GLOSARIO DE TÉRMINOS

ESTÁNDAR DE COMPETENCIAS PROFESIONALES: Implementar sistemas seguros de acceso y transmisión de datos

Código: ECP0489_3 NIVEL: 3

Actualización: Lanzamiento o instalación de una nueva versión de un software que incluye más y mejores funcionalidades y/o soluciona fallos de la versión precedente.

Autenticación: Proceso de verificar la identidad de alguien o algo. La autentificación suele tener lugar mediante la comprobación de una contraseña, un token de hardware o algún otro dato que demuestre la identidad.

Backup: (Anglicismo. En español, respaldo, copia de respaldo o copia de reserva). Copia de los datos originales que se realiza con el fin de disponer de un medio para recuperarlos en caso de su pérdida.

Certificado digital: Certificación electrónica expedida por una entidad de confianza o autoridad certificadora que vincula a su suscriptor (persona, programa o máquina) con unos datos de verificación de firma y se usa para confirmar su identidad.

Cifrado: También, encriptado. Conversión de información de un formato legible a un formato codificado. La información cifrada solo se puede comprender y procesar tras el descifrado (desencriptado).

Cifrar: Encriptar. Convertir información de un formato legible a un formato codificado. La información cifrada/encriptada solo se puede comprender y procesar tras el descifrado/desencriptado.

Clave privada: Una de las dos claves que genera un procedimiento de criptografía asimétrica. La clave privada y la pública están matemáticamente relacionadas. La clave pública se genera siempre a partir de la clave privada. La clave pública puede ser difundida por su propietario para ser usada por terceros. Estos terceros pueden usar la clave pública del propietario para cifrar mensajes que solo el propietario de la clave pública podrá leer usando su clave privada.

Confidencialidad: También, principio de privacidad. Uno de los principios de la seguridad informática. Hace referencia a que la información solo debe ser conocida por las personas autorizadas para ello. Es decir, ciertos datos o programas solo pueden ser accesibles para las personas autorizadas.

Control de acceso: Forma de limitar el acceso a un sistema o a recursos físicos o virtuales. En seguridad informática, es el proceso mediante el cual los usuarios obtienen acceso y ciertos privilegios a los sistemas, recursos o información. En el contexto de los sistemas de seguridad físicos, el control de acceso lo constituyen son los mecanismos y dispositivos que permiten autorizar o denegar el acceso físicamente a personas o vehículos a un recinto.

Cortafuegos: (Firewall). Sistema que protege redes y terminales privadas de accesos no autorizados, especialmente durante la navegación por internet.

Disponibilidad: Capacidad de un servicio, de unos datos o de un sistema, a ser accesible y utilizable por los usuarios o procesos autorizados cuando estos lo requieran. Es uno de los principios fundamentales de la ciberseguridad junto a la confidencialidad y la integridad.

Firewall: (Anglicismo. En español, cortafuegos). Sistema que protege redes y terminales privadas de accesos no autorizados, especialmente durante la navegación por internet.

Hardware: (Anglicismo). Conjunto de los componentes que conforman la parte material (física) de una computadora.

Integridad: Garantía de que la información digital no está dañada y solo pueden acceder o modificar aquellos autorizados para hacerlo.

No repudio: También, irrenunciabilidad. Mecanismos hardware y software que proveen garantía al receptor de una comunicación en cuanto que el mensaje fue originado por el emisor y no por alguien que se hizo pasar por este. Además, previene que el remitente o emisor del mensaje afirme que él no envió el mensaje. Es uno de los principios fundamentales de seguridad de la información.

Nodo: Punto de conexión que puede recibir, crear, almacenar o enviar datos a lo largo de rutas de red distribuidas. Cada nodo de la red, ya sea un punto final para la transmisión de datos o un punto de redistribución, tiene una capacidad programada o diseñada para reconocer, procesar y reenviar transmisiones a otros nodos de la red.

Protocolo: Conjunto de normas y procedimientos establecidos para el desarrollo de una actuación.

Proxy: (Anglicismo). En una red informática, servidor -programa o dispositivo-, que hace de intermediario en las peticiones de recursos que realiza un cliente a otro servidor.

Red de área local: (RAL. En inglés, Local Área Network o LAN) Red de comunicaciones de datos entre dispositivos informáticos que cubre un área limitada a metros o pocos kilómetros tal como una planta, un edificio o un grupo local de edificaciones. La LAN es generalmente de titularidad privada.

Red inalámbrica: Tipo de conexión entre sistemas informáticos que se lleva a cabo mediante ondas del espectro electromagnético.

Router: (Anglicismo. En español, encaminador). Dispositivo de interconexión entre redes de datos diferentes. Opera en el nivel tres de OSI. Un tipo es el router de banda ancha que interconecta una red local e Internet.

Servicio: Programa instalado en un equipo remoto llamado servidor y cuya funcionalidad se ofrece a otros equipos conectados a él por red llamados cliente. Son típicos los servicios/servidores de impresión, de archivos, de cualquier programa/software mediante llamadas a procedimientos remotos (RPC) o de páginas web. La mayor capacidad del servidor se pone al servicio de los clientes, lo que redunda en una mayor simplicidad y menor coste de los segundos.

Servidor: Máquina física integrada en una red informática en la que, además del sistema operativo, opera uno o varios servicios "software" que se ofrecen a otros equipos denominados clientes que pueden estar conectados a nivel local o a través de una red externa. El tipo de servicio depende del tipo de "software" del servidor. La base de la comunicación es el modelo cliente-servidor y, en lo que

concierne al intercambio de datos, entran en acción los protocolos de transmisión específicos del servicio.

Tolerancia: Máxima diferencia que se admite entre el valor nominal y el valor real o efectivo en las características físicas y químicas de un material, pieza o producto.

Trazabilidad: Conjunto de procedimientos que permiten seguir la evolución de los procesos o productos en cada una de sus etapas.

Virtualización: Creación a través de "software" de una representación en un entorno simulado (versión virtual) de algún recurso tecnológico o físico.

VPN: (Virtual Private Network. En español, Red Privada Virtual). Servicio que cifra los datos de las comunicaciones entre dos puntos, incluyendo la navegación en Internet, construyendo una red privada y segura o túnel entre la conexión de una máquina cliente y un servidor destinatario.

Vulnerabilidad: Debilidad o fallo en un sistema de información que pone en riesgo la seguridad de la información pudiendo permitir que un atacante pueda comprometer la integridad, disponibilidad o confidencialidad de la misma, por lo que es necesario encontrarlas y eliminarlas lo antes posible. Estos "agujeros" pueden tener distintos orígenes, por ejemplo: fallos de diseño, errores de configuración o carencias de procedimientos.