Módulo 3.

FUNDAMENTOS DE LA CIBERSEGURIDAD.

Oficina Asesora de Informática | Digitalízate Comunidad

Contenido.

1.Video: Introducción a la semana 3.

1.1 Introducción a los marcos y controles de seguridad.

Imagina que trabajas como analista de seguridad y recibes alertas de actividad sospechosa en la red. Descubres que deberás implementar más medidas para evitar incidentes graves. Pero ¿por dónde empiezas? Como analista, primero debes identificar los activos y riesgos cruciales. Luego implementarás los marcos y controles necesarios. En este curso, veremos cómo las/los profesionales

de seguridad usan marcos para identificar y gestionar el riesgo. También veremos cómo usar controles de seguridad para gestionar o reducir riesgos. Los marcos de seguridad son pautas usadas en la creación de planes para mitigar riesgos y amenazas a los datos y la privacidad. Ofrecen un enfoque estructurado para implementar un ciclo de seguridad. El ciclo de seguridad lo conforman políticas y normas en evolución que definen cómo la organización gestiona los riesgos, sigue las políticas establecidas y cumple con normas o leyes.

Hay varios marcos de seguridad que pueden usarse para manejar riesgos empresariales y cumplimiento normativo. Entre sus fines están proteger la información de identificación personal, abreviada como PII, proteger la información financiera, identificar debilidades de seguridad, manejar riesgos organizacionales y alinear los objetivos de seguridad con los de la empresa. Los marcos tienen cuatro componentes principales. Al conocerlos manejarás mejor los riesgos potenciales. El primer componente principal es identificar y documentar los objetivos de seguridad. Por ejemplo, una organización tiene el objetivo de alinearse con el Reglamento General de Protección de Datos de la UE, también conocido como RGPD. El RGPD es una ley de protección de datos creada para dar a los ciudadanos europeos más control sobre sus datos personales.

Se puede pedir a un/a analista de ciberseguridad identificar y documentar áreas de incumplimiento con el RGPD. El segundo componente es crear pautas para alcanzar los objetivos de ciberseguridad. Por ejemplo, al implementar políticas para cumplir con el RGPD, puede que la organización deba crear nuevas políticas sobre cómo manejar solicitudes de datos de usuarios/as individuales. El tercer componente es implementar procesos de seguridad fuertes. En el caso del RGPD, un/a analista que trabaja para una empresa de redes sociales puede diseñar procedimientos para cumplir con las solicitudes de datos de sus usuarios/as. Un ejemplo de estas solicitudes es cuando una persona intenta actualizar o eliminar su información de perfil. El último componente de los marcos de seguridad es monitorear y comunicar los resultados. Por ejemplo, puedes monitorear la red interna de la organización y reportar a tu superior o responsable de cumplimiento un problema de seguridad potencial que afecta el RGPD.

Los controles de seguridad son medidas que reducen ciertos riesgos de seguridad. Por ejemplo, puede haber una directiva de que los colaboradores deben hacer una capacitación de privacidad para evitar la filtración de datos. Como analista, puedes usar una herramienta de software para asignar de forma automática y ver quiénes realizan la capacitación. Los marcos y los controles son vitales para gestionar la seguridad de toda organización y garantizar que todas las personas colaboren para mantener un nivel de riesgo bajo. Al entender su propósito y cómo se usan, las/los analistas contribuyen al logro de los objetivos de seguridad y protegen a los/las usuarios/as. En los siguientes videos, veremos marcos

y principios que las/los analistas deben conocer para minimizar el riesgo y proteger los datos y a los/las usuarios/as.

