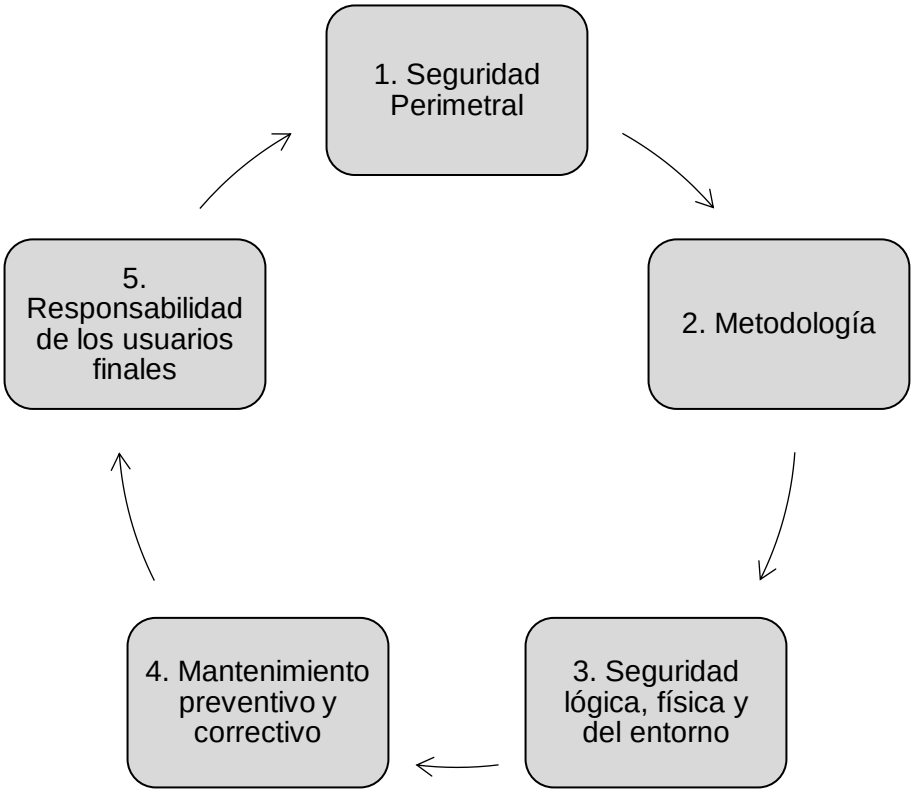
PRESENTACIÓN

Dado el valor de los datos personales, en tanto vinculados con los derechos de las personas y , de la información institucional como insumo indispensable en la gestión de los procesos de calidad educativa, bajo normas de protección de derechos de autor y la amenaza que los unos y los otros sufren de ser accezados de manera ilegal, distorsionada o para fines delincuenciales, el Colegio de la Presentación de Piedecuesta, adopta, actualiza, difunde y consolida la Política de Seguridad Perimetral de acuerdo con lo estipulado en los documentos Conpes correspondientes. Por lo cual diagnostica e identifica los riesgos posibles en la recepción, custodia, disponibilidad del Ecosistema Tecnológico, actualización, consolidación y regulación bajo los estándares de la norma de Seguridad de Información ISO 27001 de 2013 y la Ley de Protección de Datos Personales 1581 de 2012.

MODELO DE LA POLÍTICA DE SEGURIDAD PERIMETRAL



1. SEGURIDAD PERIMETRAL

La protección o coraza del Ecosistema Tecnológico permite proteger la información sensible y los equipos activos de la red de datos institucionales. Esto implica que cada paquete de tráfico transmitido debe ser direccionado, analizado, aceptado y/o rechazado en función de su potencial de riesgo a través de un medio óptimo, adopta las siguientes prácticas:

- Diseño e implementación de cableado estructurado.
- Segmentación lógica de la red de datos.
- Directrices y permisos de accesos.
- Corta fuego.
- Configuración de los equipos activos de la red.
- Direccionamiento IP.
- Capacitación al usuario final sobre prácticas sanas de interacción con el Ecosistema Tecnológico.

2. METODOLOGÍA

La automatización de los servicios prestados se reconoce como un activo valioso para el colegio, es por ello, que se establecen estrategias tecnológicas sistemáticas que permiten el control y administración de los datos de manera efectiva, gestión de los componentes de red, protocolos de comunicaciones y conductas adecuadas que impacten favorablemente a la comunidad educativa plasmadas en el Plan de Mantenimiento Tecnológico.

