FUNDAMENTOS DE LA CIBERSEGURIDAD.

Digitalízate comunidad.

MÓDULO 1.

Tabla de contenido

1. Video: Introducción a la ciberseguridad.

Imagina que te estás preparando para una tormenta. Recibiste un aviso de emergencia y te preparas reuniendo las herramientas y materiales que necesitas para mantenerte a salvo. Aseguras las ventanas y las puertas, preparas un botiquín de primeros auxilios, herramientas, comida y agua. Lo tienes todo listo. Llega la tormenta y hay fuertes vientos y lluvias que usan su fuerza para tratar de entrar en tu hogar. Notas algunas entradas de agua y las arreglas rápidamente para minimizar riesgos o posibles daños. Hacer frente a un incidente de seguridad es parecido. Las organizaciones deben prepararse para la tormenta asegurándose de contar con herramientas para mitigar y responder a las amenazas externas. El objetivo es minimizar riesgos y posibles daños. Como analista de seguridad, trabajarás para proteger tu organización y a su personal de una serie de riesgos y amenazas externas. Y si un ataque logra entrar, tú y tu equipo deberán dar una solución. Para que entiendas mejor lo que significa, definiremos la ciberseguridad y hablaremos de los roles de profesionales de seguridad de las empresas. Comencemos con algunas definiciones: La ciberseguridad, o seguridad, es la práctica de garantizar la confidencialidad, la integridad y disponibilidad de la información protegiendo las redes, los dispositivos, a las personas y los datos del acceso no autorizado o la explotación delictiva. Por ejemplo, requerir contraseñas complejas para acceder a sitios y servicios mejora la confidencialidad y dificulta que un agente de amenaza los ponga en peligro. Un agente de amenaza es cualquier persona o grupo que representa un riesgo a la seguridad. Ya conoces la definición de ciberseguridad, veamos lo que hacen los equipos de seguridad en una organización. La ciberseguridad protege contra amenazas externas e internas. Una amenaza externa es alguien de fuera de la organización intentando acceder a información privada, redes o dispositivos. Una amenaza interna procede del personal antiguo o actual, proveedores externos, o socios/as de confianza. Las internas suelen ser accidentales, como cuando una persona hace clic en un enlace comprometido en un correo. Otras veces, el agente interno participa intencionalmente en actividades como el acceso no autorizado a datos o abuso de los sistemas para uso personal. Los especialistas en ciberseguridad con experiencia ayudan a las organizaciones a mitigar o reducir el impacto de estas amenazas. Los equipos de seguridad también garantizan que una organización cumpla las normativas, leyes y directrices que requieran la implementación de estándares de seguridad específicos. Garantizar que las organizaciones cumplan la normativa puede evitar multas y auditorías, al tiempo que respetan su obligación ética de proteger a sus usuarios/as. Los equipos de seguridad mantienen y mejoran la productividad. Al crear un plan de continuidad del negocio, los equipos de seguridad permiten que cada cual haga su trabajo, incluso cuando ocurre una filtración de datos. Ser conscientes de la seguridad también puede reducir gastos vinculados a los riesgos, como la recuperación de datos o el tiempo de inactividad, y evitar posibles multas. La última ventaja de la que hablaremos es mantener la confianza en la marca. Si se comprometen los servicios o los datos de sus clientes, puede disminuir la confianza en la empresa, dañar la marca y el negocio. Si sus clientes pierden la confianza, implica menos ingresos para el negocio. Repasemos ahora algunos roles comunes basados en la seguridad. Después de completar esta certificación, estos son los posibles puestos que quizás desees buscar: Especialista o analista de seguridad, especialista o analista de ciberseguridad, analista del centro de operaciones de seguridad o SOC y analista de seguridad de la información. También conocerás las responsabilidades asociadas a algunos de estos puestos de trabajo, más adelante. Como te habrás dado cuenta, el campo de la seguridad incluye muchos temas y conceptos y cada actividad que completes en este programa es un paso más hacia un nuevo empleo. ¡Sigamos aprendiendo!