1.2. Video: Diseño seguro.

Aquí aprenderás sobre marcos y controles específicos que las organizaciones usan voluntariamente para minimizar riesgos contra sus datos y proteger a sus usuarios/as. ¡Empecemos! La tríada CID es una guía fundamental que informa cómo las organizaciones evalúan el riesgo y crean sistemas y políticas de seguridad. CID es el acrónimo de confidencialidad, integridad y disponibilidad. La confidencialidad implica que solo las personas autorizadas pueden acceder a activos o datos específicos. Por ejemplo, deben implementarse controles de acceso estrictos que definan quién puede acceder a los datos y quién no a fin de proteger la información confidencial. La integridad implica que los datos son correctos, auténticos y confiables. Para la integridad, las/los profesionales usan protección de datos como el cifrado para impedir que se altere la información. La disponibilidad implica que quien tiene autorización tenga acceso a los datos. Por ejemplo, un director puede tener más acceso a ciertos datos que un gerente, pues el director suele supervisar a más colaboradores. Definamos un término que vimos al hablar de la tríada CID: activo. Un activo es un elemento percibido como valor para una organización. El valor lo determina el costo del activo en cuestión. Por ejemplo, una app que almacena datos confidenciales, como números de seguridad social o cuentas bancarias, es un activo valioso. Conlleva más riesgo, por lo que requiere controles más estrictos en comparación con un sitio que comparte noticias públicas. Como recordarás, antes vimos los marcos y controles en general. Ahora veremos un marco creado por el Instituto Nacional de Estándares y Tecnología de EE.UU., el Marco de Ciberseguridad, conocido como el CSF, del NIST. El CSF del NIST es un marco de adhesión voluntaria que consiste en estándares, pautas y prácticas recomendadas para manejar riesgos de ciberseguridad. Es importante conocer este marco, pues los equipos de seguridad lo usan como base para gestionar el riesgo a corto y largo plazo. Gestionar y minimizar riesgos, y proteger activos contra agentes de amenazas son objetivos clave del trabajo de seguridad. Es importante entender los motivos de un agente de amenazas e identificar los activos más valiosos de la organización.

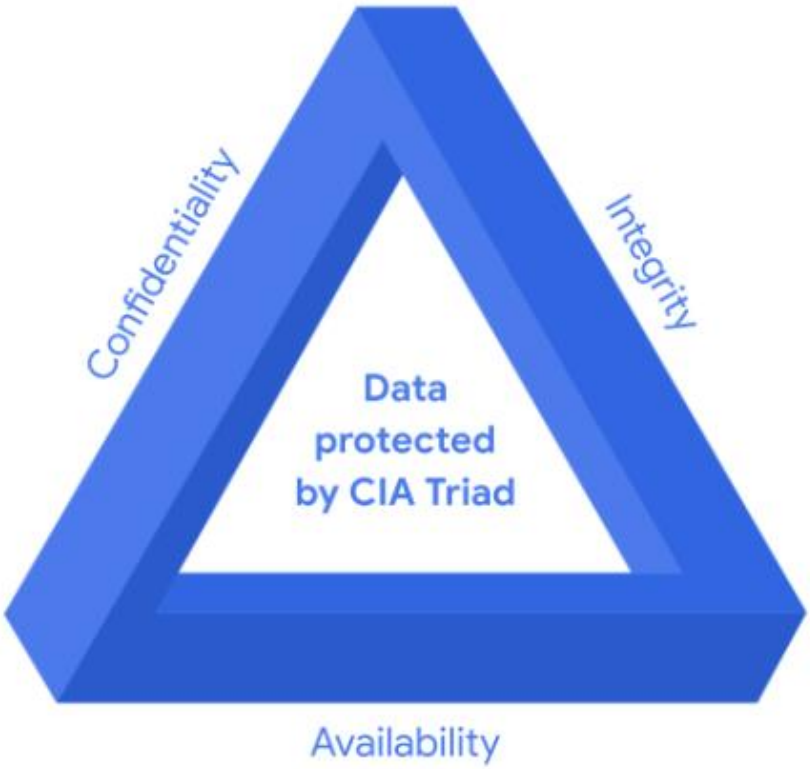
Entre las mayores amenazas están los empleados descontentos. Son los más peligrosos porque suelen tener acceso a información delicada y saben dónde hallarla. Para reducir este riesgo, las/los

profesionales usan el principio de disponibilidad y pautas organizacionales basadas en marcos para que los/las empleados/as solo accedan a datos que necesitan para su trabajo. Hay agentes de amenazas en todo el mundo. Los equipos de seguridad diversos ayudan a las organizaciones a identificar las intenciones de los atacantes. Tener varias perspectivas ayuda a las organizaciones a entender y reducir el impacto de la actividad maliciosa. Con esto concluimos la introducción a la tríada CID y el marco de Ciberseguridad del NIST, que se usa para crear procesos y proteger a las organizaciones y a sus usuarios/as. Te pueden preguntar si conoces los marcos y principios de la seguridad. O te pueden pedir explicar cómo se usan para proteger activos organizacionales. En ambos casos, en este programa habrá varias oportunidades de aprender más al respecto y aplicar los conocimientos a situaciones reales. A continuación, veremos la ética de la seguridad.

