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 **COLEGIO NUEVA INGLATERRA (INVERBAC S.A)** 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 **COLEGIO NUEVA INGLATERRA (INVERBAC S.A)** frente a las amenazas informáticas internas o externas.

2. RESPONSABILIDAD

La Política de seguridad informática es de aplicación obligatoria para todo el personal del **COLEGIO NUEVA INGLATERRA (INVERBAC S.A)**, cualquiera sea su situación contractual, la dependencia a la cual se encuentre adscrito y el nivel de las tareas que desempeñe.

El Responsable de Sistemas, debe 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.

La Asistente de Recursos Humanos cumplirá la función de notificar a todo el personal que se vincula contractualmente con el colegio, de las obligaciones respecto del cumplimiento de la Política de Seguridad Informática. De igual forma, será responsable de la notificación de la presente política y de los cambios que en ella se produzcan a todo el personal, a través de la suscripción de los compromisos de Confidencialidad.

El Jefe de Compras e Inventarios tiene la responsabilidad de mantener el inventario completo y actualizado de los recursos tecnológicos de la institución.

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 la Dirección Administrativa y Financiera y supervisados por el Responsable de Sistemas quien será el encargado del control y vigilancia del uso adecuado de la información y los recursos de Tecnología e Informática institucionales de acuerdo a la política de seguridad informática.

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. Si necesita ayuda, por favor solicitarla al Técnico de Sistemas y/o al Auxiliar de Logística y Medios Audiovisuales)

3. POLITICAS DE USO DE LAS SALAS DE TECNOLOGIA

a. 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.
b. La administración de los recursos de las salas de informática es responsabilidad de los profesores de Tecnología e 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.
c. 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.
d. 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 Responsable de Sistemas o al docente responsable de la sala.
e. 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).
f. 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.
g. En caso de pérdida, daño o deterioro de los equipos usados, el usuario debe reportar inmediatamente esta situación al docente que se encuentre en la sala para proceder a reportar a través de la plataforma institucional la respectiva solicitud soporte sistemas para el diagnóstico y 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.

h. 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.

i. 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. Adicionalmente, el personal de la institución que tenga acceso a una estación de trabajo debe hacer correcto uso del mismo, como por ejemplo realizando el encendido y apagado del equipo según la capacitación impartida en la inducción, esto con el fin de evitar daños en los mismos.

5. REPORTE DE 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.

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.

Adicionalmente, las salas de tecnología están provistas con un software de congelación de disco el cual evita la instalación de software, almacenamiento de datos, bugs y troyanos.

7. INSTALACIÓN DE SOFTWARE

Todas las instalaciones de software que se realicen sobre sistemas del **COLEGIO NUEVA INGLATERRA (INVERBAC S.A)** deben ser aprobadas por la Alta Dirección. 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. El Técnico 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 las salas de tecnología, se dispone de un programa que congela la configuración del sistema a su estado original. Adicionalmente, las demás estaciones de trabajo están protegidas por un directorio activo que bloquea la descarga e instalación de cualquier software.

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

9. 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 Responsable de Sistemas.

Las estaciones de trabajo del colegio se conectan a través de la red LAN institucional. Todo equipo debe ser revisado y aprobado por el Departamento de Tecnología antes de conectarse a cualquier nodo de la Red LAN.

Las conexiones a Internet están filtradas a través de dos sistemas: un control de contenidos del proveedor de Internet (E.T.B.) y un proxy caché (squid) instalado en uno de los servidores del colegio. El acceso a las conexiones wifi del colegio están protegidas bajo los sistemas de cifrado WPA y WPA2 ENTERPRISE.

10. 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. PLATAFORMAS TECNOLÓGICA EN LA NUBE

El **COLEGIO NUEVA INGLATERRA (INVERBAC S.A)** 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 Dirección Administrativa y Financiera y por la Alta Dirección, y dirigida por dichos entes a los responsables de su custodia.

Siendo el día 27 de Enero del año 2020 se aprueba la presente política,

Por el Gerente General

Dr. Alfredo Barbosa Luque