2024

PLAN DE CIBERSEGURIDAD

UNIDAD EDUCATIVA INTERNACIONAL LICEO IBEROAMERICANO

DATOS DE LA INSTITUCIÓN EDUCATIVA						
Código **AMIE**	**06H00239**	Denominación:	**UNIDAD EDUCATIVA**			
Nombre de la Institución		**INTERNACIONAL LICEO IBEROAMERICANO**				
Ubicación Geográfica	Zona	**3**	Distrito	**06D01**	Circuito	**06D01C10_11**
	Provincia	**CHIMBORAZO**	Canton	**RIOBAMBA**	Parroquia	**VELASCO**
Dirección de la Institución		**CALLE VELOZ 3212 Y VARGAS TORRES**				
Sostenimiento		**PARTICULAR**				
Modalidad		**PRESENCIAL**				
Jornada		**MATUTINA**				
Tipo		**HISPANA**				
Oferta Académica - Número estudiantes		Nivel	Subnivel	Hombres	Mujeres	Total
		Educación Inicial	Inicial1 (0-3 años)			
			Inicial2(3-5 años)	5	8	13
		Preparatoria		7	5	12
		EGB Elemental	Segundo EGB	7	3	10
			Tercero EGB	9	12	21
			Cuarto EGB	6	9	15
		EGB Media	Quinto EGB	7	6	13
			Sexto EGB	5	9	14
			Séptimo EGB	9	7	16
		EGB Superior	Octavo EGB	10	13	23
			Noveno EGB	10	5	15
			Décimo EGB	8	9	17
		Bachillerato	Primero BGU	13	9	22
			Segundo BGU	15	10	25
			Tercero BGU	19	21	40
		Total		130	126	256
Autoridades de la IE		Rector	**Msc. Robert Edisson Frías Bermeo**			
		Vicerrector	**Msc. Edgar Wellington Frías Bermeo**			
		Inspector	**Tlgo. Carlos Darwin Acaro Pérez**			
Nro. Personal		Tipo		Hombres	Mujeres	Total
		Docentes		4	13	17
		Administrativos		0	1	1
		Servicios		0	1	1
		Total		4	15	19
Integrantes del Gobierno Escolar		**Presidenta: Allisson Barrera**				
		Vicepresidente:				
		Secretaria:				
		Tesorero:				
Correo institucional		info@ibero.edu.ec				
Fecha de Elaboración		**30 de abril del 2024**				

Introducción:

En un entorno cada vez más digitalizado, la seguridad de la información se ha convertido en una preocupación crítica para las instituciones educativas. La Unidad Educativa Internacional Liceo Iberoamericano reconoce la importancia de proteger sus activos de información contra las crecientes amenazas cibernéticas y está comprometida a establecer un sólido marco de ciberseguridad para salvaguardar la integridad, confidencialidad y disponibilidad de sus datos.

Este plan de ciberseguridad proporciona una hoja de ruta detallada para fortalecer la postura de seguridad de la institución y mitigar los riesgos asociados con las amenazas cibernéticas. A través de la implementación de políticas, procedimientos y medidas técnicas adecuadas, la Unidad Educativa Internacional Liceo Iberoamericano se esfuerza por garantizar un entorno educativo seguro y protegido para todos los miembros de la comunidad educativa.

Objetivos Generales:

1. Establecer un marco de ciberseguridad integral que proteja los activos de información crítica de la institución contra amenazas cibernéticas.

2. Promover una cultura de seguridad de la información dentro de la comunidad educativa, aumentando la concienciación y la responsabilidad en materia de ciberseguridad.

3. Garantizar la continuidad de las operaciones educativas mediante la implementación de medidas de prevención y recuperación ante incidentes de seguridad cibernética.

Objetivos Específicos:

1. Identificar y proteger los activos de información crítica de la institución, incluyendo bases de datos de estudiantes, registros financieros, sistemas de gestión académica, entre otros.

2. Implementar políticas de seguridad de la información que establezcan directrices claras y responsabilidades para proteger los activos de información y mitigar los riesgos cibernéticos.

3. Mejorar la seguridad de los sistemas y redes de la institución mediante la implementación de medidas técnicas, como firewalls, antivirus, autenticación segura, cifrado de datos, entre otros.

4. Educar y capacitar a estudiantes, profesores y personal en buenas prácticas de seguridad de la información, incluyendo el uso seguro de recursos informáticos y la identificación de posibles amenazas cibernéticas.

5. Desarrollar un plan de gestión de incidentes que establezca procedimientos claros para detectar, responder y recuperarse de incidentes de seguridad cibernética de manera oportuna y efectiva.

6. Realizar auditorías de seguridad periódicas y pruebas de penetración para evaluar la efectividad de las medidas de seguridad implementadas y detectar posibles vulnerabilidades.

7. Establecer un plan de continuidad del negocio que garantice la disponibilidad y recuperación de los sistemas y datos críticos en caso de interrupciones significativas debido a incidentes de seguridad.

8. Mantener una estrecha colaboración con autoridades de ciberseguridad relevantes y promover la comunicación efectiva con la comunidad educativa sobre posibles amenazas y medidas de seguridad.

1. Evaluación de Riesgos

La evaluación de riesgos es un paso crítico en el desarrollo de un plan de ciberseguridad efectivo. Consiste en identificar y analizar los riesgos potenciales a los que está expuesta la información y los sistemas de la Unidad Educativa Internacional Liceo Iberoamericano. A continuación, se detallan los pasos necesarios para llevar a cabo esta evaluación:

1.1 Identificación de Activos Críticos:

1.1.1 **Datos Sensibles**: Identificar todos los tipos de datos sensibles almacenados y procesados por la institución, como información personal de los estudiantes y empleados, registros académicos, información financiera, etc.
Para la recopilación de datos se usará la siguiente matriz.