Imagina que te estás preparando para una tormenta. Recibiste un aviso de emergencia y te preparas reuniendo las herramientas y materiales que necesitas para mantenerte a salvo. Aseguras las ventanas y las puertas, preparas un botiquín de primeros auxilios, herramientas, comida y agua. Lo tienes todo listo. Llega la tormenta y hay fuertes vientos y lluvias que usan su fuerza para tratar de entrar en tu hogar. Notas algunas entradas de agua y las arreglas rápidamente para minimizar riesgos o posibles daños. Hacer frente a un incidente de seguridad es parecido. Las organizaciones deben prepararse para la tormenta asegurándose de contar con herramientas para mitigar y responder a las amenazas externas. El objetivo es minimizar riesgos y posibles daños. Como analista de seguridad, trabajarás para proteger tu organización y a su personal de una serie de riesgos y amenazas externas. Y si un ataque logra entrar, tú y tu equipo deberán dar una solución. Para que entiendas mejor lo que significa, definiremos la ciberseguridad y hablaremos de los roles de profesionales de seguridad de las empresas. Comencemos con algunas definiciones: La ciberseguridad, o seguridad, es la práctica de garantizar la confidencialidad, la integridad y disponibilidad de la información protegiendo las redes, los dispositivos, a las personas y los datos del acceso no autorizado o la explotación delictiva. Por ejemplo, requerir contraseñas complejas para acceder a sitios y servicios mejora la confidencialidad y dificulta que un agente de amenaza los ponga en peligro. Un agente de amenaza es cualquier persona o grupo que representa un riesgo a la seguridad. Ya conoces la definición de ciberseguridad, veamos lo que hacen los equipos de seguridad en una organización. La ciberseguridad protege contra amenazas externas e internas. Una amenaza externa es alguien de fuera de la organización intentando acceder a información privada, redes o dispositivos. Una amenaza interna procede del personal antiguo o actual, proveedores externos, o socios/as de confianza. Las internas suelen ser accidentales, como cuando una persona hace clic en un enlace comprometido en un correo. Otras veces, el agente interno participa intencionalmente en actividades como el acceso no autorizado a datos o abuso de los sistemas para uso personal. Los especialistas en ciberseguridad con experiencia ayudan a las organizaciones a mitigar o reducir el impacto de estas amenazas. Los equipos de seguridad también garantizan que una organización cumpla las normativas, leyes y directrices que requieran la implementación de estándares de seguridad específicos. Garantizar que las organizaciones cumplan la normativa puede evitar multas y auditorías, al tiempo que respetan su obligación ética de proteger a sus usuarios/as. Los equipos de seguridad mantienen y mejoran la productividad. Al crear un plan de continuidad del negocio, los equipos de seguridad permiten que cada cual haga su trabajo, incluso cuando ocurre una filtración de datos. Ser conscientes de la seguridad también puede reducir gastos vinculados a los riesgos, como la recuperación de datos o el tiempo de inactividad, y evitar posibles multas. La última ventaja de la que hablaremos es mantener la confianza en la marca. Si se comprometen los servicios o los datos de sus clientes, puede disminuir la confianza en la empresa, dañar la marca y el negocio. Si sus clientes pierden la confianza, implica menos ingresos para el negocio. Repasemos ahora algunos roles comunes basados en la seguridad. Después de completar esta certificación, estos son los posibles puestos que quizás desees buscar: Especialista o analista de seguridad, especialista o analista de ciberseguridad, analista del centro de operaciones de seguridad o SOC y analista de seguridad de la información. También conocerás las responsabilidades asociadas a algunos de estos puestos de trabajo, más adelante. Como te habrás dado cuenta, el campo de la seguridad incluye muchos temas y conceptos y cada actividad que completes en este programa es un paso más hacia un nuevo empleo. ¡Sigamos aprendiendo!

1.1. Responsabilidades de un analista de ciberseguridad nivel inicial.

La tecnología cambia rápidamente, al igual que las tácticas y técnicas que se usan en los ataques. Al tiempo que la infraestructura evoluciona, la ciberseguridad debe desarrollar continuamente sus habilidades para proteger y asegurar la información sensible. En este video, abordaremos algunas responsabilidades de un/a analista de seguridad principiante. Veamos, ¿qué hace un/a analista de seguridad? Un/a analista de seguridad se encarga de monitorear y proteger los sistemas y la información. Hablemos ahora de las tres responsabilidades principales que tiene. Empecemos por la protección de computadoras y sistemas de red. Para proteger las computadoras y los sistemas de red, un/a analista debe monitorear la red interna de una organización. Si detecta una amenaza, debe ser el primero en responder. Las y los analistas suelen participar en ejercicios para buscar puntos débiles en los sistemas de una organización. Por ejemplo, pueden contribuir en pruebas de penetración o hacking ético. El objetivo es penetrar o hackear la red interna de su propia organización para identificar vulnerabilidades y sugerir formas de reforzar la seguridad. Piénsalo así. Después de cerrar el auto, revisas las manijas de las puertas para asegurarte que nadie acceda a los objetos que guardas adentro. Las y los analistas de seguridad trabajan proactivamente para evitar que se produzcan amenazas. Una forma de hacerlo es colaborar con el departamento de TI, instalando software de prevención para identificar riesgos y vulnerabilidades. También pueden participar en el desarrollo de software y hardware, y trabajar con los equipos de desarrollo para respaldar la seguridad del producto implementando sistemas y procesos para proteger los datos. Por último, la realización periódica de auditorías de seguridad. Una auditoría de seguridad comprueba los registros, actividades y otros documentos de seguridad de una organización. Por ejemplo, un/a analista puede examinar problemas internamente, para garantizar que la información sensible, como las contraseñas, no esté disponible para todo el personal. Bien, hemos hablado de muchas cosas. Espero que te hayas hecho una idea de lo que hacen un/a analista de seguridad principiante. Las y los analistas de seguridad son una parte importante de cualquier organización. Sus tareas protegen a las pequeñas y grandes empresas, ONGs y agencias gubernamentales. También ayudan a mantener a salvo a la gente que trabaja para esas organizaciones.