1.3. Lectura: Controles, marcos y cumplimiento.

Anteriormente, conociste los marcos de seguridad y cómo estos proporcionan un enfoque estructurado para implementar un ciclo de vida de seguridad. Como recordatorio, el ciclo de vida de seguridad consiste en un conjunto de políticas y estándares en constante evolución. En esta lectura, profundizarás en cómo se utilizan los marcos de seguridad, los controles y las regulaciones de cumplimiento, o leyes, de manera conjunta para gestionar la seguridad y garantizar que cada cual cumpla su parte para minimizar el riesgo.

Cómo se relacionan los controles, los marcos y el cumplimiento
La tríada de confidencialidad, integridad y disponibilidad (CID) es una guía que ayuda a las organizaciones a evaluar los riesgos y a establecer sistemas y políticas de seguridad.



La tríada de CID son los tres principios fundamentales utilizados por las/los profesionales de la ciberseguridad para establecer controles adecuados que mitiguen amenazas, riesgos y vulnerabilidades.

Como recordarás, los controles de seguridad son medidas diseñadas para reducir riesgos específicos de seguridad. Por lo tanto, se utilizan junto con marcos para asegurar que los objetivos y procesos de seguridad se implementen correctamente y que las organizaciones cumplan con los requisitos regulatorios.

En tanto, los marcos de seguridad son pautas utilizadas para elaborar planes que ayuden a mitigar riesgos y amenazas a los datos y la privacidad. Tienen cuatro componentes principales:

I. Identificación y documentación de objetivos de seguridad.

II. Establecimiento de pautas para lograr los objetivos de seguridad.

III. Implementación de procesos de seguridad sólidos.

IV. Supervisión y comunicación de resultados.

Finalmente, el cumplimiento normativo, o compliance, es el proceso de adhesión a reglamentos internos y regulaciones externas.

Controles específicos, marcos y cumplimiento.

El Instituto Nacional de Estándares y Tecnología (NIST) es una agencia con sede en los Estados Unidos que desarrolla varios marcos de cumplimiento voluntario que las organizaciones de todo el mundo pueden utilizar para ayudar a gestionar el riesgo. Cuanto más alineada al cumplimiento esté una organización, menor será el riesgo.

Entre los ejemplos de marcos que se presentaron anteriormente se encuentran el Marco de Ciberseguridad del Instituto Nacional de Estándares y Tecnología (NIST) y el Marco de Gestión de Riesgos (RMF) del NIST.

Ten en cuenta que las especificaciones y pautas pueden variar según el tipo de organización para la que trabajes.

Además del Marco de Ciberseguridad del NIST y el Marco de Gestión de Riesgos (RMF) del NIST , existen varios otros controles, marcos y normas de cumplimiento con los que es importante que las/los profesionales de seguridad se familiaricen, para contribuir a mantener seguras a las organizaciones y a las personas a las que brindan servicio.

La Comisión Federal de Regulación de Energía - Corporación de Confiabilidad Eléctrica América del Norte (FERC-NERC)

La FERC-NERC es una regulación que se aplica a las organizaciones que trabajan con electricidad o que están involucradas con la red eléctrica de los Estados Unidos y América del Norte. Este tipo de organizaciones tienen la obligación de prepararse, mitigar y reportar cualquier incidente de seguridad potencial que pueda afectar negativamente a la red eléctrica. También están legalmente obligadas a cumplir con los Estándares de Confiabilidad de Protección de Infraestructura Crítica (CIP) definidos por la FERC.

Programa Federal de Gestión de Riesgos y Autorizaciones (FedRAMP®)

El FedRAMP es un programa del gobierno federal de los Estados Unidos que estandariza la evaluación, autorización, monitoreo y gestión de seguridad de los servicios en la nube y las ofertas de productos. Su objetivo es proporcionar consistencia en todo el sector gubernamental y proveedores de servicios en la nube de terceros.

