TRABAJO DE GRADO
Opción Seminario.

Informe técnico – Caso 4:

Colegio Bilingüe Nueva Generación

Corporación Universitaria Remington.
Nombre de la facultad: Ingenierías
Nombre del programa académico: Ingeniería de Sistemas

Nombres de los estudiantes autores del trabajo de grado.

Claudio Guerra Llorente
Jhonatan Smith Mosquera Rivas
David Hansel Mosquera Rodriguez

Jorge Leonardo Ramírez Restrepo - docente del seminario.
Seminario
2026

Tabla de Contenidos

Resumen

Actualmente, las instituciones educativas dependen cada vez más de la tecnología para administrar la información académica y administrativa. Por esta razón, proteger los datos de estudiantes, docentes y padres de familia se ha convertido en una necesidad para evitar pérdidas de información, accesos no autorizados o interrupciones en los servicios.
Este informe presenta un análisis del caso del Colegio Bilingüe Nueva Generación, identificando los principales activos de información, las amenazas y las vulnerabilidades que pueden afectar su funcionamiento. A partir de este diagnóstico, se proponen medidas de seguridad y buenas prácticas basadas en normas y legislación vigente, con el fin de reducir los riesgos y fortalecer la protección de la información institucional.

Palabras clave

Seguridad de la información, ciberseguridad, gestión de riesgos, activos de información y protección de datos.

Marco conceptual y normativo

Conceptos fundamentales de ciberseguridad

La seguridad de la información no es solo instalar antivirus; es una estrategia para proteger los datos más valiosos de una organización. Según la norma **ISO/IEC (2022a)**, esta disciplina se sostiene sobre tres pilares: confidencialidad, integridad y disponibilidad. En el colegio, por ejemplo, la confidencialidad es lo que evita que el historial médico o las notas de un estudiante caigan en manos equivocadas.

Para proteger algo, primero hay que saber qué se tiene. La guía **ISO/IEC (2022b)** define un activo de información como cualquier recurso con valor para la institución. En este caso, un activo es tanto el servidor físico donde guardan los archivos como los usuarios y contraseñas de los papás en la plataforma.

Por otro lado, los sistemas siempre tienen puntos débiles. **Cano (2011)** explica que el riesgo informático aparece cuando una amenaza aprovecha una vulnerabilidad para hacer daño. Un ejemplo claro en el colegio es la vulnerabilidad de tener cuentas activas de profesores que ya no trabajan allí, lo que abre la puerta a un hackeo o sabotaje Para frenar esto, **Amoroso (2013)** define una vulnerabilidad como cualquier falla de diseño o soporte que nos deje expuestos, y propone el uso de controles de seguridad (que son herramientas técnicas o reglas administrativas) para actuar como barreras y bajar el nivel de riesgo.

Finalmente, hay que entender que la tecnología no falla sola; las personas también importan. En su famoso estudio sobre ingeniería social, **Mitnick y Simón (2002)** demostraron que el eslabón más débil siempre es el factor humano. Prácticas como usar memorias USB personales o que los papás compartan sus claves confirman que el verdadero reto del colegio está en educar a su comunidad.

Marco normativo (tabla revisada según normas y aplicabilidad)

Tabla 1. Normatividad aplicable.

Las normas seleccionadas sirven como guía para proteger la información del Colegio

Norma o estándar	*Propósito*	*Aplicabilidad en la organización*
ISO/IEC 27001:2022	Establece los requisitos para un Sistema de Gestión de Seguridad de la Información.	Ayuda a organizar y proteger la información institucional.
ISO/IEC 27002:2022	Presenta controles y buenas prácticas de seguridad.	Orienta la implementación de controles para reducir riesgos.
Ley 1581 de 2012	Protege los datos personales en Colombia.	Garantiza el adecuado tratamiento de la información de estudiantes y padres.
Decreto 1377 de 2013	Reglamenta la Ley 1581.	Define procedimientos para el manejo de datos personales.
Ley 1273 de 2009	Establece los delitos informáticos en Colombia.	Sirve como respaldo legal frente a ataques o accesos no autorizados.

Bilingüe Nueva Generación y reducir los riesgos asociados al uso de la tecnología. La ISO/IEC 27001 y la ISO/IEC 27002 orientan la implementación de controles de seguridad, mientras que la Ley 1581 de 2012, el Decreto 1377 de 2013 y la Ley 1273 de 2009 establecen las obligaciones legales para el tratamiento de datos personales y la prevención de delitos informáticos. Su aplicación contribuye a fortalecer la seguridad de la información y a generar confianza en toda la comunidad educativa.