1.2. Lectura: terminología común de ciberseguridad.

Términos y conceptos clave en ciberseguridad.

Hay muchos términos y conceptos que son importantes para los/las profesionales de la ciberseguridad y conocerlos puede ayudarte a identificar mejor las amenazas que pueden perjudicar tanto a las organizaciones como a las personas. Un/a analista de seguridad o de ciberseguridad se centra en monitorear las redes en busca de infracciones. También ayuda a desarrollar estrategias para proteger una organización e investiga las tendencias de seguridad de las tecnologías de la información (TI) para mantenerse alerta y al día sobre posibles

amenazas. Además, trabaja en la prevención de incidentes. Para realizar este tipo de tareas, necesitarás desarrollar tus conocimientos sobre los siguientes conceptos clave.

- **Cumplimiento normativo (compliance) :** es el proceso de adhesión a normas internas y reglamentos externos que permite a las organizaciones evitar multas, auditorías y fallos de seguridad.

- **Marcos de seguridad:** son las directrices que se utilizan para elaborar planes de seguridad que ayuden a mitigar los riesgos y las amenazas a los datos y la privacidad.

- **Controles de seguridad:** son medidas diseñadas para reducir riesgos de seguridad específicos. Se utilizan junto a los marcos de seguridad para establecer una postura de seguridad sólida.

- **Postura de seguridad**: es la capacidad de una organización para administrar su defensa de activos y datos críticos y reaccionar ante los cambios. Una fuerte postura de seguridad conduce a un menor riesgo para la organización.

- **Agente de amenazas, o atacante malicioso**: es cualquier persona o grupo que representa un riesgo para la seguridad, que puede afectar a computadoras, aplicaciones, redes o datos.

- **Amenaza interna**: es un riesgo a la seguridad producido por una persona que pertenece o perteneció a una empresa o tiene una relación directa o de confianza con ella. Por ejemplo, si un/a empleado/a hace clic accidentalmente en un enlace de correo electrónico malicioso, o si el agente de amenazas interno realiza intencionadamente una actividad de riesgo, como acceder a los datos sin autorización.

- **Seguridad de la red**: es un conjunto de prácticas que buscan evitar accesos no autorizados a la infraestructura de red de una organización. Esto incluye datos, servicios, sistemas y dispositivos que se almacenan en la red de una organización.

- **Seguridad en la nube**: es el proceso de garantizar que los activos almacenados en la nube estén configurados o establecidos correctamente, y su acceso limitado a los/as usuarios/as autorizados/as. La nube es una red formada por un conjunto de servidores o computadoras que almacenan recursos y datos en ubicaciones físicas remotas conocidas como centros de datos a los que se puede acceder a través de Internet. La seguridad en la nube es un subcampo creciente de la ciberseguridad que se centra específicamente en la protección de este tipo de datos, aplicaciones e infraestructuras.

- **Programación**: es el proceso que permite crear un conjunto específico de instrucciones para que una computadora ejecute tareas. Estas pueden incluir:

- Automatización de tareas repetitivas (por ejemplo, buscar dominios maliciosos en una lista).

- Revisión del tráfico web.

- Alerta de actividades sospechosas.

