



SERVICIO NACIONAL DE APRENDIZAJE SENA
Procedimiento de Desarrollo Curricular
GUÍA DE APRENDIZAJE

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:**

220501014-02: Identificar los ataques más comunes a las empresas y plantear alternativas de solución de acuerdo con el conocimiento de las herramientas de control de acceso.

- **Duración de la guía:** 10 horas.



2. PRESENTACIÓN

Estimado aprendiz, el SENA le da la bienvenida a la segunda actividad de aprendizaje del programa **Redes y Seguridad**, en la cual se efectuarán actividades concernientes a la comprensión de los conceptos de los ataques informáticos en las redes tecnológicas, así mismo, se plantearán las políticas de seguridad informática.

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 prevenir la fuga de datos empresariales a través de sistemas informáticos?
- 10 consejos para evitar un ataque cibernético empresarial.
- 10 Recomendaciones básicas para evitar ataques



- Pasos para elaborar un mapa de cajas.

3. FORMULACIÓN DE LAS ACTIVIDADES DE APRENDIZAJE

3.1 Actividad de aprendizaje 2: Reconocer ataques informáticos teniendo en cuenta los diferentes tipos de redes.

A continuación, se describen las actividades y las correspondientes evidencias que conforman la actividad de aprendizaje 2:

Reconocer los diferentes ataques informáticos que afectan las redes en una empresa

Lea detenidamente el siguiente texto y dé respuesta a las preguntas formuladas. Esta actividad es clave para la comprensión del tema, por ello lo invitamos a desarrollarla.

Hoy en día, la tecnología se encuentra en toda actividad que desarrollemos. Por lo tanto, nos encontramos expuestos a posibles ataques informáticos.

¿Por qué nos encontramos expuestos a los ataques informáticos? Y, en caso de ocurrir, ¿cuáles serían las posibles consecuencias? Responda la pregunta desde la perspectiva de los hogares y desde la empresarial.

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.

Identificar los ataques más comunes a una red informática

Los ataques informáticos son *software* que, al ser ejecutados por personas expertas, invaden las redes de una empresa, con el fin de causar daño a la información.

Hay una gran cantidad de ataques, pero el más común es el virus informático, el cual se puede transferir de múltiples maneras. Las consecuencias de que un virus entre en el sistema pueden ir desde un daño parcial hasta la pérdida total de la información, la alteración de los sistemas o la extracción de información importante para la organización.

Con base en la información anterior realice lo siguiente:

- Elabore un mapa de cajas, en el cual la idea central sea los ataques informáticos.
- En el segundo nivel, escriba el nombre de los ataques informáticos que usted determine son los más comunes y que ponen en riesgo la red de información (mínimo cinco).
- En el tercer nivel, escriba los riesgos en los que se incurre por cada ataque informático.
- En el cuarto nivel, sintetice las consecuencias de estos ataques a la red de información.

Para lograr el éxito en la evidencia consulte el material de formación Fundamentos básicos de los conceptos de ataques informáticos en las redes tecnológicas,



SERVICIO NACIONAL DE APRENDIZAJE SENA
Procedimiento de Desarrollo Curricular
GUÍA DE APRENDIZAJE

correspondiente a la actividad de aprendizaje 2 y el material complementario Pasos para elaborar un mapa de cajas.

Ambiente Requerido: Ambiente Virtual de Aprendizaje.

Materiales: computador, internet, material de formación Fundamentos básicos de los conceptos de ataques informáticos en las redes tecnológicas, material complementario, glosario y biblioteca SENA.

Evidencia: Mapa de cajas. Identificar los ataques más comunes a una red informática.

Para acceder a la evidencia, remítase al menú principal, haciendo clic en el enlace Actividad 2 / Evidencia: Mapa de cajas. Identificar los ataques más comunes a una red informática.

Determinar las políticas de protección contra ataques informáticos

Todos los días las empresas están expuestas a perder información debido a la falta de seguridad frente a los ataques informáticos, nos encontramos en riesgo desde el momento de encender el computador y navegar en internet. Por lo tanto, debemos estar preparados para estos eventos que perjudican la información de datos y aplicativos que reposan en nuestros equipos.