Centro de Seguridad en Internet (CIS®)

El CIS es una organización sin fines de lucro que se enfoca en múltiples áreas. Proporciona un conjunto de controles que pueden utilizarse para proteger sistemas y redes contra ataques. Su objetivo es ayudar a las organizaciones a establecer un mejor plan de defensa. Además, el CIS proporciona controles aplicables que las/los profesionales de seguridad pueden seguir ante un eventual incidente de seguridad.

Reglamento General de Protección de Datos (RGPD)

El RGPD es una normativa general de datos de la Unión Europea (UE) que protege el procesamiento de los datos de sus residentes y su derecho a la privacidad dentro y fuera del territorio. Por ejemplo, si una organización no es transparente en relación con los datos que posee sobre un/a ciudadano/a de la UE o la razón por la que los tiene, esto constituye una infracción que puede resultar en una multa para la organización. Además, si se produce una filtración y los datos de una persona se ven comprometidos, este debe ser informado. La organización afectada tiene 72 horas para notificarla sobre esta situación.

Estándares de seguridad de datos del sector de las tarjetas de pago (PCI DSS)

PCI DSS es un estándar de seguridad internacional destinado a garantizar que las organizaciones que almacenan aceptan, procesan y transmiten información de tarjetas de crédito lo hagan en un entorno seguro. El objetivo de esta norma es reducir el fraude con tarjetas de crédito.

Ley de Transferencia y Responsabilidad de los Seguros Médicos (HIPAA)

La HIPAA es una ley federal de los Estados Unidos establecida en 1996 para proteger la información médica de las personas. Esta ley prohíbe que la información de un/una paciente sea compartida sin su consentimiento. Se rige por tres reglas:

- Privacidad
- Seguridad
- Notificación de filtraciones

Las organizaciones que almacenan datos de pacientes tienen la obligación legal de informarles en caso de que ocurra una violación de seguridad, ya que la exposición de la Información Médica Protegida (PHI) de las/ los pacientes puede conducir al robo de identidad y al fraude de seguros. La PHI se refiere a la información relacionada con la salud física o mental pasada, presente o futura de una persona, ya sea un plan de atención o pagos por la atención. Además de comprender la HIPAA como una ley, las/los profesionales de la seguridad también deben familiarizarse con la Alianza de Confianza de Información de Salud (HITRUST®), que es un marco de seguridad y un programa de garantía que ayuda a las instituciones a cumplir con la HIPAA.

Organización Internacional para la Normalización (ISO)

La ISO fue creada para establecer estándares internacionales relacionados con la tecnología, la fabricación y la gestión en todo el mundo. Ayuda a las organizaciones a mejorar sus procesos y procedimientos en cuanto a retención del personal, planificación, gestión de residuos y servicios.

Controles de Sistemas y Organizaciones (SOC tipo 1, SOC tipo 2)

Este estándar fue desarrollado por la junta de normas de auditoría del Instituto Americano de Contables Públicos Certificados® (AICPA). Los informes SOC1 y SOC2 se enfocan en las políticas de acceso de los/as usuarios/as de una organización en diferentes niveles, tales como:

- Asociado/a
- Supervisor/a
- Gerente/a
- Ejecutivo/a
- Proveedor/a
- Otros

Estos informes se utilizan para evaluar el cumplimiento financiero de una organización, así como los niveles de riesgo asociados. También abordan aspectos críticos como la confidencialidad, privacidad, integridad, disponibilidad, seguridad y la seguridad general de los datos. Es importante destacar que cualquier falla en el control de estos aspectos puede resultar en posibles fraudes.

Consejo profesional: Existen numerosas regulaciones que se revisan con frecuencia. Te recomendamos mantenerte al día con los cambios y explorar más marcos, controles y normas de cumplimiento. Dos sugerencias para investigar: la Ley Gramm-Leach-Bliley y la Ley Sarbanes-Oxley.