- Conclusiones clave

1.3. Cuestionario practico: pon aprueba tus conocimientos: introducción a la ciberseguridad.

1. ¿Cuáles son los tres elementos clave de la tríada CIA? 1 punto

- ◯ Normas de cumplimiento, instrucciones y acceso
- ◯ Confianza de los clientes, aumento de los ingresos y progreso
- ◯ Continuidad, invulnerabilidad y consecución de los objetivos de negocio
- ◯ Confidencialidad, integridad y disponibilidad de la información

2. ¿Cuáles son las principales responsabilidades de un/a analista de seguridad de nivel inicial? Selecciona tres respuestas. 1 punto

- ☐ Buscar debilidades
- ☐ Crear leyes de cumplimiento
- ☐ Monitorear los sistemas
- ☐ Proteger la información

3. Completa el espacio en blanco: Realizar _____ permite a las y los profesionales de la ciberseguridad revisar los registros, actividades y documentos relacionados con la seguridad de una organización. 1 punto

- ◯ desarrollos de software
- ◯ hacking ético
- ◯ auditorías de seguridad
- ◯ pruebas de penetración

4. ¿De qué manera los equipos de seguridad aportan valor a una organización? Selecciona dos respuestas. 1 punto

- ☐ Protección contra amenazas externas e internas
- ☐ Reducción de la productividad empresarial
- ☐ Lograr el cumplimiento de la normativa
- ☐ Incremento de los gastos operativos

2. Competencias básicas para profesionales de ciberseguridad para profesionales en ciber seguridad.

2.1. Video: habilidades básicas para profesionales de ciberseguridad.

En cualquier trabajo, necesitas ciertas habilidades para tener éxito, y muchas de estas son transferibles de un puesto al siguiente. No importa en qué trabajas actualmente, es probable que ya poseas muchas de ellas. Tener una trayectoria diversa mejora tus habilidades básicas, es decir, tus

perspectivas y tu experiencia personal son muy valiosas. En este video, hablaremos de las habilidades técnicas y transferibles que son muy útiles para un/a analista de seguridad. Las habilidades transferibles proceden de otras áreas y se pueden aplicar a otras profesiones, al igual que las habilidades técnicas, pero sin requerir conocimientos de herramientas, políticas y procedimientos específicos. Hablemos de las principales habilidades transferibles que tal vez ya tengas y te ayudarán como analista de seguridad. La comunicación es una habilidad transferible para un/a analista de seguridad. Con frecuencia tendrás que describir amenazas, riesgos o vulnerabilidades a personas que pueden no tener conocimientos técnicos. Por ejemplo, puedes tener que interpretar y comunicar directivas y procedimientos a otras personas. O deberás reportar tus hallazgos a tus supervisores/as, con el fin de adoptar las medidas apropiadas para proteger la organización. Otra habilidad transferible es la colaboración. Un/a analista de seguridad suele colaborar con ingenieros/as, investigadores/as forenses digitales y gerentes de programas. Por ejemplo, si estás trabajando para lanzar una nueva función de seguridad, es probable que tengas un/a gerente de proyecto, un/a ingeniero/a y un/a hacker ético en tu equipo. Un/a analista de seguridad también debe ser capaz de analizar escenarios complejos. Por ejemplo, puede necesitar hacer recomendaciones sobre cómo las distintas herramientas pueden mejorar la eficiencia y salvaguardar la red interna. La última habilidad transferible es la resolución de problemas. Detectar un problema de seguridad, diagnosticarlo y brindar soluciones es una habilidad necesaria para mantener seguras las operaciones. Entender los agentes de amenazas e identificar tendencias brinda información para manejar futuros ataques. Bien, ahora que cubrimos las principales habilidades transferibles, hablemos sobre las habilidades técnicas que debes desarrollar como analista de seguridad. Poseer conocimientos básicos en lenguajes de programación es importante, ya que puedes tener que programar para automatizar tareas e identificar mensajes de error. Al igual que al aprender un idioma, un lenguaje de programación puede parecer complicado al principio. Sin embargo, en este programa se supone que no tienes experiencia en programación, así que empezaremos desde cero y te brindaré varios ejercicios para que practiques con lenguajes como Python y SQL.

Otra habilidad técnica importante es saber cómo usar herramientas de gestión de eventos e información de seguridad (SIEM). Un/a profesional de la seguridad usa las herramientas SIEM para identificar y analizar amenazas de seguridad, riesgos y vulnerabilidades. Por ejemplo, una herramienta SIEM puede avisarte que una persona desconocida accedió al sistema. En ese caso, puedes usar la informática forense para investigar el incidente. Hablemos ahora de la informática forense. Al igual que la investigación y la ciencia forense del sistema penal, la investigación forense digital trata de identificar, analizar y preservar las pruebas delictivas dentro de las redes, computadoras y dispositivos electrónicos. Ten en cuenta que es posible que ya poseas algunas de estas habilidades básicas. Y si no tienes las técnicas, no pasa nada. Este programa está diseñado para ayudarte a adquirir esas habilidades. Por ejemplo, en los siete años en los que trabajé en ciberseguridad, descubrí que debemos tener curiosidad intelectual y motivación para seguir aprendiendo y tener éxito. Personalmente, dedico tiempo de forma periódica para profundizar en Python y SQL, con el fin de satisfacer las demandas de los proyectos en los que trabajo. Podrás aprender Python y SQL más adelante. A lo largo del programa, adquirirás los conocimientos y habilidades necesarias para trabajar en ciberseguridad.

