**Términos y definiciones del Curso 2**

A

**Activo:** Elemento percibido como valioso para una organización.

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

**Amenaza externa:** Cualquier riesgo a la seguridadproducido fuera de la organización que tenga el potencial de dañar sus activos.

**Amenaza interna:** Riesgo a la seguridadproducido por una persona que pertenece o perteneció a una empresao tiene una relación directa o de confianza con ella.

**Auditoría de seguridad:** Revisión de los controles, políticas y procedimientos de seguridad de una organización.

**Autenticación:** Proceso de verificar la identidad de una persona.

**Autorización:** Proceso de determinar si un/a usuario/a autentificado/a tiene acceso a recursos específicos en un sistema.

**Autorizar:** Sexto paso del RMF del NIST que se refiere a asumir la responsabilidad de los riesgos de seguridad y privacidad que puedan existir en una organización.

B

**Biometría:** (Consultar **Datos biométricos**).

C

**Categorizar:** Segundo paso del Marco de Gestión de Riesgos (RMF) del NIST, que se lleva a cabo para desarrollar procesos y tareas de gestión de riesgos.

**Chronicle:** Herramienta nativa de la nube diseñada para conservar, analizar y buscar datos.

**Cifrado:** Proceso de convertir datos de un formato legible a uno codificado con el fin de protegerlos.

**Confidencialidad:** Propiedad según la cual únicamente las personas autorizadas pueden acceder a activos o datos específicos.

**Continuidad del negocio:** Capacidad de una organización para seguir funcionando durante una interrupción no planificada del servicio.

**Controles de seguridad:** Medidas de prevención diseñadas para reducir riesgos de ciberseguridad específicos.

D

**Datos biométricos:** Características físicas únicas que se pueden utilizar para verificar la identidad de una persona.

**Detectar:** Función central del NIST relacionada con la identificación de posibles incidentes de seguridad y la mejora de las capacidades de monitoreo y respuesta.

**Disponibilidad:** Propiedad según la cual todas las personas autorizadas pueden acceder a activos o datos específicos.

E

**Evaluar:** Quinto paso del Marco de Gestión de Riesgos (RMF) del NIST, para determinar si los controles establecidos se han implementado correctamente

G

**Gestión de eventos e información de seguridad (SIEM por sus siglas en inglés)**: Solución de seguridad que recopila y analiza los datos de registro para monitorear actividades críticas en una organización.

I

**Identificar**: Función central del NIST relacionada con la gestión del riesgo de ciberseguridad y su efecto sobre las personas y los activos de una organización.

**Implementar:** Cuarto paso del Marco de Gestión de Riesgos (RMF) del NIST, que consiste en aplicar planes de seguridad y privacidad en una organización.

**Ingeniería social:** Técnica de manipulación que busca engañar a las personas con el fin de que revelen información o realicen determinadas acciones.

**Integridad:** Cualidad que identifica los datos como correctos, auténticos y confiables.

L

**Log:** (Consultar **Registro**).

M

**Manual de estrategias:** Guía que proporciona detalles sobre cualquier acción operativa.

**Marco de Ciberseguridad (CSF) del Instituto Nacional de Estándares y Tecnología (NIST):** 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.

**Métricas:** Atributos técnicos clave, como el tiempo de respuesta, la disponibilidad y la tasa de fallos, que se utilizan para evaluar el rendimiento de una aplicación de software.

**Monitorear**: Séptimo paso del Marco de Gestión de Riesgos (RMF) del NIST, que consiste en evaluar cómo están funcionando los sistemas.

O

**Open Web Application Security Project (OWASP):** Organización sin fines de lucro centrada en mejorar la seguridad del software.

**Orquestación, automatización y respuesta de seguridad (SOAR):** Conjunto de aplicaciones, herramientas y flujos de trabajo que utilizan la automatización para responder a incidentes de seguridad.

P

**Playbook:** (Consultar **Manual de estrategias**).

**Postura de seguridad:** Capacidad de una organización para administrar la defensa de sus activos y datos críticos y reaccionar ante los cambios.

**Preparar:** Primer paso del Marco de Gestión de Riesgos (RMF) del NIST, relacionado con las actividades necesarias para gestionar los riesgos de seguridad y privacidad antes de que se produzca una vulneración.

**Proteger:** Función central del NIST que consiste en resguardar a una organización a través de la implementación de políticas, procedimientos, capacitación y herramientas que ayuden a mitigar las amenazas a la ciberseguridad.

**Publicación Especial (SP) del Instituto Nacional de Estándares y Tecnología (NIST) 800-53:** Marco unificado para proteger la seguridad de los sistemas de información dentro del gobierno federal de los EE.UU.

R

**Ransomware:** (Consular **Secuestro de datos**)

**Recuperar:** Función central del NIST que consiste en restablecer el funcionamiento normal de los sistemas afectados.

**Reducción del riesgo:** Proceso de disponer de procedimientos y reglas adecuadas para reducir rápidamente el impacto de cualquier amenaza, por ejemplo, una brecha.

**Registro (log):** Inventario de eventos que tienen lugar dentro de los sistemas de una organización.

**Responder:** Función central del NIST relacionada con asegurarse de que se utilicen los procedimientos adecuados para contener, neutralizar y analizar incidentes de seguridad, e implementar mejoras en el proceso de seguridad.

**Responsabilidad compartida:** Idea de que todas las personas de una organización asuman un papel activo en la reducción del riesgo y el mantenimiento de la seguridad física y virtual.

**Respuesta a incidentes:** Intento rápido de una organización de identificar un ataque, contener los daños y corregir los efectos de una infracción de seguridad.

**Riesgo:** Cualquier hecho que pueda afectar a la confidencialidad, integridad o disponibilidad de un activo.

S

**Secuestro de datos (Ransomware):** Ataque malicioso que consiste en cifrar los datos de una organización para exigir el pago de un rescate para restablecer el acceso a ellos.

**Seleccionar**: Tercer paso del Marco de Gestión de Riesgos (RMF) del NIST que consiste en elegir, personalizar y capturar la documentación de los controles que protegen a una organización.

**Sistema Operativo (SO):** Interfaz entre la computadora y el/la usuario/a.

**Software antivirus:** Programa utilizado para prevenir, detectar y eliminar software malicioso y virus.

**Splunk Cloud:** Herramienta alojada en la nube que se utiliza para recopilar, buscar y monitorear datos de registro.

**Splunk Enterprise:** Herramienta utilizada para retener, analizar y buscar datos de registro de una organización y proporcionar información de seguridad y alertas en tiempo real.

T

**Tríada de confidencialidad, integridad y disponibilidad (CID):** Guía que ayuda a las organizaciones a evaluar los riesgos y establecer sistemas y políticas de seguridad.

V

**Vector de ataque:** Método que se utiliza para penetrar las defensas de seguridad de un sistema informático.

**Vulnerabilidad:** Debilidad que puede ser aprovechada por una amenaza.