1.4. Cuestionario practico: Pon a prueba tus conocimientos: Marcos y controles.

1. Completa el espacio en blanco: Los _____ de seguridad son un conjunto de pautas utilizadas para desarrollar planes que ayuden a mitigar los riesgos y las amenazas a los datos y la privacidad. **1 punto**

   - ○ regulaciones
   - ○ controles
   - ○ marcos
   - ○ ciclos de vida

2. Una organización requiere que su personal realice un nuevo programa de capacitación sobre privacidad de datos cada año para reducir el riesgo de una violación de datos. ¿De qué ejemplo es este requisito de entrenamiento? **1 punto**

   - ○ Control de seguridad
   - ○ Confidencialidad de los datos
   - ○ Marco de Ciberseguridad del Instituto Nacional de Estándares y Tecnología (NIST)
   - ○ Información de identificación personal (PII)

3. ¿Cuál es una guía que ayuda a las organizaciones en la consideración del riesgo al establecer sistemas y políticas de seguridad? **1 punto**

   - ○ Reglamento General de Protección de Datos (RGPD)
   - ○ Información de identificación personal sensible (SPII)
   - ○ Tríada de confidencialidad, integridad y disponibilidad (CID)
   - ○ Marco de Ciberseguridad (CSF)

4. Los equipos de seguridad utilizan el Marco de Ciberseguridad del NIST como base para gestionar el riesgo a corto y largo plazo. **1 punto**

   - ○ Verdadero
   - ○ Falso

2. La ética de ciberseguridad.2. La ética de

ciberseguridad.

2.1. Video: La ética en la ciberseguridad.

Para la seguridad, las nuevas tecnologías traen nuevos desafíos. No siempre está claro cuál es la decisión correcta o incorrecta para cada nuevo incidente o riesgo. Por ejemplo, imagina que trabajas como analista de seguridad de nivel inicial y recibes una alerta de riesgo alto. La investigas y descubres que se transfirieron datos sin autorización.

Te esmeras para identificar quién hizo la transferencia y descubres que es un amigo del trabajo. ¿Qué haces? Éticamente, como profesional, debes ser imparcial y preservar la seguridad y confidencialidad. Aunque es normal proteger a un amigo, sin importar quién sea el usuario en cuestión, tienes la responsabilidad y obligación de seguir las políticas y protocolos que aprendiste en la capacitación. En muchos casos, los equipos de seguridad tienen más acceso a datos e información que otros colaboradores. Las/los profesionales deben respetar ese privilegio y actuar éticamente. La ética de la seguridad da pautas para tomar decisiones apropiadas como profesional. Otro ejemplo: si como analista tienes la capacidad para darte acceso a los datos de nómina y aumentarte el sueldo, ¿deberías hacerlo solo porque puedes? La respuesta es no. Nunca debes abusar del acceso que se te ha otorgado y confiado. Hablemos de los principios éticos que plantean dudas al estudiar soluciones para mitigar los riesgos. Estos son la confidencialidad, la protección de la privacidad y las leyes. Empecemos por el primero: confidencialidad. Antes vimos la confidencialidad como parte de la tríada CID. Ahora analicemos cómo aplicarla a la ética.

Como aprendiz de ciberseguridad, verás información propietaria o información privada, como PII. Tu deber ético es mantener su confidencialidad y protegerla. Por ejemplo, puedes ayudar a un colega dándole acceso informático fuera de los canales debidamente documentados. Sin embargo, esta violación ética puede tener consecuencias graves, incluyendo sanciones, la pérdida de tu reputación profesional y repercusiones legales tanto para ti como para tu colega. El segundo principio para considerar es la protección de la privacidad. Esta implica preservar los datos personales contra un uso no autorizado. Por ejemplo, tu superior te envía un correo personal fuera del horario laboral para pedir el teléfono de un colega. Te explica que no puede acceder a los datos de empleados en ese momento, pero necesita hablar urgentemente con esa persona. Como analista de ciberseguridad, debes seguir las políticas y procedimientos. En este ejemplo, indican que los datos de empleados/as se guardan en una base de datos segura que nunca se debe ver ni compartir de otra forma. Por lo tanto, acceder y compartir datos personales no sería ético. En este tipo de situación, es difícil saber que hacer. La mejor respuesta es seguir las políticas y procedimientos establecidos.