Otra habilidad técnica importante es saber cómo usar herramientas de gestión de eventos e información de seguridad (SIEM). Un/a profesional de la seguridad usa las herramientas SIEM para identificar y analizar amenazas de seguridad, riesgos y vulnerabilidades. Por ejemplo, una herramienta

SIEM puede avisarte que una persona desconocida accedió al sistema. En ese caso, puedes usar la informática forense para investigar el incidente. Hablemos ahora de la informática forense. Al igual que la investigación y la ciencia forense del sistema penal, la investigación forense digital trata de identificar, analizar y preservar las pruebas delictivas dentro de las redes, computadoras y dispositivos electrónicos. Ten en cuenta que es posible que ya poseas algunas de estas habilidades básicas. Y si no tienes las técnicas, no pasa nada. Este programa está diseñado para ayudarte a adquirir esas habilidades. Por ejemplo, en los siete años en los que trabajé en ciberseguridad, descubrí que debemos tener curiosidad intelectual y motivación para seguir aprendiendo y tener éxito. Personalmente, dedico tiempo de forma periódica para profundizar en Python y SQL, con el fin de satisfacer las demandas de los proyectos en los que trabajo. Podrás aprender Python y SQL más adelante. A lo largo del programa, adquirirás los conocimientos y habilidades necesarias para trabajar en ciberseguridad. Nota previamente guardada: En cualquier trabajo, necesitas ciertas habilidades para tener éxito, y muchas de estas son transferibles de un puesto al siguiente. No importa en qué trabajas actualmente, es probable que ya poseas muchas de ellas. Tener una trayectoria diversa mejora tus habilidades básicas, es decir, tus perspectivas y tu experiencia personal son muy valiosas. En este video, hablaremos de las habilidades técnicas y transferibles que son muy útiles para un/a analista de seguridad. Las habilidades transferibles proceden de otras áreas y se pueden aplicar a otras profesiones, al igual que las habilidades técnicas, pero sin requerir conocimientos de herramientas, políticas y procedimientos específicos. Hablemos de las principales habilidades transferibles que tal vez ya tengas y te ayudarán como analista de seguridad. La comunicación es una habilidad transferible para un/a analista de seguridad. Con frecuencia tendrás que describir amenazas, riesgos o vulnerabilidades a personas que pueden no tener conocimientos técnicos. Por ejemplo, puedes tener que interpretar y comunicar directivas y procedimientos a otras personas. O deberás reportar tus hallazgos a tus supervisores/as, con el fin de adoptar las medidas apropiadas para proteger la organización. Otra habilidad transferible es la colaboración. Un/a analista de seguridad suele colaborar con ingenieros/as, investigadores/as forenses digitales y gerentes de programas. Por ejemplo, si estás trabajando para lanzar una nueva función de seguridad, es probable que tengas un/a gerente de proyecto, un/a ingeniero/a y un/a hacker ético en tu equipo. Un/a analista de seguridad también debe ser capaz de analizar escenarios complejos. Por ejemplo, puede necesitar hacer recomendaciones sobre cómo las distintas herramientas pueden mejorar la eficiencia y salvaguardar la red interna. La última habilidad transferible es la resolución de problemas. Detectar un problema de seguridad, diagnosticarlo y brindar soluciones es una habilidad necesaria para mantener seguras las operaciones. Entender los agentes de amenazas e identificar tendencias brinda información para manejar futuros ataques. Bien, ahora que cubrimos las principales habilidades transferibles, hablemos sobre las habilidades técnicas que debes desarrollar como analista de seguridad. Poseer conocimientos básicos en lenguajes de programación es importante, ya que puedes tener que programar para automatizar tareas e identificar mensajes de error. Al igual que al aprender un idioma, un lenguaje de programación puede parecer complicado al principio. Sin embargo, en este programa se supone que no tienes experiencia en programación, así que empezaremos desde cero y te brindaré varios ejercicios para que practiques con lenguajes como Python y SQL.

