Recomendaciones de seguridad en la red

1. Propósito y alcance

El siguiente documento sintetiza controles y recomendaciones orientados a proteger la infraestructura, la información y la integridad de los usuarios, así como a prevenir accesos no autorizados, spam, ataques y difusión de contenido ilegal, incluido material de abuso sexual infantil (CSAM). La seguridad se aborda mediante defensa en profundidad, protección perimetral, segmentación, gestión de accesos, monitoreo, cumplimiento normativo y prácticas de uso responsable del servicio.

2. Enfoque general de seguridad

La estrategia de seguridad se basa en la combinación de diversas capas de protección para asegurar la integridad, confidencialidad y disponibilidad de los servicios y datos. Este enfoque integra controles internos de infraestructura, mecanismos de operación y monitoreo, y recomendaciones de comportamiento seguro para los usuarios.

3. Controles técnicos de infraestructura

3.1 Protección perimetral con firewalls y cortafuegos

La protección perimetral funciona como primera línea de defensa, mediante el monitoreo y control del tráfico de red entrante y saliente con base en reglas de seguridad predefinidas. Los controles de cortafuegos también se consideran relevantes para los dispositivos de conexión de los usuarios, como medida complementaria frente a virus, spyware, spam y otros riesgos presentes en internet.

- Inspección de estado (Stateful Inspection): mantiene registro del estado de las conexiones y permite únicamente tráfico de respuesta legítimo.
- Filtrado de paquetes: bloquea o permite tráfico según direcciones IP de origen y destino, puertos y protocolos.
- Prevención y detección de intrusiones (IPS/IDS): identifica y bloquea patrones de ataque conocidos.
- Seguridad perimetral avanzada: protege e identifica de manera temprana eventos e incidentes que afectan la confidencialidad, disponibilidad e integridad de la información.

- Alta disponibilidad: las soluciones de cortafuegos y la arquitectura de alta disponibilidad contribuyen a proteger los datos y la información que los usuarios crean, distribuyen o transmiten a través de la red de internet.

3.2 Listas de Control de Acceso (ACLs)

Los equipos de red core, acceso y transporte cuentan con Listas de Control de Acceso (ACLs), las cuales proporcionan control granular sobre el flujo de tráfico dentro de la red.

- Control de tráfico interno: restringe el tráfico entre segmentos de red, permitiendo solo los protocolos y puertos necesarios.
- Mitigación de ataques: reduce la propagación de ataques internos al limitar la superficie de ataque disponible.
- Protección de servicios: asegura que solo hosts autorizados accedan a servicios específicos en los equipos de red.

3.3 Segregación de redes mediante VRF para gestión

La red de gestión se mantiene separada de la red de tráfico de usuarios mediante VRFs (Virtual Routing and Forwarding), lo que permite aislar lógicamente los entornos de administración y datos.

- Aislamiento lógico: una VRF crea una instancia de tabla de enrutamiento independiente, separando el tráfico de gestión del tráfico de datos de los usuarios.
- Seguridad mejorada: reduce la superficie de ataque porque el acceso a equipos de red para fines de gestión solo es posible desde interfaces y segmentos específicos dentro de la VRF de gestión.
- Minimización de riesgos: evita que el tráfico de usuarios, incluido tráfico malicioso o de spam, interfiera o acceda a recursos críticos de gestión de la infraestructura.

3.4 Gestión de cuentas y credenciales de acceso

La gestión de cuentas de acceso para equipos de red, acceso y transporte se fundamenta en controles de depuración, individualización de credenciales y robustez de contraseñas.

- Depuración regular: las cuentas inactivas o en desuso se eliminan o depuran de manera regular para minimizar puntos de entrada potenciales para actores no autorizados.
- Cuentas de uso único: cada técnico o administrador cuenta con credencial individual, lo que permite trazabilidad clara de las acciones.

- Contraseñas robustas: se exige el uso de contraseñas con políticas de complejidad, como longitud mínima, combinación de caracteres y rotación periódica, para dificultar ataques de fuerza bruta y adivinación de contraseñas.
- Uso personal de credenciales: las contraseñas no deben divulgarse y deben cambiarse periódicamente según las recomendaciones de dificultad aplicables a cada sistema o aplicación.

