Política de Seguridad en la Red para la Protección de los Usuarios

1. Objetivo

Proteger a los usuarios de la empresa contra amenazas cibernéticas, garantizar la privacidad de sus datos y asegurar un entorno de trabajo seguro y confiable.

2. Alcance

Esta política se aplica a todos los empleados, contratistas y terceros que utilicen los recursos de la red de la empresa.

3. Normatividad Vigente

La política se alinea con las regulaciones y normativas colombianas, incluyendo:

- **Ley 1581 de 2012**: Protección de Datos Personales.
- **Decreto 1377 de 2013**: Reglamentación de la Ley 1581.
- **Resolución 500 de 2021**: Lineamientos y estándares para la estrategia de seguridad digital.

4. Directrices Generales

- **Protección de Datos Personales**: Implementar medidas para proteger los datos personales de los usuarios, asegurando su confidencialidad, integridad y disponibilidad.
- **Concienciación y Capacitación**: Proveer formación continua a los usuarios sobre buenas prácticas de seguridad y normativas vigentes.
- **Control de Acceso**: Establecer mecanismos de autenticación y autorización para asegurar que solo usuarios autorizados accedan a los recursos de la red.
- **Monitoreo y Auditoría**: Realizar monitoreos continuos y auditorías periódicas para detectar y responder a incidentes de seguridad que puedan afectar a los usuarios.

5. Controles Específicos

- **Firewall y Sistemas de Detección de Intrusos (IDS/IPS):** Implementar y mantener firewalls y sistemas IDS/IPS para proteger la red contra accesos no autorizados y ataques.

- **Política de Contraseñas**: Establecer políticas de contraseñas robustas para el acceso a nuestros enrutadores, que incluyan requisitos de complejidad y cambios periódicos.
- **Cifrado de Datos**: Utilizar cifrado para proteger datos sensibles tanto en tránsito como en reposo.
- **Acceso Remoto Seguro**: Implementar soluciones de VPN y autenticación multifactor para accesos remotos.
- **Protección contra Pishing**: Implementar soluciones en nuestro Firewall que valide la autenticidad de los nombres de dominio resueltos por el protocolo DNS.
- **Gestión de Parches**: Mantener actualizados todos los equipos de borde así como las aplicaciones con los últimos parches de seguridad.

6. Procedimientos de Respuesta a Incidentes

- **Detección y Notificación**: Establecer procedimientos para la detección y notificación inmediata de incidentes de seguridad que afecten a los usuarios.
- **Respuesta y Mitigación**: Definir pasos claros para la respuesta y mitigación de incidentes, incluyendo la contención, erradicación y recuperación.
- **Análisis Post-Incidente**: Realizar análisis post-incidente para identificar causas raíz y mejorar las medidas de seguridad.

7. Revisión y Actualización

- **Auditorías Periódicas**: Realizar auditorías de seguridad periódicas para evaluar la efectividad de la política y realizar ajustes necesarios.
- **Actualización de la Política**: Revisar y actualizar la política de seguridad al menos una vez al año o cuando se introduzcan cambios significativos en la infraestructura o normativas.

Esta política de seguridad en la red está diseñada para proteger a los usuarios de la empresa, asegurando la privacidad de sus datos y un entorno de trabajo seguro y confiable.