Marco contextual

Descripción de la organización

El Colegio Bilingüe Nueva Generación es una institución educativa privada que ofrece formación desde preescolar hasta grado undécimo. Cuenta con aproximadamente 1.450 estudiantes y 160 colaboradores. Su actividad principal es brindar educación bilingüe apoyada en herramientas tecnológicas para facilitar los procesos académicos y administrativos.

La institución está organizada en áreas como Rectoría, Coordinación Académica, Tecnología, Talento Humano, Tesorería, Admisiones y Bienestar Estudiantil. Además, dispone de una infraestructura tecnológica compuesta por computadores, plataformas académicas, servidor local, red WiFi, copias de seguridad en la nube y una aplicación para la comunicación con los padres de familia.

Sus principales procesos incluyen la gestión académica, la administración de la información estudiantil, la gestión financiera, el talento humano y la comunicación con la comunidad educativa.

Problemática identificada

Durante el diagnóstico se identificaron varias debilidades en materia de seguridad de la información. Entre ellas se encuentran el uso de aplicaciones de mensajería personal para compartir información institucional, cuentas activas de exdocentes, contraseñas sin cambios periódicos, uso de memorias USB personales y la ausencia de políticas claras para la gestión de incidentes.

Estas situaciones aumentan el riesgo de pérdida o filtración de información y justifican la necesidad de implementar controles y buenas prácticas que fortalezcan la seguridad de los datos y garanticen la continuidad de las actividades del colegio.

Identificación y análisis de activos

Inventario de activos

Tabla 2. Inventario de activos

Activo	*Tipo*	*Descripción*	*Criticidad*
Base de datos de Estudiantes	Información	Contiene datos personales, académicos y disciplinarios.	Alta
Plataforma académica	Software	Permite registrar notas, asistencia y boletines.	Alta
Servidor institucional	Hardware	Almacena la información y los sistemas del colegio.	Alta
Red WiFi institucional	Red	Brinda conectividad a usuarios y equipos.	Media
Copias de seguridad en la nube	Información	Respalda la información para su recuperación.	Alta
Correo institucional	Software	Medio oficial de comunicación interna.	Media

Los activos con mayor criticidad son la base de datos de estudiantes, la plataforma académica, el servidor institucional y las copias de seguridad, ya que contienen información esencial para el funcionamiento del colegio. Si alguno de estos recursos se

ve comprometido, podrían presentarse pérdidas de información, interrupción de las actividades académicas y afectaciones a la privacidad de estudiantes, docentes y padres de familia. Por esta razón, requieren mayores controles de seguridad y monitoreo permanente.

Análisis de amenazas y vulnerabilidades

Tabla 3. Amenazas y vulnerabilidades

Activo	***Amenaza***	***Vulnerabilidad***
Base de datos de estudiantes	Robo o fuga de información	Falta de clasificación de la información y controles de acceso.
Plataforma académica	Acceso no autorizado	Cuentas activas de exdocentes y contraseñas débiles.
Servidor institucional	Ataques de ransomware	Copias de seguridad sin pruebas periódicas y actualizaciones insuficientes.
Red WiFi institucional	Intrusión a la red	Configuración de seguridad y autenticación insuficientes.
Correo institucional	Phishing	Falta de capacitación y de autenticación multifactor.

Análisis

Las situaciones que representan mayor riesgo para el colegio son el acceso no autorizado a la plataforma académica y la posible pérdida de información almacenada en el servidor. Estas amenazas podrían afectar datos personales, calificaciones y documentos institucionales. Además, el uso de dispositivos USB personales y la falta de capacitación en ciberseguridad aumentan la posibilidad de incidentes. Por ello, es importante fortalecer los controles de acceso, actualizar las políticas de seguridad y promover buenas prácticas entre los usuarios para reducir los riesgos.

Análisis y gestión de riesgos

Metodología de análisis

Para evaluar los riesgos del Colegio Bilingüe Nueva Generación se utilizó una metodología basada en la valoración del impacto y la probabilidad de ocurrencia de cada riesgo. El impacto se determinó según las consecuencias que tendría un incidente sobre la información, la continuidad de las actividades y la reputación de la institución. La probabilidad se estimó considerando las vulnerabilidades identificadas y la posibilidad de que una amenaza se materialice.
Con la combinación de estos dos criterios fue posible clasificar los riesgos en niveles bajo, medio y alto, facilitando la priorización de las acciones de seguridad (ISO/IEC, 2022; ISO/IEC, 2022; MinTIC, 2024).

