posible razón para ello, es que el documento estaba abierto al momento de adjuntarse. Por eso, es recomendable que cierre el archivo e intente el procedimiento nuevamente.

Participar en el sondeo de evaluación del programa

Recuerde realizar el sondeo de evaluación del programa con el fin de conocer su experiencia en el proceso de aprendizaje que ha culminado.

Para acceder al sondeo remítase al menú principal, haciendo clic en el enlace Actividad 4 / Sondeo de evaluación del programa.

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
De conocimiento. **Evidencia:** Foro. Reconocer la importancia de las políticas de seguridad informática en una empresa.	Crea planes de acción para el establecimiento de políticas de seguridad informática.	**Rúbrica.** Foro.
De conocimiento. **Evidencia:** Actividad interactiva. Implantar las políticas de seguridad informática en una empresa.		**Cuestionario.** Actividad interactiva.
De producto. **Evidencia:** Plan de acción. Diseñar políticas de seguridad informática para una empresa.		**Lista de chequeo.** Informe.

5. GLOSARIO DE TÉRMINOS

***Backup*:** copia idéntica de la información.

Base de datos: todo el paquete de información que se transmite a través de una red.

Contraseña: combinaciones de caracteres que permiten el acceso a información.

Políticas de seguridad: controles establecidos dentro de una empresa para garantizar la protección de la información.

Usuario: persona autorizada para tener acceso a la información.

Virus: archivos ejecutables que dañan la información de un sistema de datos.

6. REFERENTES BIBLIOGRÁFICOS

Ministerio de Ambiente y Desarrollo Sostenible. (s.f.). *Política de seguridad informática.* Recuperado de http://www.minambiente.gov.co/index.php/tecnologias-de-la-informacion-y-la-comunicacion/gestion-ti/politica-de-seguridad-informatica

Secretaría de TIC, Ciencia, Tecnología e Innovación. (2013). *Políticas de seguridad informática de la gobernación del Meta. Recuperado de* https://www.meta.gov.co/web/sites/default/files/adjuntos/M-TIC-01%20POLITICA%20SEGURIDAD%20V3.pdf

Tuyú Technology. (2017). *¿Por qué es tan importante la seguridad informática?* Recuperado de www.tuyu.es/importancia-seguridad-informatica/

7. CONTROL DEL DOCUMENTO

	Nombre	Cargo	Dependencia	Fecha
Autor(es)	Olga Elena Meneses Camino.	Desarrollador de contenidos.	Centro para la Formación Cafetera-Regional Caldas.	Marzo de 2019.

8. CONTROL DE CAMBIOS

	Nombre	Cargo	Dependencia	Fecha	Razón del cambio
Autor(es)	Juan Carlos Ramírez Molina.	E-pedagogo instruccional.	Centro Agroindustrial Regional Quindío	Abril de 2019.	Ajustes pedagógicos y metodológicos en las actividades y sus correspondientes evidencias.

	Lina Marcela Cardona Orozco.	Evaluador de contenidos.	Centro de Atención Sector Agropecuario-Regional Risaralda.	Mayo de 2019.	Ajustes pedagógicos y metodológicos en las actividades y sus correspondientes evidencias.
	Erika Alejandra Beltrán Cuesta.	Evaluador de calidad instruccional.	Centro de Atención Sector Agropecuario-Regional Risaralda.	Mayo de 2019.	Ajustes pedagógicos y metodológicos en las actividades y sus correspondientes evidencias.