**Términos del glosario de la semana 2**

**Términos y definiciones del curso 5, semana 2**

**Algoritmo:** Conjunto de instrucciones definidas, ordenadas y acotadas para resolver un problema, realizar un cálculo o desarrollar una tarea.

**Algoritmo de cifrado (cipher):** Algoritmo que cifra la información.

**Aprovisionamiento de usuarios:** Proceso de creación, actualización, modificación o eliminación de cuentas o perfiles de usuarios.

**Ataque de fuerza bruta:** Proceso de ensayo y error para descubrir información privada, como, por ejemplo, una contraseña.

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

**Autenticación básica:** Tecnología utilizada para establecer la solicitud de un usuario de acceder a un servidor.

**Autenticación multifactor (MFA):** Medida de seguridad que exige a un usuario verificar su identidad en dos o más formas para acceder a un sistema o red.

**Bit:** La unidad más pequeña de medición de datos en una computadora.

**Cargador:** Código malicioso que se inicia después de que un usuario inicia un programa dropper.

**Certificado digital:** Documento electrónico que verifica la identidad del titular de una clave pública.

**Cifrado (encriptación):** Proceso de convertir datos de un formato legible a uno codificado.

**Cifrado asimétrico:** Sistema criptográfico que utiliza dos claves, una pública y otra privada, para cifrar y descifrar datos.

**Cifrado simétrico:** Sistema criptográfico que utiliza una única clave para cifrar y descifrar datos.

**Clave criptográfica:** Secuencia de datos que descifra el texto cifrado o viceversa.

**Colisión de hash:** Situación en la que diferentes entradas comparten el mismo valor hash.

**Controles de acceso:** Tipo de controles de seguridad que gestionan el acceso, la autorización y el manejo de la información.

**Controles de seguridad:** Pautas diseñadas para abordar y eliminar riesgos de seguridad específicos, como la alteración o eliminación de información de perfiles, entre otros.

**Cookie de sesión:** Token que utilizan los sitios web para validar una sesión y determinar su duración.

**Criptografía:** (Consultar Cifrado).

**Custodio de datos:** Cualquier persona o entidad responsable del manejo, transporte y almacenamiento seguro de la información

**Estándar de Seguridad de Datos para la Industria de Tarjetas de Pago (PCI-DSS):** Guía que define controles para la protección de los datos de titulares de tarjetas de pago y otros datos sensibles de autenticación, durante su procesamiento, almacenamiento y transmisión.

**Evaluación de seguridad:** Proceso de verificación que busca determinar la eficacia de las capacidades de ciberseguridad actuales contra las amenazas.

**Función hash:** Algoritmo que produce un código que no se puede descifrar.

**Gestión de identidad y acceso (IAM):** Conjunto de procesos y tecnologías que ayuda a las organizaciones a administrar las identidades digitales en su entorno.

**Identificador de sesión (ID de sesión):** Token único que identifica a un usuario y a su dispositivo mientras accede a un sistema.

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

**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.

**Infraestructura de clave pública (PKI, por sus siglas en inglés):** Marco de cifrado que garantiza la seguridad del intercambio de información en línea.

**Inicio de sesión único (SSO):** Solución de autenticación que combina varios inicios de sesión diferentes en uno solo.

**No repudio:** Concepto según el cual no se puede negar la autenticidad de una información.

**OAuth “Open Authorization” (autorización abierta):** Protocolo de autorización de estándar abierto que comparte el acceso designado entre aplicaciones.

**Principio de mínimo privilegio:** El concepto de otorgar únicamente el acceso y la autorización mínimos necesarios para ejecutar una tarea o función.

**Privacidad de la información:** Protección contra el acceso y la difusión de datos no autorizados.

**Propietario de datos:** Persona que tiene la potestad de decidir quién puede acceder a su información, editarla, usarla o destruirla.

**Salting (salado):** Protección adicional que se utiliza para reforzar las funciones hash que consiste en añadir un factor aleatorio a cada hash con el fin de que no se pueda predecir.

**Secuestro de sesión:** Ataque malicioso que consiste en obtener el identificador de sesión de un usuario legítimo.

**Segregación de funciones:** Principio según el cuál no se debe otorgar a una misma persona accesos a dos o más responsabilidades dentro del sistema que le permitirían hacer un uso indebido del mismo.

**Sesión:** Secuencia de solicitudes y respuestas de autenticación básica HTTP de red asociadas con el mismo usuario.

**Tabla Arcoíris (Tabla Rainbow):** Archivo de valores hash generados previamente y su texto sin cifrar asociado.

**Tabla hash:** Estructura de datos que se utiliza para almacenar y hacer referencia a los valores hash.

**Token de interfaz de programación de aplicaciones (API):** Pequeño bloque de código cifrado que contiene información sobre un usuario.