4. Prevención de spam, contenido malicioso y contenido ilegal

Las medidas de firewalls, ACLs, segmentación, monitoreo y gestión de acceso contribuyen a prevenir el spamming, la actividad maliciosa y la difusión de contenido ilegal.

- Bloqueo de puertos comunes de spam: los firewalls y las ACLs bloquean tráfico en puertos comúnmente utilizados para spam, por ejemplo, el puerto 25 sin autenticación para SMTP cuando no corresponde a una conexión controlada.
- Monitoreo de anomalías de tráfico: los sistemas de monitoreo detectan patrones de tráfico inusuales que podrían indicar spamming o ataques.
- Análisis de flujo de datos: el análisis del volumen y tipo de tráfico permite identificar patrones asociados con spam o distribución de contenido ilegal.
- Colaboración y cumplimiento normativo: se contempla la cooperación con autoridades legales y organizaciones de seguridad cibernética para identificar y bloquear fuentes de contenido ilegal, incluida la aplicación de filtros a nivel de red basados en listas negras proporcionadas por entidades relevantes, la atención rápida de solicitudes de bloqueo y el reporte de actividades sospechosas.

5. Operación de seguridad, monitoreo y cumplimiento

Los servicios de seguridad perimetral son gestionados y monitoreados por un Centro de Operaciones de Seguridad (SOC), con el objetivo de identificar de forma temprana eventos e incidentes que puedan afectar la confidencialidad, disponibilidad e integridad de la información.

La política de seguridad de la información se implementa conforme a criterios regulatorios y estándares internacionales vigentes. Como referencia normativa, se considera el artículo 5.1.2.3.1 de la Resolución CRC 5050 de 2016, modificada por la Resolución CRC 5569 de 2018.

El compromiso de seguridad se mantiene mediante la revisión continua de políticas y la adaptación a nuevas amenazas, con el fin de sostener un entorno de red seguro y responsable.

6. Recomendaciones de uso responsable y seguro del servicio

Además de los controles técnicos de infraestructura, el uso responsable por parte de los usuarios reduce la exposición a riesgos en internet. Las recomendaciones consolidadas son las siguientes:

- Programa de seguridad confiable: utilizar una solución de seguridad de marca conocida y confiable que proteja los dispositivos de conexión contra virus, spyware, spam y otros riesgos de la red.
- Cortafuegos en la conexión: procurar el acceso a internet a través de un cortafuegos que contribuya a mitigar riesgos de seguridad.
- Protección de datos personales y financieros: ser cuidadoso con la información que se entrega en internet y evitar divulgar datos personales, información financiera o contraseñas.
- Copias de seguridad: realizar respaldos periódicos de la información importante, preferiblemente en unidades de almacenamiento extraíbles, y evitar usar dichas unidades en dispositivos desconocidos.
- Correos sospechosos: desconfiar de mensajes de correo electrónico de contenido dudoso; no responderlos, no descargar su contenido, no acceder a enlaces y no ejecutar programas enlazados en ellos.
- Dispositivos compartidos: crear usuarios separados para cada persona que utilice el dispositivo y cerrar siempre la sesión de las cuentas de internet.
- Redes abiertas: evitar acceder a cuentas personales o páginas web que soliciten información personal, financiera o contraseñas cuando se utilicen redes abiertas.
- Red doméstica: mantener activada la función de seguridad para autenticación en la red de internet doméstica.

7. Conclusión

La implementación conjunta de firewalls perimetrales, ACLs en los niveles de red, segregación mediante VRF, gestión rigurosa de cuentas, monitoreo, análisis de tráfico, operación desde SOC, arquitectura de alta disponibilidad y prácticas de uso seguro constituye un marco integral para proteger la infraestructura y los datos. Estas medidas reducen accesos no autorizados, spamming, ataques y riesgos asociados con contenido ilegal, y se fortalecen mediante revisión continua, cumplimiento normativo y adaptación frente a nuevas amenazas.