



POLÍTICA DE SEGURIDAD DE LA INFORMACION

Tiene como fin definir y reglamentar las normas generales de la seguridad informática, así como los procedimientos para proteger, preservar y administrar la información y los activos informáticos del Colegio de cara a las amenazas informáticas internas o externas.

ALCANCE Y RESPONSABILIDAD

La política de seguridad de la información está dirigida a personal docente, personal administrativo, estudiantes, contratistas, terceros, aprendices, que de manera directa o indirecta hagan uso de la información que gestiona el colegio, es cumplimiento obligatorio y aplica para todo el personal del colegio.

La política tendrá seguimiento, gestión, monitoreo y/o auditoría con base a la norma ISO/IEC 27001:2013 bajo la guía de controles ISO/IEC 27002:2013.

- El jefe de Talento Humano cumple la función de informar a todo el personal que se vincula contractualmente con el colegio, de las obligaciones respecto del cumplimiento de la Política de Seguridad de la Información.
- El líder de Sistemas deberá seguir y adoptar los lineamientos de la presente política y cumplir los requerimientos que en materia de seguridad de la información se establezcan para la operación, administración, comunicación y mantenimiento de los sistemas de información y los recursos tecnológicos del colegio.
- El jefe de Compras e Inventarios tiene la responsabilidad de mantener el inventario completo y actualizado de los recursos tecnológicos del colegio.
- Los estudiantes del colegio deben leer y conocer la política de seguridad de la información y los lineamientos de uso de las salas de tecnología.
- Todos los usuarios externos y personal de empresas externas deben estar autorizados por el área de Talento Humano y supervisados por el líder de Sistemas quien será el encargado del control y vigilancia del uso adecuado de la información y los recursos Tecnológicos del Colegio.
- Es responsabilidad de todo el equipo administrativo y docente velar por el buen uso de los recursos tecnológicos que el colegio pone a su disposición.

SEGURIDAD EN LOS EQUIPOS INFORMATICOS

Los servidores que contengan información y servicios institucionales deben ser mantenidos en un ambiente seguro, utilizando software de protección de intrusos (firewall), control de acceso activo (contraseñas robustas y seguras), deben estar soportados por sistemas eléctricos regulados y soportados mediante el uso de UPS.

Los computadores e infraestructura tecnológica deben estar correctamente asegurados y gestionados por personal autorizado del colegio, el cual, debe estar capacitado acerca del



contenido de esta política y de las responsabilidades personales en el uso y administración de la información institucional.

INSTALACIÓN DE SOFTWARE

Toda instalación de software que se realice en los servidores, computadores o sistemas informáticos del Colegio debe contar con la aprobación formal de las directivas del colegio. El líder de Sistemas del colegio deberá desinstalar de los sistemas informáticos cualquier software no autorizado y que atente contra la seguridad de la información.

Para evitar la instalación de software no autorizado en la infraestructura tecnológica del colegio, los computadores y servidores están protegidas por un directorio activo que bloquea la descarga e instalación de cualquier tipo de software.

GESTION A INCIDENTES DE SEGURIDAD

El personal del Colegio debe reportar con diligencia, prontitud y responsabilidad presuntas violaciones de seguridad al responsable de Sistemas, quien debe garantizar las herramientas informáticas para que formalmente se realice el reporte e investigación de incidentes de seguridad.

PROTECCIÓN CONTRA SOFTWARE MALICIOSO, VIRUS Y ATAQUES

Todos los servidores y computadores deben ser protegidos por software antivirus con capacidad de actualización automática en cuanto virus, software malicioso o ataques intrusivos, en caso de encontrar eventos inusuales en los sistemas informáticos, servidores o computadores del colegio por causa de virus o software malicioso deberá ser reportado a las directivas del colegio.

CONFIGURACIONES DE RED Y ACCESO A INTERNET

La configuración de servidores, enrutadores, switches y otros dispositivos de seguridad de red debe ser administrada, documentada y custodiada por el líder de Sistemas.

Todos los servidores, computadores, impresoras del Colegio se conectan a través de la red LAN institucional. Todo equipo debe ser revisado y aprobado por el área de Tecnología antes de conectarse a cualquier nodo de la Red LAN.

Las conexiones a Internet e intranet están filtradas a través del sistema de seguridad perimetral Firewall, instalado en uno de los servidores del Colegio y el acceso a las conexiones wifi del colegio están protegidas bajo los sistemas de cifrado WPA y WPA2 ENTERPRISE CISCO.

CORREO ELECTRÓNICO

Las normas generales de uso responsable del correo electrónico institucional, así como los protocolos de asignación y desactivación de cuentas de correo electrónico están consignadas en nuestra **política de uso del correo electrónico institucional**.

COPIAS DE SEGURIDAD

Toda información que pertenezca a los activos de información institucional o que sea de interés para un proceso operativo o de misión crítica debe ser respaldada por copias de seguridad. Dicho procedimiento debe incluir las actividades de almacenamiento de las copias en sitios seguros. Las dependencias del colegio deben realizar pruebas controladas para asegurar que las copias de seguridad pueden ser correctamente leídas y restauradas. La creación de copias de seguridad de archivos usados, custodiados o producidos por usuarios individuales es responsabilidad exclusiva de dichos usuarios.

“Formamos para la fe, la vida, la estudiosidad y la vida en comunidad”

“We educate for faith, life, studiousness and community”



El área de Sistemas se encarga de dar cumplimiento al cronograma de copias de seguridad establecido por la institución y es responsable de su custodia.

PLATAFORMAS TECNOLÓGICA EN LA NUBE

El colegio utiliza el servicio e infraestructura tecnológica de Google, a través del producto G Suite for education, para el uso de los siguientes servicios: correo electrónico institucional Gmail, Drive, calendario, documentos, hojas de cálculo, presentaciones, formularios, sites y Google Classroom asociados al dominio institucional www.santotomas.edu.co.

El detalle de la condiciones de uso de las herramientas que incluye Google Apps for Education, puede visitar: <https://www.google.com/intl/es-419/edu/products/productivity-tools/>.

Elaboró	Revisó	Aprobó
Carlos Ángel Rocha Líder de Sistemas	Juan Carlos Pachón Gestión y Calidad	Comité de Gestión
2024-09-22	2024-09-26	2024-09-27