Para evitar este riesgo, se hace necesario establecer e implementar una política de protección contra los ataques, que nos permita ejecutar con tranquilidad las operaciones informáticas.

Por lo anterior y con el fin de cumplir con esta evidencia, siga las indicaciones que se describen a continuación:



SERVICIO NACIONAL DE APRENDIZAJE SENA
Procedimiento de Desarrollo Curricular
GUÍA DE APRENDIZAJE

1. Tenga en cuenta lo aprendido en el material de formación Fundamentos básicos de los conceptos de ataques informáticos en las redes tecnológicas, correspondiente a la actividad de aprendizaje 2.
2. Diseñe un plegable en el que se estructure una política de seguridad informática con sus respectivas acciones de prevención y cada uno de los procesos a efectuar frente a los posibles ataques que pueda sufrir una empresa.
3. Recuerde responder a la pregunta formulada en la evidencia Reconocer los diferentes ataques informáticos que afectan las redes en una empresa, que se encuentra al inicio de esta guía de aprendizaje.
4. 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 Fundamentos básicos de los conceptos de ataques informáticos en las redes tecnológicas, material complementario, glosario y biblioteca SENA.

Evidencia: Plegable. Determinar las políticas de protección contra ataques informáticos.

Para acceder a la evidencia remítase al menú principal, haciendo clic en el enlace Actividad 2 / Evidencia: Plegable. Determinar las políticas de protección contra ataques informáticos.

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



SERVICIO NACIONAL DE APRENDIZAJE SENA
Procedimiento de Desarrollo Curricular
GUÍA DE APRENDIZAJE

abierto al momento de adjuntarse. Por eso, es recomendable que cierre el archivo e intente el procedimiento nuevamente.

4. ACTIVIDADES DE EVALUACIÓN

Evidencias de aprendizaje	Criterios de evaluación	Técnicas e instrumentos de evaluación
De conocimiento. Evidencia: Mapa de cajas. Identificar los ataques más comunes a una red informática.	Establece la estructura de una política de seguridad informática.	Lista de chequeo. Mapa de cajas.
De producto. Evidencia: Plegable. Determinar las políticas de protección contra ataques informáticos.		Lista de chequeo. Plegable.

5. GLOSARIO DE TÉRMINOS

Ataque informático: acción intencionada de personas que buscan hacer daño parcial o total a una red tecnológica o a un sistema de información.

Baiting: ataque de equipos y redes de información que se lleva a cabo a través de medios extraíbles.

Malware: ataques informáticos que se realizan a través de virus.

Phishing: suplantación de identidad en una red o sistema de información.

Pirata informático: persona con gran conocimiento en sistemas tecnológicos que accede a las redes informáticas ilegalmente.



SERVICIO NACIONAL DE APRENDIZAJE SENA
Procedimiento de Desarrollo Curricular
GUÍA DE APRENDIZAJE

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

6. REFERENTES BIBLIOGRÁFICOS

Equipo editorial. (2018). *10 consejos para evitar un ataque cibernético empresarial*.

Recuperado de <https://reportedigital.com/seguridad/ataque-cibernetico-empresa-consejos/>

Freepik. (s.f.). *Pirata informático*. Recuperado de https://www.freepik.es/vector-premium/pirata-informatico-robar-datos-confidenciales_2156268.htm

Globalfinanz. Gestión Correduría de Seguros. (s.f.). *Empresas expuestas a ataques informáticos o cibernéticos*. Recuperado de <https://www.responsabilidadconsejerosydirectivos.com/ataques-ciberneticos-en-las-empresas/>

Impulsapopular. (2007). *¿Cómo prevenir la fuga de datos empresariales a través de sistemas informáticos?* Recuperado de <https://www.impulsapopular.com/tecnologia/como-prevenir-la-fuga-de-datos-empresariales-a-traves-de-sistemas-informaticos/>

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.



SERVICIO NACIONAL DE APRENDIZAJE SENA
Procedimiento de Desarrollo Curricular
GUÍA DE APRENDIZAJE

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.	Evaluator 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.	Evaluator de calidad instruccional.	Centro de Atención Sector Agropecuario-Regional Risaralda.	Mayo de 2019.	Ajustes pedagógicos y metodológicos en las actividades y sus correspondientes evidencias.