26 / 09 / 24 / Ciberseguridad - Google - Modulo 1

- Especialidad de seguridad
  - Analista o especialista en Seguridad
  - " " en Ciberseguridad.
  - Analista de centro de operaciones de seg (SOC)

Ciberseguridad: es la practica de garantizar la Confidencialidad, la integridad y la disponibilidad de la información mediante la protección de las redes, los dispositivos, las personas y los datos contra el acceso no autorizado o la explotación delictiva

Actor de amenaza (threat actor)

Es Cualquier persona o grupo que presenta un riesgo de Seguridad

Benefets of Security (beneficios de Seguridad)

- Protege Contra las amenazas externas o internas
  - (amenaza externa es una persona ajena a la organización que intenta acceder a información)redes o dispositevos prevados).
  - (amenaza interna proviene de empleados actuales o anteriores, Provedores externos o socios de confianza).

- Cumplir Con el Cumplimiento normativo (emplementar estandares de seguridad)

- Mantener y mejorar la productividad empresarial

- Reducir los gastos asociados con los riesgos
  - Como la recuperación de la perdida de datos o el tiempo de inactividad operativo, y, potencialmente evetar multas

- Mantenimiento de la Confianza en la marca

26 09 24 Introducción a la ciberseguridad - módulo 1 - Google

Lenguajes: Python y SQL

Responsabilidades Laborales

¿Qué hacen los analistas de seguridad?

Son responsables de vigilar y proteger la información y los sistemas

- Responsabilidades de un analista de Seguridad (son 3)

  - Proteger los sistemas informáticos y de redes.

    Requiere que un analista supervise la red interna de una organización. Si se detecta una amenaza, entonces un analista suele ser el primero en responder. Los analistas tambien suelen participar en ejercicios para buscar debilidades

  - Instalar Software preventivos.

    Una forma de hacerlo es trabajando con equipos de tecnología de la información (TI), para la instalación de software preventivos con el fin de identificar riesgos y vulnerabilidades.

    los analistas también pueden participar en el desarrollo de software y hardware. A menudo trabajaran con equipos de desarrollo para apoyar la seguridad de los productos estableciendo procesos y sistemas adecuados para satisfacer las necesidades de protección de datos

26/09/24 Introducción a la ciberseguridad - modulo 1 - Google

- Realizar auditorías de seguridad periódicas.

Es una revisión de los registros de seguridad de una organización, actividades y otros documentos relacionados

Competencias básicas de la ciberseguridad

- Habilidades transferibles: son habilidades de otras áreas que pueden aplicarse a diferentes carreras

- Habilidades técnicas: tambien pueden aplicarse a varias profesiones. Sin embargo, a veces pueden requerir el conocimiento de herramientas, procedimientos y políticas especificas.

- Habilidades transferibles (basicas)

  - Comunicación
  - Colaboración
  - Análisis
  - Resolución de Problemas (requerida)

- Habilidades técnicas (basicas)

  - Lenguaje de programación (Python y SQL)
  - Herramientas de administración de información y eventos de Seguridad (SIEM)
  - Informática forense

26/09/24 Competencias básicas para los profesionales de la ciberseguridad

Información de identificación Personal (PII)

La información de identificación personal, o PII, es cualquier información que se utiliza para deducir la identidad de una persona. La PII incluye el nombre completo, la fecha de nacimiento, la dirección física, el número de teléfono, la dirección de correo electrónico, el protocolo de internet o la dirección IP de una persona e información similar.

La información de identificación personal confidencial (sensible) (SPII), es un tipo específico de PII que se rige por pautas de manejo más estrictas y puede incluir números de Seguridad Social, información médica o financiera y datos biométricos, como reconocimiento facial. Si se roba la SPII, esto tiene el potencial de ser significativamente más perjudicial para una persona que si se roba la PII

los datos de PII y SPII son activos claves para un actor de amenazas buscará si una organización sufre violación