3. SEGURIDAD LÓGICA, FÍSICA Y DEL ENTORNO

La seguridad perimetral establece los controles necesarios para asegurar la infraestructura lógica y física de la red de datos y el Ecosistema Tecnológico del colegio.

3.1 ÁREAS LÓGICAS SEGURAS

Se dispone en el colegio de espacios físicos dentro de los cuales se garantiza la protección y resguardo de los equipos activos de la red, se limita el acceso a estos solo al personal autorizado para evitar así daños e interferencias en el normal funcionamiento del servicio. En las áreas seguras se encuentran los servidores, rack, switch, UPS, consolas de sensores de humo, Access Paint, consola del circuito cerrado de televisión y terminal del proveedor del servicio de internet.

3.2 PROMOCIÓN DE BUENAS PRÁCTICAS EN EL USO DE LOS EQUIPOS

El uso cotidiano de las estaciones de trabajo, hace que estas se llenan de cookies, archivos temporales y otro tipo de información que con el paso del tiempo ralentizan el funcionamiento del equipo, para esto, existen algunas actividades que si se ejecutánd en forma periódica mantienen de manera óptima las estaciones de trabajo, es por ello que se establece:

- Borrar la memoria caché de los navegadores regularmente para minimizar riesgos de vulnerabilidad y maximizar la rapidez de carga de la información.
- Instalar programas seguros y gratuitos para operaciones automáticas.

- Limitar la descarga de software, películas, spotify y videos musicales, entre otros, a personal no autorizado de acuerdo a su función y rol dentro del colegio.

3.3 ÁREAS FÍSICAS SEGURAS

Los requisitos para la seguridad física deben tener en cuenta los niveles de protección del perímetro de las instalaciones o elementos que contienen la información a proteger, se destacan:

- Alarmas con sistema de protección contra fuego de acuerdo con la legislación vigente.
- Cerraduras en todos los espacios donde residan dispositivos electrónicos, cuartos de telecomunicaciones y oficinas, entre otros.
- Protocolos de información para los colaboradores que acceden a los centros de datos los procedimientos de seguridad y emergencia con acceso específicos para la función realizada.
- Supervisión del personal externo autorizado para reparaciones locativas o procedimientos administrativos propios de la red de datos. Se deben supervisar constantemente por el líder de sistemas, se asegura que los accesos a otras áreas estén bloqueados y que todo el cableado esté seguro. Se aconseja realizar una inspección física de las instalaciones al finalizar los trabajos.
- Los derechos de acceso deben revisarse periódicamente y revocar los permisos según corresponda.
- Revisar las zonas seguras a la finalización de las visitas.
- Prohibir el uso de móviles y/o cámaras a no ser que estén expresamente autorizados dentro de la zona segura.
- Adoptar medidas de protección contra daños eléctricos con fuentes de alimentación reguladas, líneas de alimentación separadas y respaldadas.
- Control medioambiental para cumplir con las especificaciones del fabricante en cuanto a condiciones de humedad, temperatura, protección contra polvo o materiales que puedan dañar los equipos tecnológicos.
- Los cables de potencia deben estar separados de los cables de comunicaciones para evitar interferencias.
- Como medidas adicionales se debe realizar barridos técnicos de los cables de comunicación para dispositivos no autorizados conectados a la red de datos.
- El cableado alrededor de las salas de servidores y centros de datos deben estar aislado de forma segura para evitar la conexión de dispositivos no autorizados.
- Prever medidas de protección ante desastres naturales, incendios, asonadas y eventos de orden público.

4. MANTENIMIENTO PREVENTIVO Y CORRECTIVO

El mantenimiento preventivo y correctivo es la adopción de controles para garantizar que los equipos de cómputo y/o elementos activos de la red se mantengan adecuadamente garantizando su disponibilidad del mayor tiempo posible. Se diseña un Plan de Mantenimiento que involucre las partes interesadas, entre ellas, la coordinación de comunicaciones, coordinación de sistemas, coordinación administrativa y financiera, líderes de sistemas u otra instancia que se requiera. Para ello se debe tener presente:

- Hoja de Vida del equipo de cómputo y/o elemento activo de red.
- Mantenimiento preventivo y/o correctivo de los de equipos de cómputo y elementos activos de la red realizado solo por el personal autorizado.
- Realización de copias de seguridad sistemáticas de la información para evitar pérdida de los datos por eventos fortuitos.
- Remisión de los equipos en beneficio de garantía al servicio especializado, por ningún motivo debe realizar algún tipo de mantenimiento correctivo que llegase a afectar la misma.