2.2. Lectura: habilidades transferibles y técnicas en ciberseguridad.

Anteriormente, aprendiste que las y los analistas en ciberseguridad necesitan desarrollar ciertas habilidades básicas para tener éxito en el ejercicio de su profesión. Las habilidades transferibles son

competencias de otras áreas de estudio o práctica que pueden aplicarse a diferentes carreras. Las habilidades técnicas también pueden aplicarse a varias profesiones; sin embargo, normalmente requieren el conocimiento de herramientas, procedimientos y políticas específicas. En esta lección profundizarás tanto en las habilidades transferibles como en las técnicas.

Habilidades transferibles.
Probablemente hayas desarrollado habilidades transferibles a lo largo de tu vida; algunas de ellas te ayudarán a prosperar como profesional en ciberseguridad. Por ejemplo:

- **Comunicación**: como analista de ciberseguridad, deberás comunicarte y colaborar con otras personas. Comprender las preguntas o inquietudes de los/las demás y comunicar la información con claridad a personas con conocimientos técnicos y no técnicos te ayudará a mitigar los problemas de seguridad rápidamente.

- **Resolución de problemas:** una de tus principales tareas como analista de ciberseguridad será identificar y resolver problemas de forma proactiva. Puedes hacerlo reconociendo patrones de ataque y determinando la solución más eficaz para minimizar el riesgo. No tengas miedo de probar cosas nuevas y ten en cuenta que es difícil encontrar una solución perfecta a un problema, y es probable que te tengas que conformar con un punto intermedio.

- **Gestión del tiempo:** tener sentido de la urgencia y priorizar adecuadamente las tareas es esencial en el campo de la ciberseguridad. Por lo tanto, una gestión eficaz del tiempo te ayudará a minimizar los posibles daños y riesgos para los activos y datos críticos. Además, será importante que sepas priorizar las tareas y enfocarte en el tema más urgente.

- **Mentalidad de crecimiento:** la ciberseguridad es un sector en plena evolución, por lo que una habilidad transferible importante es la voluntad de aprender. La tecnología avanza rápido, ¡y eso es positivo! Esto no significa que tengas que aprender todo, pero sí que tendrás que seguir haciéndolo a lo largo de tu carrera. Afortunadamente, podrás aplicar gran parte de lo que aprendas en este programa a tu desarrollo profesional continuado.

- **Diversidad de perspectivas:** la única manera de llegar lejos es trabajando conjuntamente con otras personas. El respeto mutuo y los diversos puntos de vista te permitirán encontrar mejores soluciones a los problemas de seguridad.

Habilidades técnicas
Hay muchos conocimientos técnicos que te ayudarán a tener éxito en el campo de la ciberseguridad. Aprenderás y practicarás estas habilidades a medida que avances en el programa de certificación. Estos son algunos conceptos y herramientas que tendrás que entender y utilizar:

Lenguajes de programación: comprender cómo usar los lenguajes de programación te permitirá automatizar tareas que de otro modo requerirían mucho tiempo, como, por ejemplo, la búsqueda de datos para identificar posibles amenazas o la organización y el análisis de información para identificar patrones relacionados con problemas de seguridad.

- **Sistemas de detección de intrusiones (IDS):** las y los analistas en ciberseguridad utilizan los IDS para monitorear la actividad del sistema y las alertas de posibles intrusiones. Es

importante familiarizarse con ellos porque son una herramienta clave para proteger activos y datos. Por ejemplo, puedes usar un IDS para monitorear las redes en busca de signos de actividad maliciosa, como el acceso no autorizado a una red.

- **Conocimiento del panorama de amenazas:** es vital estar al tanto de las tendencias actuales relacionadas con los agentes de amenazas, el malware o las metodologías. Este conocimiento permite a los equipos de ciberseguridad construir defensas más sólidas contra las tácticas y técnicas de los agentes de amenazas. Si te mantienes al día sobre las tendencias y patrones de ataque, serás capaz de reconocer cuando surgen nuevos tipos de amenazas, como, por ejemplo, una nueva variante de ransomware.

- **Respuesta a incidentes**: las y los analistas en ciberseguridad deben poder seguir las políticas y procedimientos establecidos para responder adecuadamente a los incidentes. Por ejemplo, poder iniciar el proceso de respuesta a incidentes ante un posible ataque de malware lo que podría implicar tener que llevar a cabo una investigación para identificar el problema de raíz y establecer formas de remediarlo.