El tercer principio que veremos es la ley. Las leyes son reglas que reconoce una comunidad y que aplica una entidad gobernante. Por ejemplo, imagina un profesional de un hospital capacitado para manejar PII y SPII para cumplir con las normativas. Tiene archivos con datos confidenciales que nunca deben dejarse sin supervisión. Pero llega tarde a una reunión. En lugar de guardar los archivos en un área designada, los deja en su escritorio sin supervisión. Al regresar, los archivos no están. Esta persona infringió varias regulaciones de cumplimiento, y

sus acciones no fueron ética ni legalmente correctas, ya que su negligencia causó la pérdida de datos privados de pacientes y del hospital. En el campo de la seguridad, recuerda que la tecnología evoluciona, y también las tácticas y técnicas de los atacantes. Debido a esto, las/los profesionales deben seguir pensando críticamente cómo responder a los ataques. Tener una ética sólida guía las decisiones para seguir los procesos y procedimientos correctos a fin de mitigar los riesgos en evolución.

2.2. Lectura: Los conceptos éticos que guían las decisiones de la ciberseguridad.

Previamente, se te presentó el concepto de ética de la ciberseguridad. La ética de la ciberseguridad refiere a una serie de pautas fundamentales para tomar decisiones apropiadas como profesional de la seguridad. Ser ético/a implica mantener la imparcialidad y preservar la seguridad y confidencialidad de los datos privados. Contar con un sólido sentido de ética te ayudará a tomar decisiones acertadas como profesional de la ciberseguridad, permitiéndote mitigar las amenazas planteadas por las tácticas y técnicas en constante evolución de ataques maliciosos. En esta lectura, ampliarás tus conocimientos sobre conceptos éticos adicionales que son esenciales para tomar decisiones adecuadas sobre cómo responder legal y éticamente a los ataques, protegiendo tanto a las organizaciones como a las personas involucradas.

Preocupaciones éticas y leyes relacionadas con los contraataques.

Postura de los Estados Unidos sobre los contraataques.

En los Estados Unidos, está prohibido realizar contraataques contra agentes de amenaza debido a leyes como la Ley de Abuso y Fraude Informático de 1986 y la Ley de Intercambio de Información de Seguridad Cibernética de 2015, entre otras. En lugar de contraatacar, solo se permite la defensa. La acción de contraatacar en los Estados Unidos se considera un acto de justicia por mano propia, reservado para las fuerzas del orden. Además, los contraataques pueden llevar a una escalada de la situación y causar aún más daño. Por último, si el agente amenazante es un/a hacktivista patrocinado/a por el estado, los contraataques pueden tener serias implicaciones internacionales. Un/a hacktivista es una persona que utiliza el hackeo (hacking) o piratería informática para lograr objetivos políticos, como promover cambios sociales o desobediencia civil.

Por estas razones, solo se permite que los/las empleados/as autorizados/as por el gobierno federal y el personal militar realicen contraataques en los Estados Unidos.

Postura internacional sobre los contraataques.

La Corte Internacional de Justicia (CIJ), que actualiza regularmente sus políticas y regulaciones, establece que una persona o grupo puede contraatacar si:

- El contraataque solo afectará a la parte que atacó primero.
- El contraataque es una comunicación directa pidiendo al atacante inicial que se detenga.
- El contraataque no escala la situación.

- Los efectos del contraataque se pueden revertir.

Metodologías y principios éticos.

Dado que los contraataques generalmente son desaprobados o ilegales, en el ámbito de la ciberseguridad se han creado marcos y controles, como la tríada de confidencialidad, integridad y disponibilidad (CID) y otros discutidos anteriormente en el programa, para abordar cuestiones relacionadas con la confidencialidad, protección de la privacidad y cumplimiento de leyes. Con el fin de comprender mejor la relación entre estos aspectos y las obligaciones éticas de las/los profesionales de la ciberseguridad, es importante revisar los siguientes conceptos fundamentales sobre el uso de la ética para proteger a las organizaciones y a las personas.

La confidencialidad implica que solo los/as usuarios/as autorizados/as pueden acceder a activos o datos específicos. Desde el punto de vista ético, la confidencialidad requiere un alto nivel de respeto por la privacidad con el objetivo de proteger los activos y datos privados.

La protección de la privacidad implica preservar la información personal de un uso no autorizado. La información de identificación personal (PII) y la información de identificación personal sensible (SPII) son tipos de datos personales que pueden causar daño a las personas en caso de robo. Los datos de PII incluyen cualquier información que se puede utilizar para deducir la identidad de una persona, como su nombre y número de teléfono. Por otro lado, los datos de SPII son una categoría más restrictiva de PII y abarcan números de seguridad social y números de tarjetas de crédito. Para proteger adecuadamente los datos de PII y SPII, las/los profesionales de ciberseguridad tienen la responsabilidad ética de proteger la información privada, identificar vulnerabilidades de seguridad, gestionar los riesgos empresariales y alinear las medidas de seguridad con los objetivos del negocio.