4.1 RETIRO DE BIENES

Para el retiro de un equipo de cómputo, elemento activo de red o equipo de comunicaciones, entre otro, se debe diligenciar el formato R-AF-M04 SALIDA DE ACTIVOS FIJOS, el cual permite llevar un registro causal y de debido proceso.

Para el control y movimiento de un equipo de cómputo, elemento activo de red o equipo de comunicaciones, entre otros, se debe diligenciar el formato R-GS-03 Vs. 01 PLANILLA DE MOVILIDAD EQUIPOS, el cual permite llevar un registro causal y de debido proceso.

4.2 REUTILIZACIÓN DE EQUIPOS DE CÓMPUTO

Los equipos averiados deben estar sujetos a una evaluación de riesgo realizada por el líder de sistemas antes de disponer de los mismos para una reparación o para dar de baja, activando el siguiente protocolo:

- Realizar copia de seguridad de toda la información existente.
- Formatear e instalar el sistema operativo, paquete ofimático, antivirus, herramientas administrativas y demás aplicaciones propias de la gestión realizada por el usuario final.
- Restablecer la copia de seguridad garantizando la apertura de los documentos con sus respectivos programas.
- Si definitivamente el equipo esta averiado, se procederá a darlo de baja conservando aquellas piezas que sirvan para repotenciar otros equipos como memoria RAM, Disco Duro, Unidad DVD, teclados, mouse y pantallas, entre otros, notificando a rectoría para continuar con el debido proceso.

4.3 ELIMINACIÓN DE EQUIPOS

Los equipos después de su vida útil de deben aislar, custodiar y garantizar su disposición final en los centros autorizados para tal fin, donde prevalezca siempre el cuidado y protección al medio ambiente.

5. RESPONSABILIDAD DE LOS USUARIOS FINALES

Los actores principales del Ecosistema Tecnológico hacen referencia a los usuarios finales de las partes interesadas, donde se destacan los colaboradores del colegio como ejes articuladores de procesos operativos, académicos, administrativos y directivos, en razón de ello, se convierten en unidades dinamizadoras del Ecosistema Tecnológico centrando su atención en prácticas saludables de interacción informática.

5.1 USO DE DISPOSITIVOS PERSONALES

El uso de dispositivos personales por parte de los colaboradores como portátiles, tabletas y celulares en el lugar de trabajo con el objeto de su práctica laboral con acceso a recursos del colegio tales como correos institucionales, bases de datos, software o aplicaciones para análisis y procesamiento de la información benefician la independencia en la toma de decisiones y mejoran la experiencia final de usuario, no obstante, requieren atenerse a las siguientes consideraciones:

- Aceptar y estar de acuerdo con la Política de Seguridad Perimetral establecida por el colegio.
- Actitud asertiva y consciente del uso de la red de datos.
- Disponer de un antivirus debidamente configurado y actualizado.
- Establecer mecanismos para actualización tanto del sistema operativo, como de las aplicaciones relacionadas con la seguridad.
- Impedir guardar de forma automática las credenciales de acceso asociadas a las herramientas del colegio desde el dispositivo.
- Tener consciencia de navegación segura.

5.2 CONTRASEÑAS ROBUSTAS

Se recomienda los siguientes aspectos fundamentales en la creación de contraseñas:

- Longitud mínima de 8 caracteres.
- Se sugiere combinación alfanumérica con caracteres especiales (@, *, %, &, $, #).
- Preferiblemente no usar fechas especiales como nacimiento, cumpleaños o aniversario.
- Se recomienda no guardar las contraseñas, ni tener activas las opciones de autocompletado en los equipos de cómputo, sobre todo en aquellos quipos que no son de nuestro uso personal.
- Se sugiere cambiar la contraseña con regularidad.

5.3 ADMINISTRACIÓN DE CREDENCIALES DE ACCESO

Los usuarios de la comunidad educativa acuerdo con su naturaleza de trabajo o rol en el sistema, tienen acceso a diferentes instancias del Ecosistema Tecnológico a través de diversas credenciales, entre ellas:

- Ecosistema Educa
- Plataforma Arukay
- Presentación virtual, y/o
- Aplicaciones especializadas

Ante el retiro o entrega de cargo de un colaborador, el líder de sistemas realiza el cambio de las contraseñas de acceso a todo el Ecosistema Tecnológico.

