SEGURIDAD DE LA RED Y CONTROLES PARENTALES

En cumplimiento de lo establecido en la Resolución CRC 5050 de 2016 y demás normas que la modifiquen o complementen, SERVICIOS DIGITALES MIRAFLORES CONECTA S.A.S. presenta el siguiente documento técnico, el cual expone las acciones adoptadas para garantizar la seguridad de la red, la protección de los usuarios frente a contenidos inapropiados y los mecanismos de control parental aplicables.

1.1. MEDIDAS ADOPTADAS POR SERVICIOS DIGITALES MIRAFLORES CONECTA S.A.S. PARA GARANTIZAR LA SEGURIDAD DE LA RED

SERVICIOS DIGITALES MIRAFLORES CONECTA S.A.S. ha adoptado diversas medidas para garantizar la seguridad de la red y cumplir con la Resolución 5050 de la CRC. Se implementaron sistemas de autenticación multifactorial y control de acceso robusto para asegurar que solo los usuarios autorizados puedan acceder a los sistemas críticos. Además, se instalaron firewalls avanzados y sistemas de detección y prevención de intrusiones (IDS/IPS) para proteger la infraestructura de la red. Todo el tráfico sensible se cifra mediante protocolos seguros como SSL/TLS, tanto en tránsito como en almacenamiento, garantizando la confidencialidad de los datos. La empresa cuenta con un plan de respuesta ante incidentes documentado, con procedimientos claros para identificar, contener y mitigar cualquier incidente de seguridad, y notificando a las autoridades pertinentes en caso de incidencias graves. Se realizan evaluaciones periódicas de riesgos y escenarios de vulnerabilidades para detectar y mitigar posibles amenazas. SERVICIOS DIGITALES MIRAFLORES CONECTA S.A.S. cumple con la Ley 1581 de 2012 sobre protección de datos personales, asegurando que los datos no se difunden con los protegidos, y ha implementado soluciones de filtrado para bloquear contenidos ilegales o inapropiados. La empresa también realiza auditorías de seguridad internas y externas para verificar el cumplimiento normativo, y mantiene programas de capacitación continua para todo el personal en seguridad cibernética y buenas prácticas. Además, se implementaron soluciones avanzadas de mitigación de ataques DDoS para asegurar la continuidad del servicio. Con estas medidas SERVICIOS DIGITALES MIRAFLORES CONECTA S.A.S. garantiza un entorno

seguro y conforme con la normativa vigente, protegiendo tanto la infraestructura de red como la privacidad de los usuarios. Diseñados para obtener información personal o financiera del usuario; la exposición a malware y virus, programas maliciosos que pueden dañar equipos, robar información o controlar dispositivos de forma remota; y finalmente, la adicción digital, caracterizada por el uso excesivo e incontrolado del internet, especialmente en videojuegos o redes sociales, afectando negativamente el rendimiento académico, las relaciones sociales y la salud mental. En respuesta a este panorama, SERVICIOS DIGITALES MIRAFLORES CONECTA S.A.S. comprometida con la seguridad digital, promueve el uso consciente y responsable del servicio de internet, e implementa acciones orientadas a sensibilizar y acompañar a sus usuarios en la adopción de prácticas y herramientas tecnológicas que contribuyan a un entorno digital más seguro, especialmente para los niños, niñas y adolescentes.

1.2. SEGURIDAD DEL CORE DE LA RED

SERVICIOS DIGITALES MIRAFLORES CONECTA S.A.S. ha implementado medidas específicas para proteger el core de la red, que es esencial para el funcionamiento de sus servicios de telecomunicaciones. Este componente clave, encargado de gestionar el tráfico de datos y controlar las conexiones dentro de la red, cuenta con mecanismos de redundancia y alta disponibilidad para garantizar la continuidad del servicio en caso de fallos o incidentes. El acceso al core está restringido a personal autorizado y capacitado, mediante controles estrictos tanto físicos como remotos. Además, las comunicaciones dentro del core se cifran utilizando protocolos seguros, lo que asegura la integridad y confidencialidad de los datos en todo momento. El monitoreo continuo del core permite detectar y mitigar amenazas o fallas rápidamente, asegurando que la red funcione de manera eficiente y sin interrupciones. Estas medidas refuerzan la seguridad del core de la red de SERVICIOS DIGITALES MIRAFLORES CONECTA S.A.S., alineándose con las mejores prácticas del sector y el cumplimiento de la Resolución 5050 de la CRC.