2.3. Video: la importancia de la ciberseguridad.

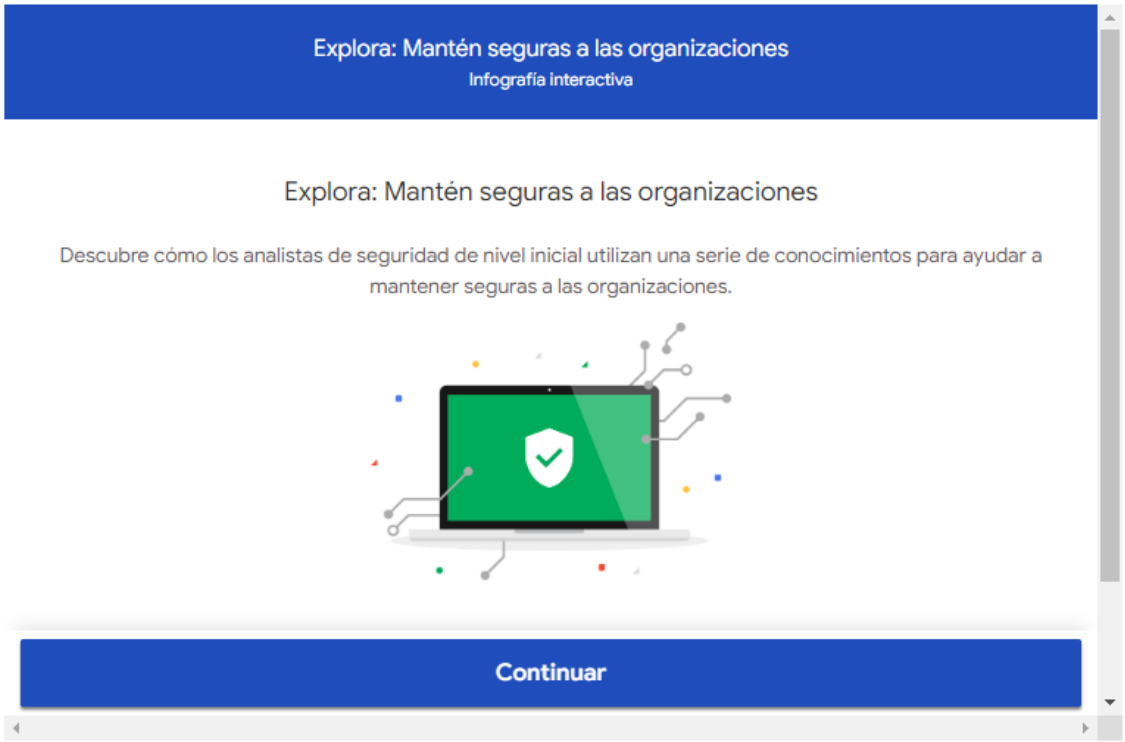
Como mencionamos, las y los profesionales de la seguridad protegen muchos activos físicos y digitales. Estas habilidades son buscadas por las organizaciones y entidades gubernamentales, porque deben gestionar riesgos. Hablemos de por qué es tan importante la ciberseguridad. Es esencial para garantizar la continuidad del negocio y el estatus ético de una organización. Hay implicaciones legales y morales para mantener la seguridad de una organización. Una filtración de datos, por ejemplo, afecta a toda la gente asociada a la organización. Esto se debe a que las pérdidas o fugas de datos pueden dañar la reputación de una organización, así como la vida y reputación de sus clientes. Con medidas de seguridad sólidas, las organizaciones aumentan la confianza de las personas, lo que permite que crezcan sus finanzas y su reputación. Como mencionamos, las organizaciones no son las únicas que sufren por una filtración de datos. Proteger los datos de usuarios/as, clientes y proveedores es una parte importante para prevenir incidentes que puedan exponer información de identificación personal. La información de identificación personal, o PII, es cualquier información de la que se pueda deducir la identidad de una persona. PII incluye el nombre, fecha de nacimiento, dirección física, número de teléfono, dirección de correo electrónico, protocolo de Internet, o dirección IP e información similar de una persona. La información de identificación personal sensible, o SPII, es un tipo específico de PII que se rige por pautas de manejo más estrictas y puede incluir números de seguridad social, datos médicos, financieros y biométricos, como el reconocimiento facial. El robo de datos SPII es potencialmente mucho más perjudicial para una persona que el robo de datos PII.

Los datos PII y SPII son activos clave que buscará un agente de amenazas si una organización sufre una filtración. Si la información de identificación personal se pone en riesgo, se filtra o se roba, la suplantación de la identidad es la principal preocupación. La suplantación de la identidad consiste en robar datos personales para cometer fraude haciéndose pasar por la víctima. Su objetivo principal es el beneficio económico. Vimos varias razones por las que la seguridad es importante. Las empresas necesitan analistas de seguridad como tú para cubrir la demanda actual y futura para proteger los datos, productos y personas, garantizando al mismo tiempo la confidencialidad, integridad y el acceso seguro a la información. Por esto, la Oficina de Estadísticas

Laborales de EE. UU. espera que la demanda de profesionales de la seguridad aumente más del 30% para 2030.

