

POLÍTICA DE SEGURIDAD INFORMÁTICA



1. Alcance y propósito

El alcance de este documento y cualquier norma institucional relacionada a la seguridad informática se suscribe a todas las dependencias académicas y administrativas del LICEO SANTA BERNARDITA y que se aplica a toda la comunidad educativa, incluyendo personal administrativo, personal docente y estudiantes.

El propósito de esta política es definir y reglamentar las normas generales de la seguridad informática, así como los procedimientos para proteger, preservar y administrar la información del LICEO SANTA BERNARDITA frente a las amenazas informáticas internas o externas.

2. Responsabilidad

La Política de seguridad informática es de aplicación obligatoria para todo el personal del LICEO SANTA BERNARDITA, cualquiera sea su situación contractual, la dependencia a la cual se encuentre adscrito y el nivel de las tareas que desempeñe.

Todos los encargados en esta área, deben seguir los lineamientos de la presente política y cumplir los requerimientos que en materia de seguridad informática se establezcan para la operación, administración, comunicación y mantenimiento de los sistemas de información y los recursos de tecnología de la entidad.

Los estudiantes deben leer y conocer la política de seguridad informática, así como la política de uso de las salas de tecnología durante cada año académico, con el apoyo en las clases de tecnología y la publicación en línea para ser consultada. El manual de convivencia debe contemplar procesos y sanciones disciplinarias para los casos en que se presente usos de información que violen los términos y condiciones.

Todos los usuarios externos y personal de empresas externas deben estar autorizados por un miembro del personal del colegio quien será responsable del control y vigilancia del uso adecuado de la información y los recursos institucionales de acuerdo a la política de seguridad informática.

También es responsabilidad de todo el equipo docente velar por el buen uso de los recursos tecnológicos que el colegio pone a su disposición. (No desconecte los cables o dispositivos de los equipos, ni los cambie de sitio.

3. Políticas de uso de las salas de tecnología

1. La institución ofrecerá a los usuarios de las salas de informática los recursos de hardware, software y conectividad disponibles, para que sirvan como apoyo en sus actividades académicas. El uso académico prima sobre cualquier otra utilización.

2. La administración de los recursos de las salas de informática es responsabilidad de los profesores de informática. En caso de utilización de las salas por parte de otra asignatura, el grupo de estudiantes estará en todo momento bajo la responsabilidad del profesor acompañante.

3. Con el fin de favorecer el uso adecuado de los computadores, se sugiere evitar la búsqueda abierta en Internet, la orientación y acompañamiento del profesor es muy importante para evitar distracciones durante el desarrollo de las actividades.

4. Los usuarios únicamente pueden utilizar los servicios para los cuales están autorizados. Sin la debida autorización, no se permite copiar software o modificar los archivos que se encuentren allí. Para cualquier cambio en el sistema se debe solicitar permiso al Departamento de Tecnología o al docente responsable de la sala.

5. Bajo ninguna circunstancia se podrá utilizar el nombre (login), código o clave de acceso (password) de otro usuario. Cada usuario debe permitir su plena identificación en la Red de la Institución. (Se podría restringir el uso por parte del administrador del sistema).

6. No se permite el ingreso y/o consumo de alimentos (incluyendo bebidas) dentro de las salas de tecnología. Los profesores deben ser particularmente modelos en este sentido.

7. En caso de pérdida, daño o deterioro de los equipos usados, el usuario debe reportar inmediatamente esta situación al profesor que se encuentre en la sala para proceder a su reparación. Si se determina que el daño fue causado por mal manejo o maltrato del equipo, el usuario responsable debe encargarse de la reparación del mismo.

8. El colegio dispone del uso de un equipo por estudiante por tal razón es importante que cada estudiante ocupe su espacio sin interferir con el trabajo de los demás estudiantes.

9. Es importante que exista un ambiente de buen trato dentro de la sala, utilizando un lenguaje adecuado al comunicarse de forma verbal o a través del computador.

4. Seguridad en los equipos

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 seguras) y deben ser alimentados por sistemas de potencia eléctrica regulados y estar protegidos por UPS.

Las estaciones de trabajo deben estar correctamente aseguradas y operadas por personal de la institución 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. 5. Reporte de incidentes de seguridad

El personal del colegio debe reportar con diligencia, prontitud y responsabilidad presuntas violaciones de seguridad a coordinación, quienes deben garantizar las herramientas informáticas para que formalmente se realice el reporte e investigación de incidentes de seguridad.

6. Protección contra software malicioso y virus

Todos los sistemas informáticos deben ser protegidos por software antivirus con capacidad de actualización automática en cuanto virus y software malicioso. Los usuarios de las estaciones no están autorizados a deshabilitar este control. En caso de encontrar algo inusual en los sistemas informáticos del colegio por causa de virus o software malicioso deberá ser reportado inmediatamente.

7. Instalación de Software

Todas las instalaciones de software que se realicen sobre sistemas del LICEO SANTA BERNARDITA deben ser aprobadas por coordinación. No se permite la instalación de software que viole las leyes de propiedad intelectual y derechos de autor en especial la ley 23 de 1982 y relacionadas. Los profesores del colegio deberán desinstalar de los sistemas informáticos cualquier software no autorizado.

Para evitar la instalación de software no autorizado en las estaciones de trabajo, se dispone de un programa que congela la configuración del sistema a su estado original.

8. 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.

9. 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 y la firma empleada por el personal administrativo y docente; están consignadas en nuestra *política de uso del correo electrónico institucional*.

11. Plataforma tecnológica en la nube

El LICEO SANTA BERNARDITA utiliza la 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.

Para mayor información de las herramientas que incluye Google Apps for Education, puede visitar: <https://www.google.com/intl/es-419/edu/products/productivity-tools/>

12. Intercambio de Información con Organizaciones Externas

Las peticiones de información por parte de entes externos de control deben ser aprobadas por la Rectoría y Gerencia general, y dirigida por dichos entes a los responsables de su custodia.