2. ACCIONES QUE DEBE TOMAR EL USUARIO PARA GARANTIZAR LA SEGURIDAD EN LA RED

Para garantizar la seguridad en la red y proteger tanto la información personal como la integridad de los dispositivos conectados, los usuarios deben asumir un rol activo en la implementación de prácticas responsables y alineadas con los estándares actuales de ciberseguridad. Una de las principales recomendaciones es el uso de contraseñas robustas y únicas para cada servicio digital, combinando letras mayúsculas, minúsculas, números y caracteres especiales, además de actualizar dichas contraseñas periódicamente. Esta medida debe complementarse con la activación de mecanismos de autenticación multifactor (MFA), los cuales añaden una capa adicional de seguridad mediante el uso de códigos temporales, aplicaciones de autenticación o dispositivos físicos de verificación. Del mismo modo, se debe prestar especial atención a la seguridad de la red Wi-Fi doméstica, asegurándose de que el router esté configurado con protocolos de cifrados seguros como WPA3, cambiando el nombre y contraseña predeterminados, y limitando el número de dispositivos conectados. En caso de necesitar conectarse a redes públicas o abiertas, es fundamental utilizar una VPN (Red Privada Virtual), que permite cifrar todo el tráfico y proteger los datos del usuario frente a posibles interceptaciones. Por otro lado, es imprescindible mantener todos los dispositivos actualizados, incluyendo computadores, teléfonos móviles, tabletas y equipos IoT (como cámaras, asistentes virtuales o televisores inteligentes), instalando las actualizaciones de seguridad que los fabricantes liberan periódicamente para corregir vulnerabilidades. El uso de software de seguridad confiable, como antivirus, antimalware y cortafuegos personales, también es esencial para detectar y bloquear amenazas en tiempo real. En cuanto al comportamiento digital, el usuario debe estar alerta ante posibles ataques de phishing y suplantación de identidad, evitando abrir enlaces o archivos adjuntos de correos electrónicos sospechosos, verificando la autenticidad de las fuentes, y nunca proporcionando información confidencial a través de canales no oficiales o inseguros.

Asimismo, se recomienda deshabilitar funciones innecesarias en los dispositivos, como la compartición automática de archivos, conexiones remotas o el Bluetooth cuando no esté en uso, ya que estas funciones pueden ser explotadas por atacantes. Una buena práctica adicional es la realización

frecuente de copias de seguridad de la información crítica, ya sea en dispositivos físicos externos o en servicios de almacenamiento en la nube, asegurándose de que dichos respaldos estén cifrados y protegidos con acceso restringido. También se debe realizar un monitoreo periódico del tráfico de red doméstico y de los dispositivos conectados, a fin de identificar accesos no autorizados o comportamientos anómalos. Este monitoreo puede realizarse desde la interfaz administrativa del router o con herramientas especializadas. Finalmente, los usuarios deben adoptar una cultura de educación continua en ciberseguridad, actualizándose frente a las nuevas formas de amenazas y reforzando la conciencia digital en su entorno familiar, especialmente con menores de edad, quienes requieren orientación adicional para navegar de forma segura. Estas acciones, aunque sencillas en su mayoría, tienen un impacto significativo en la protección de los entornos digitales personales y familiares. Adoptarlas de manera consistente contribuye no solo a la defensa individual, sino también a la integridad general de la red del proveedor y al cumplimiento de las disposiciones legales vigentes en materia de seguridad digital, como las establecidas por la Resolución 5050 de la CRC y la Ley 1581 de 2012. La seguridad en la red es una responsabilidad compartida entre el prestador del servicio y el usuario final, por lo tanto, el compromiso activo del usuario es indispensable para construir un ecosistema digital más confiable y resiliente frente a las amenazas actuales. Para activar y configurar el control parental en los sistemas operativos Windows 7, 8, 8.1 y 10, el usuario administrador debe seguir procedimientos específicos adaptados a cada versión del sistema.

En Windows 7, el proceso consiste en:

a) Hacer clic en el botón Inicio y acceder al Panel de control;
b) Seleccionar la opción “Cuentas de usuario y protección infantil” y luego “Control parental”;
c) Elegir una cuenta estándar existente o crear una nueva para el menor;
d) Activar el control parental marcando “Activado, aplicar la configuración actual”;
e) Establecer restricciones como límites de tiempo, bloqueo de juegos por clasificación y selección de programas permitidos;
f) Guardar los cambios.

En Windows 8 y 8.1, donde se incorpora la herramienta “Seguridad Familiar”, se debe:

a) Ingresar al Panel de control, seleccionar “Cuentas de usuario y protección infantil” y hacer clic en “Configurar seguridad familiar para cualquier usuario”;
b) Elegir o crear una cuenta estándar para el menor;
c) Activar la función de Seguridad Familiar;
d) Vincular la cuenta del menor a una cuenta Microsoft para acceder a funciones avanzadas;
e) Configurar desde el portal familia.microsoft.com filtros web, límites de uso, control de aplicaciones y generación de informes de actividad;
f) Confirmar la configuración y verificar el correcto funcionamiento.

En Windows 10, el control parental se gestiona en su totalidad mediante Microsoft Family Safety, y el procedimiento es:

a) Ir a Configuración > Cuentas > Familia y otros usuarios;
b) Hacer clic en “Agregar un miembro de la familia” y seleccionar “Agregar un menor”;
c) Ingresando su correo electrónico Microsoft o creando uno nuevo;
d) Aceptar la invitación desde la cuenta del menor;
e) Acceder al portal web familia.microsoft.com para gestionar filtros de contenido, límites de tiempo por dispositivo y aplicación, restricciones de juegos y aplicaciones según la edad, revisión de historial de actividad y control de compras;
f) Guardar la configuración y realizar seguimiento regular.