2.4. Complemento no calificado: Exploración: Mantener la seguridad de las organizaciones.

Exploración: mantener la seguridad de las organizaciones



Se evidencian varios tips sobre cómo mantener la seguridad en las organizaciones.

2.5. Cuadro de aviso de la discusión: El valor de la ciberseguridad.

El valor de la ciberseguridad

Ahora que ya sabes qué es la ciberseguridad y cómo las y los profesionales en este campo protegen a las personas y las organizaciones, es el momento de considerar tu propio rol en ciberseguridad. Imagina que es tu primer día como profesional y piensa en lo siguiente:

- ¿Qué problemas de ciberseguridad estás resolviendo?
- ¿Cómo proteges a tu organización?
- ¿Cómo proteges a las personas?
- ¿Qué es lo más emocionante de tu día?

2.6. Cuestionario practico: Pon aprueba tus conocimientos: Habilidades básicas para profesionales de la ciberseguridad.

1. ¿Cuáles de las siguientes competencias son habilidades transferibles y pueden aplicarse en casi cualquier campo? Selecciona todas las opciones que correspondan. **1 punto**

- [ ] Comunicación escrita y oral
- [ ] Resolución de problemas
- [ ] Análisis
- [ ] Programación

2. ¿Cuáles de las siguientes competencias son habilidades técnicas necesarias para convertirse en analista de ciberseguridad de nivel inicial? Selecciona todas las opciones que correspondan. **1 punto**

- [ ] Redacción de reglamentos
- [ ] Análisis de datos
- [ ] Desarrollo de software
- [ ] Programación

3. Completa el espacio en blanco: _____ identifican, analizan y preservan pruebas delictivas en redes, computadoras y dispositivos electrónicos. **1 punto**

- ◯ Las y los profesionales de la inteligencia empresarial
- ◯ Las y los hackers éticos
- ◯ Las y los analistas de centros de operaciones de seguridad
- ◯ Los/las investigadores/as forenses digitales

4. ¿Qué ejemplos de información personal identificable sensible (SPII) deben proteger las y los profesionales de la ciberseguridad? Selecciona dos respuestas. **1 punto**

- [ ] Apellidos
- [ ] Números de cuentas bancarias
- [ ] Direcciones de correo electrónico
- [ ] Registros médicos

3. Revisión: introducción al apasionante mundo de la ciberseguridad.

3.1. Video: conclusión.

Felicitaciones por completar la primera sección de este curso. Rapásemos rápidamente lo que vimos hasta ahora, antes de seguir. Definimos la ciberseguridad y presentamos las ventajas de implementar la seguridad en una organización. Luego hablamos sobre responsabilidades laborales, como gestión de amenazas e instalación de software preventivo.

Presentamos algunas habilidades básicas importantes, como la colaboración y la informática forense. Terminamos hablando del valor de la seguridad y cómo respalda funciones empresariales cruciales. Espero que hayas comprendido mejor la ciberseguridad. Si crees que necesitas repasar antes de seguir, puedes retroceder y revisar cualquier contenido. Al aprender lo básico, estás sentando los cimientos de tu carrera en ciberseguridad. Próximamente, veremos algunos ataques que modelaron el sector de la seguridad.

3.2. Lectura: Términos del glosario de la semana1.

Términos y definiciones del curso 1, semana 1:

- **Agente de amenaza:** Persona o grupo de personas que representa una amenaza intencional para computadoras, aplicaciones o redes.

- **Amenaza:** Cualquier circunstancia o evento que pueda afectar los activos de manera negativa.

- **Amenaza interna:** Riesgo a la seguridad producido por una persona que pertenece o perteneció a una empresa o tiene una relación directa o de confianza con ella.

- **Ciberseguridad (o seguridad cibernética):** Práctica de garantizar la confidencialidad, integridad y disponibilidad de la información mediante la protección de redes, dispositivos, personas y datos contra el acceso no autorizado o la explotación delictiva.

- **Habilidades técnicas:** Competencias que requieren conocimiento de herramientas, procedimientos y políticas específicas**.**

- **Habilidades transferibles**: Competencias de otras áreas que pueden aplicarse a diferentes carreras.

- **Información de identificación personal (PII por sus siglas en inglés):** Cualquier información que pueda usarse para deducir la identidad de una persona.

- **Información de identificación personal sensible (SPII por sus siglas en inglés):** Tipo específico de Información de identificación personal que se rige por pautas de manejo más estrictas**.**

- **Seguridad de redes:** Práctica de evitar accesos no autorizados a la infraestructura de red de una organización**.**