Empresa Nacional Promotora del Desarrollo Territorial S.A.

Glosario Técnico

A

- **Activo Crítico**: Elemento esencial para el funcionamiento de una organización que, en caso de comprometerse, puede causar interrupciones significativas en las operaciones o pérdida de datos.
- **Análisis de Comportamiento**: Técnica que observa y evalúa el comportamiento de sistemas, usuarios o aplicaciones para detectar patrones anómalos que puedan indicar amenazas de seguridad.
- **Análisis de Vulnerabilidades**: Procedimiento para identificar debilidades en un sistema de información, evaluando su exposición a amenazas potenciales y recomendando medidas correctivas.
- **Arquitectura de Seguridad**: Diseño estructurado que establece los componentes, políticas, herramientas y procesos necesarios para proteger la infraestructura tecnológica y los datos de una organización.

B

- **BGP (Border Gateway Protocol)**: Protocolo de enrutamiento utilizado para intercambiar información de encaminamiento entre sistemas autónomos en redes grandes, como Internet.

C

- **Cifrado SSL/TLS**: Método de seguridad que utiliza certificados digitales y criptografía para proteger las comunicaciones entre servidores y clientes en Internet.
- **Cluster**: Conjunto de servidores o sistemas que trabajan conjuntamente como una sola unidad lógica para mejorar la disponibilidad, escalabilidad y redundancia de servicios.
- **Confidencialidad**: Salvaguarda que impide la divulgación de información a personas, entidades o procesos no autorizados.
- **Control de Acceso Basado en Roles (RBAC)**: Sistema que restringe el acceso a recursos según los roles asignados a los usuarios dentro de una organización.

D

- **Defensa en Profundidad**: Estrategia de seguridad que implementa múltiples capas de protección para mitigar riesgos, retrasar ataques y asegurar redundancia en las medidas de seguridad.
- **Decreto 1008 de 2018**: Regulación que establece lineamientos para la implementación de la Política de Gobierno Digital en Colombia, subrogando disposiciones anteriores relacionadas con tecnologías de la información.

- **Devolución de Llamada (Callback)**: Técnica que analiza el tráfico saliente para identificar conexiones a direcciones sospechosas relacionadas con actividades maliciosas.

E

- **Enrutamiento Basado en Políticas**: Método que define rutas específicas para el tráfico de red según criterios personalizados como IP de origen, destino, protocolos o aplicaciones utilizadas.
- **Especificaciones Técnicas**: Conjunto detallado de requisitos y características que deben cumplir los sistemas o servicios contratados para garantizar el cumplimiento de objetivos.
- **Evaluación de Riesgos Operacionales**: Proceso de análisis integral que identifica, mide y gestiona riesgos asociados a las operaciones, asegurando continuidad y resiliencia.

F

- **Firewall Stateful**: Cortafuegos que rastrea el estado y contexto de las conexiones de red para filtrar tráfico con base en reglas específicas y contexto de sesión.
- **Firmware**: Software embebido en hardware que controla funciones básicas de dispositivos electrónicos.
- **Funcionalidad NGFW**: Conjunto de capacidades avanzadas de cortafuegos que incluye inspección de aplicaciones, control granular, protección contra amenazas y gestión centralizada.

G

- **Gestión de Incidentes de Seguridad**: Proceso estructurado para identificar, analizar y responder a eventos de seguridad que puedan comprometer activos de información o infraestructura tecnológica.
- **Gobierno Digital**: Estrategia que promueve el uso de tecnologías de la información para mejorar la gestión pública y la prestación de servicios a los ciudadanos.

H

- **Habilitadores Transversales**: Componentes estratégicos que soportan la implementación de políticas de tecnología, como seguridad, arquitectura empresarial y servicios digitales.

I

- **Inspección Profunda de Paquetes (DPI)**: Tecnología que analiza el contenido de los datos transmitidos en la red para identificar aplicaciones, comportamientos sospechosos y amenazas.
- **Integración con Active Directory**: Funcionalidad que permite utilizar el directorio de usuarios de Microsoft para autenticar y controlar accesos a recursos y aplicaciones.

L

- **Latencia**: Tiempo que tarda un paquete de datos en viajar desde el origen hasta el destino, medida clave en el rendimiento de redes.

M

- **Mecanismos Anti-Evasión**: Métodos utilizados en soluciones de seguridad para detectar y bloquear técnicas sofisticadas empleadas por atacantes para evadir las defensas.
- **Mitre ATT&CK**: Base de conocimiento que documenta técnicas y tácticas empleadas por actores maliciosos, utilizada como referencia para evaluar y mejorar estrategias de ciberseguridad.

N

- **NAT64/NPTv6**: Tecnologías de traducción de direcciones que permiten la interoperabilidad entre redes IPv4 e IPv6, esenciales en entornos híbridos.
- **Nivel de Disponibilidad (TIER)**: Clasificación de centros de datos según su redundancia y tiempo de actividad garantizado, con TIER 4 representando el nivel más alto.

P

- **Prevención de Intrusiones (IPS)**: Tecnología que monitorea y bloquea actividades maliciosas identificadas en tiempo real, asegurando la protección proactiva contra ataques.
- **Protección Avanzada contra Amenazas (ATP)**: Soluciones que utilizan inteligencia artificial, sandboxing y técnicas de análisis avanzado para detectar y mitigar amenazas desconocidas y persistentes.

R

- **Resiliencia Operacional**: Capacidad de una organización para adaptarse, responder y recuperarse rápidamente de eventos disruptivos que afecten sus operaciones.
- **Resolución 500 de 2021**: Lineamientos y estándares para la seguridad digital en Colombia, con énfasis en auditorías, análisis de vulnerabilidades y pruebas de penetración.

S

- **Segmentación de Red**: Estrategia de ciberseguridad que divide una red en segmentos lógicos para limitar el movimiento lateral de atacantes y proteger activos críticos.
- **Seguridad y Privacidad**: Conjunto de medidas y prácticas diseñadas para proteger los datos y garantizar el cumplimiento de regulaciones sobre privacidad.

T

- **Técnicas de Escaneo de Vulnerabilidades**: Métodos automatizados que identifican brechas de seguridad en sistemas, aplicaciones y redes.

- **Tecnología de Engaño (Deception Technology)**: Herramienta que emplea activos falsos para desviar y atrapar atacantes, generando inteligencia procesable para mejorar defensas.

U

- **Usuarios Privilegiados**: Personas o sistemas con acceso elevado a recursos y configuraciones críticas dentro de una organización.

V

- **Virtualización de Recursos**: Técnica que permite ejecutar múltiples entornos operativos y aplicaciones en un solo hardware físico para optimizar el uso de recursos.
- **Visibilidad de Tráfico**: Capacidad de monitorear y analizar el tráfico de red para identificar patrones de uso, detectar anomalías y prevenir amenazas.

Z

- **Zero Trust**: Modelo de seguridad que asume que todas las conexiones y usuarios son potencialmente no confiables y requiere verificación continua de identidades y permisos.