GLOSARIO DE TÉRMINOS

ESTÁNDAR DE COMPETENCIAS PROFESIONALES: Gestionar incidentes de ciberseguridad

Código: ECP0488_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.

Antivirus: Tipo de software que se utiliza para evitar, buscar, detectar y eliminar virus de un ordenador.

Ciberseguridad: Conjunto de elementos, medidas y equipos destinados a defender las computadoras, los servidores, los dispositivos móviles, los sistemas electrónicos, las redes y los datos de ataques maliciosos. También se conoce como seguridad de tecnología de la información, seguridad de la información electrónica o seguridad informática.

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.

DRP: (Disaster Recovering Plan. En español, Plan de Recuperación de Desastres). Estrategia que se seguirá para restablecer los servicios de TI, conocidos como el Hardware y Software después de haber sufrido una afectación por una catástrofe natural, epidemiológica, fallo masivo, daño premeditado (secuestro de la información, ransomware, hackeos, robo de datos) o un ataque de cualquier tipo el cual atente contra la continuidad del negocio.

EDR: (Endpoint Detection and Response). Herramienta que proporciona monitorización y análisis continuo del dispositivo terminal (endpoint) y la red. La finalidad es identificar, detectar y prevenir amenazas avanzadas (APT) con mayor facilidad. La tecnología EDR detecta ataques que nuestro antivirus ha pasado por alto. Monitoriza y evalúa todas las actividades de la red (eventos de los usuarios, archivos, procesos, registros, memoria y red). Detecta ataques informáticos en tiempo real, y permite tomar medidas inmediatas si es necesario.

EPP: (Endpoint Protection Platform). Solución de seguridad integral desplegada en equipos terminales para protegerse de amenazas. Las soluciones EPP son gestionadas típicamente en la nube y usan datos en ella para asistir en soluciones avanzadas de monitorización y solución remotas. Contienen una suite de tecnologías de seguridad tales como antivirus, encriptación de datos y prevención de pérdida de datos.

Evento: Notificación automática que ha habido algún tipo de acción y que suele disparar una acción o conjunto de acciones que, a su vez, pueden dar como resultado un evento en particular o una serie de eventos.

IDS: (Intrusion Detection System. En español, Sistema de Detección de Intrusos). Sistema de supervisión que detecta actividades sospechosas y genera alertas al detectarlas.

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

Intranet: (Anglicismo). Red informática interna de una empresa u organismo, basada en los estándares de Internet, en la que las computadoras están conectadas a uno o varios servidores web.

IOC: (Indicators of compromise). Descripción de un incidente de ciberseguridad o cualquier actividad maliciosa, que es posible identificar mediante patrones. Los IOC permiten mejorar la reacción, generar una alerta y una respuesta al momento de ser detectados por algún sistema de seguridad (WAF, FW, IPS, EDR, Antispam, etc). Los patrones que se pueden encontrar en un IOC hacen énfasis a las evidencias que pueden existir en las redes o en los equipos.

IPS: (Intrusion Prevention System. En español, Sistema de Prevención de Intrusiones). Dispositivo o aplicación software que monitoriza una red para detectar y responder a cualquier actividad maliciosa o violaciones de la política de seguridad. Cualquier actividad o violación maliciosa es reportada o recogida de manera centralizada usando un sistema de seguridad de la información y de gestión de eventos. A diferencia de los IDS, los IPS son capaces de responder a intrusiones detectadas en el momento de su descubrimiento.

Monitorización: Acción realizada por elementos físicos y "software" que registran la situación en que están cada uno de los aspectos que se desean controlar.

OSINT: (Open Source INTelligence. En español, Inteligencia de Fuentes Abiertas). Conjunto de técnicas y herramientas para recopilar información pública, analizar los datos y correlacionarlos convirtiéndolos en conocimiento útil.

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

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.

SIEM: (Security Information and Event Management. En español, gestión de información y eventos de seguridad). Solución de seguridad que ayuda a las organizaciones a reconocer posibles amenazas y vulnerabilidades de seguridad antes de que tengan la oportunidad de interrumpir operaciones empresariales.

Virus: Programa informático elaborado de manera anónima que tiene la capacidad de reproducirse y transmitirse independientemente de la voluntad del

operador y que causa alteraciones más o menos graves en el funcionamiento de la computadora.

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.