Las leyes son normas reconocidas por una comunidad y aplicadas por una entidad gubernamental. Como profesional de la seguridad, tendrás la responsabilidad ética de proteger a tu organización, su infraestructura interna y a las personas allí involucradas. Para lograrlo debes:

- Mantener la imparcialidad y llevar a cabo tu trabajo de manera honesta, responsable y con el máximo respeto por la ley.
- Ser transparente y basar tus acciones en evidencias.
- Garantizar un profundo compromiso con el trabajo que realizas, para que puedas abordar de manera adecuada y ética los problemas que surjan.
- Mantenerte al día y buscar constantemente mejorar tus habilidades, de manera que puedas contribuir al avance y al mejoramiento del panorama de la ciberseguridad.

Un ejemplo relevante es la Ley de Transferecia y Responsabilidad de los Seguros Médicos (HIPAA), una ley federal de los Estados Unidos establecida para proteger la información de salud de las/los pacientes, también conocida como Protected Health Information (PHI) o información de salud protegida. Esta ley prohíbe compartir la información de las/los pacientes sin su consentimiento. Por lo tanto, como profesional de la ciberseguridad, es tu responsabilidad garantizar que la organización en la que trabajas cumpla con su obligación legal y ética de informar a las personas en caso de que se produzca una violación de seguridad que exponga sus datos médicos.

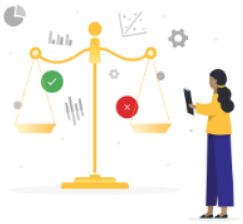
2.3. Complemento no calificado: Practica: Ética para profesionales de la ciberseguridad.

Práctica: Ética para profesionales de la ciberseguridad

Práctica: Ética para profesionales de la ciberseguridad
Ejercicio de opción múltiple

Práctica: Ética para profesionales de la ciberseguridad

Analiza diversos escenarios que podrías enfrentar en tu rol como analista de seguridad y reflexiona sobre cómo responderías a incidentes de seguridad, teniendo en cuenta tus conocimientos sobre ética en este campo.



Continuar

2.4. Cuadro de aviso de la discusión: Uso de la ética para tomar decisiones.

Ya conoces de qué se trata la ética en ciberseguridad y ejemplos específicos de cómo se aplica en el entorno laboral. Ahora, es momento de que compartas un poco de tu experiencia e intercambies ideas con otros/as estudiantes del curso.

Opción 1: Tu ejemplo puede estar relacionado con un entorno laboral, académico o voluntario, y debe enfocarse en un momento en el que elegiste tomar un camino ético de acción.

Para este tema de debate, ten en cuenta lo siguiente:

- ¿Cuál era la situación?
- ¿Cómo usaste la ética para tomar esa decisión?
- ¿Cuál fue el impacto o resultado de tu decisión?

Opción 2: Tu ejemplo puede estar relacionado con un entorno laboral, académico o voluntario, y debe enfocarse en un momento en el que otra persona eligió tomar un camino ético de acción.

Para este tema de debate, ten en cuenta lo siguiente:

- ¿Cuál era la situación?
- ¿Cómo usó esa persona la ética para tomar esa decisión?
- ¿Cuál fue el impacto o resultado de la decisión de esa persona?

2.5 Cuestionario practico: Pon a prueba tus conocimientos: Ética en ciberseguridad.

1. Una persona capacitada en el manejo de información de identificación personal (PII) e información de identificación personal sensible (SPII) deja información confidencial de pacientes desbloqueada en un área pública. ¿Qué principios éticos se violan en este caso? Selecciona todas las opciones que correspondan. **1 punto**

- [ ] Protección de la privacidad
- [ ] Confidencialidad
- [ ] Imparcialidad
- [ ] Leyes

2. Completa el espacio en blanco: La protección de la privacidad significa preservar _____ contra el acceso o uso no autorizado. **1 punto**

