GLOSARIO DE TÉRMINOS

CUALIFICACIÓN PROFESIONAL: SEGURIDAD INFORMÁTICA

Código: IFC153_3 NIVEL: 3

Amenaza: Posible causa de un incidente no deseado, lo cual puede resultar en un daño a un sistema, persona u organización.

Análisis de riesgos: Uso sistemático de la información para identificar fuentes y para estimar el riesgo.

Análisis de vulnerabilidades: Recopilar, analizar y sistematizar, de una forma estructurada y lógica, información sobre la vulnerabilidad de la información.

Analizador de protocolos: Herramienta software que nos permite analizar el tráfico, a nivel de protocolos, que discurre por una red informática.

Appliance: Dispositivo hardware independiente con software integrado diseñado para proporcionar un recurso específico.

Autoridad de certificación (CA): Entidad de confianza, responsable de emitir y revocar certificados digitales, utilizados en la firma electrónica, para lo cual se emplea en la criptografía de clave pública.

Certificado digital: Documento digital mediante el cual un tercero confiable (una autoridad de certificación) garantiza la vinculación entre la identidad de un sujeto o entidad y una clave pública.

Confidencialidad: Propiedad de que una información esté disponible y no sea divulgada a personas, entidades o procesos no autorizados.

Demilitarized Zone (DMZ) [Zona Desmilitarizada]: Subred, dentro de una red de área local, que permite proporcionar servicios a una red externa (normalmente internet) aislando al resto de equipos de la red local de los problemas de seguridad provenientes de la red externa.

Domain Name System (DNS) [Sistema de Nombres de Dominio]: Sistema de nomenclatura para sistemas informáticos que permite asociar nombres de dominio a direcciones IP.

Dynamic Host Configuration Protocol (DHCP) [Protocolo de configuración dinámica de host]: Protocolo de red que permite a los host obtener de forma automática los parámetros de configuración para conectarse a una red.

Firewall [Cortafuegos]: Dispositivo o software encargado de proteger una red permitiendo los accesos autorizados y limitando los no autorizados. Además pueden cifrar, descifrar y limitar el tráfico siguiendo un conjunto de reglas configuradas.

Firma digital: Esquema matemático que sirve para demostrar la autenticidad de un mensaje digital o de un documento electrónico.

Gateway [Pasarela]: Dispositivo que permite la interconexión de redes con diferentes arquitecturas.

Infraestructura de clave pública (PKI): Conjunto de protocolos, servicios y estándares para las comunicaciones seguras mediante el uso de certificados digitales y firmas digitales.

Internet Protocol Security (IPSec)[Seguridad del Protocolo Internet]: Protocolo que permite la creación de VPNs asegurando las comunicaciones sobre el protocolo IP.

Malicious software (Malware) [Software malicioso]: Software que se infiltra en un sistema informático con el objeto de obtener información, controlar los equipos o dañar el sistema.

Network Address Translation (NAT) [Traducción de Dirección de Red]: Método utilizado por los routers en el que se cambia la dirección IP en la cabecera de los paquetes IP comúnmente utilizado para permitir el uso de direcciones privadas para el acceso a internet.

Network intrusion detection system (NIDS) [Sistema de detección de intrusos en una Red]: Sistema de detección que permite localizar anomalías como ataques de denegación de servicio o intentos de acceso indebido analizando el tráfico de red en tiempo real.

Objetivo de punto de recuperación (RPO): Período máximo que se permite en una organización de posible pérdida de datos. Determina la frecuencia de realización de copias de seguridad.

Objetivo de tiempo de recuperación (RTO): Tiempo que la organización puede permitirse tener caído un determinado servicio, antes de que esta caída le ocasione consecuencias inaceptables, relacionadas con una ruptura en la continuidad del negocio.

Open system interconnection (OSI) [Interconexión de sistemas abiertos]: Modelo de arquitectura utilizado como referencia para los sistemas de comunicación.

Red Privada Virtual (VPN): Red privada de comunicaciones, implementada sobre una infraestructura pública.

Secure Sockets Layer (SSL) [Capa de conexión segura]: Protocolo que proporciona conexiones seguras a través de una red.

Seguridad de Información: Preservación de la confidencialidad, integridad y disponibilidad de la información.

Sistema de Detección de Intrusos (IDS): Programa usado para detectar accesos no autorizados a un ordenador o a una red.

Sistema de Prevención de Intrusos (IPS): Dispositivo que ejerce el control de acceso en una red informática para proteger a los sistemas informáticos de ataques y abusos.

Virtual Private Network (VPN) [Red privada Virtual]: Tecnología que permite estender una red de área local através de una red pública garantizando la seguridad.

Vulnerabilidad: Debilidad de un activo o control que puede ser explotado por una fuente de riesgo. Debilidad de software, hardware o servicio en línea que puede ser explotada por una amenaza.