Matriz de riesgos

Tabla 4. Matriz de riesgos

Riesgo	***Impacto***	***Probabilidad***	***Nivel***
Acceso no autorizado a la plataforma académica	Alto	Alto	Alto
Pérdida de información por ransomware	Alto	Medio	Alto
Fuga de datos personales	Alto	Medio	Alto
Infección por malware mediante USB	Medio	Medio	Medio
Interrupción de la red institucional	Medio	Alto	Alto
Phishing a docentes y administrativos			

Análisis de los riesgos prioritarios

Los riesgos con mayor prioridad son el acceso no autorizado a la plataforma académica, la pérdida de información por ransomware, la fuga de datos personales y los ataques de phishing. El acceso no autorizado fue clasificado con impacto alto debido a que podría permitir la modificación de notas, historiales académicos y datos sensibles; su probabilidad es media porque existen cuentas de exdocentes activas y contraseñas

débiles. El ransomware presenta impacto alto por la posible interrupción de las actividades académicas y administrativas, mientras que su probabilidad es media por la ausencia de pruebas periódicas de recuperación. El phishing fue valorado con impacto y probabilidad altos debido al uso intensivo del correo electrónico y la falta de capacitación continua.

Políticas y controles de seguridad

Políticas propuestas

Tabla 5. Políticas de seguridad

Política	***Objetivo***	***Riesgo asociado***
Política de contraseñas seguras	Fortalecer el acceso a los sistemas.	Accesos no autorizados.
Política de copias de seguridad	Garantizar la recuperación de la información.	Pérdida de datos por ransomware.
Política de uso de dispositivos USB	Evitar el ingreso de malware.	Infección de equipos.
Política de gestión de usuarios	Eliminar cuentas inactivas y controlar permisos.	Uso indebido de credenciales.
Política de capacitación	Promover buenas prácticas de seguridad.	Errores humanos y phishing.

Controles propuestos

Tabla 6. Controles de seguridad

Riesgo	***Control***	***Justificación***
Acceso no autorizado	Autenticación de dos factores (2FA).	Aumenta la seguridad de las cuentas.
Pérdida de información	Copias de seguridad automáticas y pruebas de recuperación.	Permite recuperar la información ante incidentes.
Malware	Antivirus actualizado y restricción del uso de USB.	Reduce el riesgo de infecciones.
Phishing	Capacitaciones periódicas al personal.	Disminuye la posibilidad de fraudes y robo de credenciales.
Cuentas inactivas	Revisión periódica de usuarios y permisos.	Evita accesos de personas no autorizadas.

justificación

Las políticas y controles propuestos guardan relación directa con los hallazgos identificados. El uso de aplicaciones de mensajería personal se mitiga mediante la adopción de canales corporativos oficiales; el uso de memorias USB personales se controla con restricciones técnicas y análisis antimalware; las cuentas inactivas se gestionan mediante revisiones periódicas de permisos; y el riesgo de phishing se reduce con campañas de capacitación y autenticación multifactor.

Gestión de incidentes y continuidad del negocio

Para evitar que un ataque informático detenga las clases o la administración del colegio, es necesario mapear los problemas potenciales y definir una ruta rápida de acción.

Tabla 7. Incidentes potenciales

Incidente	***Descripción***	***Impacto***
Infección por Ransomware	Cifrado y secuestro de los archivos de contabilidad y matrículas en el servidor local.	**Alto:** Bloquea la operación de Tesorería y Admisiones de inmediato.
Alteración de Notas	Modificación no autorizada de calificaciones usando cuentas de exdocentes aún activas.	**Alto:** Pérdida de credibilidad institucional y problemas con el Ministerio.
Fuga de Datos Sensibles Datos	Filtración pública de historiales psicológicos o datos de menores desde chats personales.	**Crítico:** Demandas legales directas bajo la Ley 1581 de protección de datos.
Caída de la Plataforma LMS	Indisponibilidad de la plataforma de clases virtuales y tareas durante periodos de exámenes.	**Medio:** Retraso en el calendario académico y quejas de padres de familia.