- ( ) las redes empresariales
- ( ) los procesos de cumplimiento
- ( ) la documentación
- ( ) la información personal

3. Recibes un mensaje de texto en tu dispositivo personal de parte de tu superior , en el que indica que no puede acceder a la base de datos segura en línea de la empresa. El motivo de dicho acceso es que, para actualizar el calendario mensual de eventos de la compañía, necesita saber cuanto antes la fecha de cumpleaños de un empleado de la empresa. Sin embargo, las políticas y procedimientos de tu organización establecen claramente que la información de las personas que trabajan en la empresa nunca debe ser accedida o compartida a través de canales de comunicación personales. Frente a esta situación, ¿qué deberías hacer? **1 punto**

- ( ) Darle a tu superior la fecha de nacimiento del empleado; un evento es un gesto amistoso.
- ( ) Solicitar a tu superior que se identifique para asegurarte de que el mensaje de texto sea auténtico; luego, proporcionar la fecha de cumpleaños.
- ( ) Pedirle a tu superior que proporcione pruebas de su incapacidad para acceder a la base de datos.
- ( ) Declinar de manera respetuosa y recordarle a tu superior las políticas de la organización.

4. Trabajas para una empresa de servicios públicos con sede en los Estados Unidos que ha sufrido una violación de datos. Varios grupos hacktivistas se atribuyen la responsabilidad del ataque. Sin embargo, no hay evidencia que permita verificar sus afirmaciones. ¿Cuál es la manera más ética de responder a este incidente? **1 punto**

- ( ) Dirigirte a un grupo hacktivista específico como advertencia a los demás.
- ( ) Mejorar la seguridad de la empresa para ayudar a prevenir futuros ataques.
- ( ) Realizar ciberataques contra cada grupo hacktivista que se atribuyó la responsabilidad.
- ( ) Escalar la situación involucrando a otras organizaciones que fueron atacadas.

3. Repaso: Protección frente a amenazas, riesgos y vulnerabilidades.

3.1. Lectura: Términos y definiciones módulo 3.

- **Activo**: Elemento percibido como valioso para una organización.
- **Arquitectura de seguridad:** Tipo de diseño de seguridad compuesto por múltiples herramientas y procesos, que se utiliza para proteger a una organización de los riesgos y amenazas externas.
- **Confidencialidad:** Propiedad según la cual únicamente las personas autorizadas pueden acceder a activos o datos específicos.
- **Controles de seguridad:** Pautas diseñadas para abordar y eliminar riesgos de seguridad específicos, como la alteración o la eliminación de información de perfiles, entre otros.
- **Disponibilidad:** Principio según el cual los datos son accesibles para las personas autorizadas a utilizarlos.
- **Ética de la seguridad:** Pautas para tomar decisiones apropiadas como profesional de la seguridad.
- **Gobernanza de seguridad:** Prácticas que ayudan a apoyar, definir y dirigir los esfuerzos de seguridad de una organización.
- **Hacktivista:** Persona que utiliza el hacking para lograr objetivos políticos.
- **Información médica protegida (PHI por sus siglas en inglés):** Cualquier información relacionada con la salud, o la condición física o mental pasada, presente o futura de una persona.
- **Integridad:** Cualidad que identifica a los datos como correctos, auténticos y confiables.
- **Ley de Transferencia y Responsabilidad de los Seguros Médicos (HIPAA):** Ley federal de los Estados Unidos establecida para proteger la información de salud de los pacientes.
- **Marco de Ciberseguridad del Instituto Nacional de Estándares y Tecnología (NIST por sus siglas en inglés)**: Marco de adhesión voluntaria creado en los Estados Unidos, que incluye estándares, pautas y prácticas recomendadas para gestionar los riesgos de ciberseguridad.
- **Marcos de seguridad:** Pautas utilizadas para crear planes que ayuden a mitigar el riesgo y las amenazas a los datos y la privacidad.
- **Open Web Application Security Project (OWASP):** Organización sin fines de lucro centrada en mejorar

la seguridad de software.

- **Protección de la privacidad:** Acto de proteger la información personal de usos no autorizados.
- **Tríada de confidencialidad, integridad y disponibilidad (CID):** Guía que ayuda a las organizaciones a evaluar los riesgos y establecer sistemas y políticas de seguridad**.**