En caso de que el cargo a entregar fuese del líder de comunicaciones y/o sistemas, en las actas de entrega debe quedar constancia de los usuarios y las contraseñas de las distintas plataformas

administrables, entre ellas: servidores, router, DNS, web site, Google Workspace, Simat, Presentación Virtual, Arukay, Educa Norma y redes sociales, entre otras.

Revisión de permisos: Los derechos de acceso deben revisarse periódicamente y revocarse según corresponda.

6. GLOSARIO DE TÉRMINOS

Administrador de Red: Persona capacitada y especializada en gestionar los recursos de red informática.

Autenticación: Es situación en la cual se puede verificar que un documento o dato pertenece a quien dice pertenecer, en el Ecosistema Tecnológico, se realiza mediante un usuario y una contraseña.

Botnet: Software malicioso que permite su control remoto, obligándoles a enviar spam, propagar virus o realizar ataques que impiden el servicio a otros equipos sin el conocimiento o el consentimiento de los propietarios reales de los equipos.

Cableado Estructurado: Tendido de cables de par trenzado, coaxial o fibra óptica, debidamente certificado y etiquetado.

Control de Acceso: Es la administración correcta de los usuarios que acceden a los servicios de red.

Confidencialidad: Protección de la información que los usuarios seguros cursan dentro de la red de datos ante usuarios no autorizados.

Cuarto de Comunicación: Es el área dedicada al alojamiento exclusivo de equipos informáticos asociado al cableado de telecomunicaciones.

Datos: Conjunto de información lógica software que viaja través de la red de datos.

Dirección IP: Etiqueta numérica compuesta por cuatro números enteros entre 0 y 255 el cual es único e identifica al equipo dentro de la red.

Disponibilidad: Conjunto de elementos ofrecidos a nivel de hardware y software al servicio de los usuarios finales.

Ecosistema Tecnológico: La interacción de todos los componentes tecnológicos que intervienen en el hacer y quehacer del colegio, así mismo, hace referencia a todas las plataformas software institucionales.

Hardware: Elementos físicos de un sistema informático, es decir, cableado estructurado, monitores, CPU, dispositivos de almacenamiento, tarjetas de red u otros dispositivos de entrada – salida de datos.

Identificación: Se denomina identificación al momento en que el usuario se da a conocer en un sistema informático a través del usuario y contraseña.

Integridad: En la protección de los datos, permite asegurar que la información no presenta adulteración y la transmisión no incurre en alteración, ni envíos no autorizados o accidentales que pueden ocurrir dentro de la red.

LAN: Red de área local.

Malware: Programas de software informático (gusanos, troyanos, adware, keylogger y dialer, entre otros) que se instalan sin el conocimiento ni la autorización de la víctima y ejecutan acciones dañinas en la computadora, generalmente se sitúan de forma adicional cuando se instalan aplicaciones gratuitas de internet.

Ransomware: Ataque que consiste en el cifrado de la información conocido como secuestro, las víctimas de este ataque son extorsionadas solicitando el pago de dinero para recuperar información sensible preferiblemente con dinero digital en transacciones anónimas y difíciles de rastrear.

Responsabilidad: Seguimiento y correcto almacenamiento de todas las actividades seguras, accidentales y no autorizadas que se den dentro de la red.

Software: Conjunto de programas lógicos que hacen funcionar el hardware, abarcan los sistemas operativos, el software ofimático y los drivers, entre otros.

Subred: Porción de la red, que constituye una nueva red lógica.

Usuario: Persona que utiliza los recursos de la red de datos y el Ecosistema Tecnológico, previo a su autenticación y registro dentro del sistema.

VLAN (Virtual LAN): También conocidas como redes de área local virtuales, es una tecnología de redes que nos permite crear redes lógicas independientes dentro de la misma red física.

WAN: Red de área global.

Zona desmilitarizada – DMZ: Sector de la red donde se encuentran alojados los servidores o acceso sensible a dispositivos activos de la red.

Fecha	Descripción de Cambio	Responsable
22 de noviembre de 2022	Se realiza ajuste detallado del documento base Política de Internet y Seguridad Perimetral reorganizando la información en cinco componentes: a) Seguridad Perimetral, b) Metodología, c) Seguridad lógica, física y del entorno, d) Mantenimiento preventivo y correctivo, y e) Responsabilidad de los usuarios finales. Se realiza corrección de estilo gramatical. Se cambia el nombre a Política de Seguridad Perimetral.	Luz Mary Díaz Mahecha