Tabla 8. Plan básico de respuesta

Fase	***Acción***
Identificación	El técnico de soporte detecta la anomalía o recibe el reporte de los usuarios y notifica al Coordinador de TI.
Contención	Se aíslan las redes Wi-Fi, se desconectan los servidores afectados de internet y se congelan las cuentas comprometidas.
Erradicación	El equipo de TI elimina el malware del sistema, revoca los accesos viejos y parcha la vulnerabilidad explotada.
Recuperación	Se limpian los equipos afectados y se restaura la última copia de seguridad guardada en la nube para volver a operar.

Estrategia de respuesta y continuidad operativa: El Coordinador de TI será responsable de activar el plan de respuesta a incidentes y coordinar las acciones de contención. El equipo de soporte ejecutará las tareas técnicas de aislamiento, erradicación y recuperación. La Rectoría y las áreas administrativas comunicarán las medidas adoptadas a la comunidad educativa. En caso de una afectación grave, los servicios críticos serán restaurados utilizando las copias de seguridad en la nube para garantizar la continuidad operativa del colegio.

Si el colegio llega a sufrir un incidente grave, la prioridad es reaccionar con rapidez para que las actividades no se congelen. Ante un hackeo o pérdida del servidor físico, la institución activaría la continuidad operativa migrando de forma temporal los procesos críticos a la nube. Mientras el departamento de TI trabaja en limpiar y reparar la infraestructura local siguiendo los pasos de contención y erradicación de la tabla, las áreas administrativas y los docentes usarían la aplicación móvil y los respaldos Cloud para seguir atendiendo a los padres y reportando notas. Esto garantiza que el plantel

pueda seguir funcionando y proteja la información sin necesidad de suspender las labores escolares.

Tabla 9. Hallazgos organizacionales

Situación observada	***Riesgo asociado***
Compartición de credenciales de accesos por padres de familia.	Alteración de notas y suplantación de acudientes legales.
Uso de apps de mensajería personal para fines laborales.	Exposición de datos de menores en redes de terceros desprotegidas.

Tabla 10. Recomendaciones de mejora

Hallazgo	***Recomendación***
Compartición de accesos.	Desplegar talleres de concientización y habilitar factor de doble autenticación (2FA).
Uso indebido de canales.	Proveer canales corporativos oficiales y capacitar en el uso del correo institucional.

Fortalecimiento de la cultura organizacional

Las recomendaciones propuestas contribuirían a fortalecer la cultura de ciberseguridad en el Colegio Bilingüe Nueva Generación al promover buenas prácticas entre docentes, estudiantes y personal administrativo. La capacitación constante, el uso de canales oficiales de comunicación y la implementación de mecanismos como la autenticación en dos factores ayudarán a reducir errores humanos y accesos no autorizados. De esta manera, la institución podrá proteger mejor la información que administra y generar mayor confianza en toda la comunidad educativa.

Conclusiones

- El análisis realizado permitió identificar que la información del Colegio Bilingüe Nueva Generación es uno de sus activos más importantes, por lo que requiere medidas de protección que garanticen su confidencialidad, integridad y disponibilidad.

- Se evidenció que varias de las vulnerabilidades encontradas, como el uso de contraseñas débiles, cuentas de exdocentes activas y el uso de dispositivos personales, pueden aumentar el riesgo de incidentes de seguridad si no se implementan controles adecuados.

- La aplicación de normas como la ISO/IEC 27001 y la legislación colombiana sobre protección de datos proporciona una base para fortalecer la gestión de la seguridad de la información y cumplir con las obligaciones legales de la institución.

- La implementación de políticas de seguridad, controles de acceso, copias de seguridad y programas de capacitación contribuirá a disminuir los riesgos identificados y a mejorar la continuidad de las actividades académicas y administrativas.

- Finalmente, fortalecer la cultura de ciberseguridad entre docentes, estudiantes y personal administrativo permitirá que toda la comunidad educativa participe activamente en la protección de la información y en la prevención de futuros incidentes.

Referencias

Congreso de la República de Colombia. (2009). *Ley 1273 de 2009, por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones*.
https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=34492

Congreso de la República de Colombia. (2012). *Ley 1581 de 2012, por la cual se dictan disposiciones generales para la protección de datos personales*.
https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=49981

International Organization for Standardization. (2022). *ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection — Information security management systems — Requirements.*

International Organization for Standardization. (2022). *ISO/IEC 27002:2022 Information security, cybersecurity and privacy protection — Information security controls.*

Ministerio de Tecnologías de la Información y las Comunicaciones. (2024). *Guía de Seguridad y Privacidad de la Información.*
Presidencia de la República de Colombia. (2013). *Decreto 1377 de 2013*.
https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=53646