Tipo de Datos Sensibles	Descripción	Ejemplos
Información Personal	Datos identificativos de estudiantes y empleados	Nombres, apellidos, números de identificación, fotos
Registros Académicos	Información sobre el rendimiento académico	Calificaciones, historial de cursos, asistencia

Información Financiera	Datos relacionados con transacciones y pagos	Matrículas, pagos de colegiaturas, becas, donaciones
Datos de Salud	Información médica y de salud	Expedientes médicos, alergias, condiciones médicas
Comunicaciones Electrónicas	Correos electrónicos, mensajes	Correos institucionales, chats, mensajes de texto
Datos de Acceso	Credenciales de inicio de sesión	Nombres de usuario, contraseñas, PINs
Datos Biométricos	Datos físicos únicos de identificación	Huellas dactilares, escaneos de retina
Información de Contacto	Datos de contacto de estudiantes y empleados	Direcciones, números de teléfono, correos electrónicos

1.1.2 **Infraestructura de TI**: Identificar todos los sistemas de información críticos, redes, servidores, bases de datos y otros activos de TI utilizados por la institución para almacenar, procesar y transmitir datos.

1.1.3 **Recursos Humanos**: Identificar al personal de TI y otros empleados clave que tienen acceso a información crítica y desempeñan un papel importante en la gestión de la seguridad de la información.

1.2 Evaluación de Amenazas:

1.2.1 **Amenazas Externas**: Identificar posibles amenazas externas, como ataques de hackers, malware, phishing, ataques de denegación de servicio (DDoS), entre otros, que podrían comprometer la seguridad de la información de la institución.

Matriz de Amenazas Externas para la Unidad Educativa Internacional Liceo Iberoamericano

Amenaza	Descripción	Impacto	Probabilidad	Acciones
Ataques de Hackers	Acceso no autorizado a sistemas y datos para robar, modificar o destruir información.	Alto	Media	- Implementar sistemas de detección y prevención de intrusiones (IDS/IPS). - Mantener software y sistemas actualizados - Realizar auditorías de seguridad periódicas.
Malware	Software malicioso que puede infectar sistemas, robar información, o dañar datos y dispositivos.	Alto	Alta	- Utilizar soluciones antivirus y antimalware actualizadas. - Realizar análisis de seguridad regulares. - Implementar políticas de descarga segura y educación del usuario.

Phishing	Intentos de obtener información sensible mediante engaños, usualmente a través de correos electrónicos fraudulentos.	Medio	Alta	- Capacitar a los usuarios sobre la identificación de correos electrónicos de phishing. - Implementar filtros de spam y análisis de correos electrónicos. - Simulaciones de phishing.
Ataques de Denegación de Servicio (DDoS)	Sobrecargar sistemas y redes con tráfico excesivo, haciendo que los servicios sean inaccesibles.	Alto	Media	- Implementar soluciones de mitigación DDoS. - Utilizar servicios de protección en la nube. - Monitorear el tráfico de red para detectar patrones anómalos.
Ransomware	Malware que encripta datos y exige un rescate para su liberación.	Alto	Media	- Realizar copias de seguridad regulares y almacenarlas fuera de línea. - Capacitar a los usuarios sobre cómo evitar infecciones. - Implementar soluciones de seguridad de endpoint.
Ingeniería Social	Técnicas de manipulación psicológica para obtener información confidencial o acceso a sistemas.	Medio	Media	- Capacitar a los empleados sobre los riesgos de la ingeniería social. - Establecer protocolos de verificación de identidad. - Realizar pruebas de penetración sociales.

Acciones Generales a Implementar

Evaluación y Monitoreo Continuo:

- Realizar evaluaciones regulares de vulnerabilidades y pruebas de penetración para identificar posibles puntos débiles.
- Implementar herramientas de monitoreo en tiempo real para detectar y responder a incidentes de seguridad.

Capacitación y Concienciación:

- Desarrollar programas de capacitación para todos los empleados y estudiantes sobre las mejores prácticas de seguridad informática.
- Realizar campañas de concienciación sobre las últimas amenazas y técnicas de ataque.

Políticas y Procedimientos de Seguridad:

- Establecer políticas claras sobre el uso de dispositivos y redes de la institución.
- Desarrollar y mantener un plan de respuesta a incidentes de seguridad.

Tecnología y Herramientas de Seguridad:

- Implementar soluciones de firewall, antivirus, antimalware y sistemas de detección de intrusiones.
- Utilizar autenticación multifactor (MFA) para acceso a sistemas críticos.

Colaboración y Comunicación:

- Fomentar la colaboración entre diferentes departamentos para mejorar la seguridad general.
- Mantener una comunicación abierta con entidades externas de ciberseguridad y participar en redes de información sobre amenazas.

1.2.2 **Amenazas Internas**: Evaluar el riesgo de amenazas internas, como el acceso no autorizado por parte de empleados, la negligencia en el manejo de datos sensibles, el robo de información confidencial, etc.

Matriz de Amenazas Internas para la Unidad Educativa Internacional Liceo Iberoamericano

Amenaza	Descripción	Impacto Potencial	Probabilidad	Acciones a Realizar
Acceso No Autorizado por Empleados	Acceso a sistemas y datos sensibles sin permisos adecuados, ya sea por intención maliciosa o error.	Alto	Media	- Implementar controles de acceso basados en roles (RBAC - Revisar y actualizar regularmente los permisos de usuario. - Utilizar autenticación multifactor (MFA).
Negligencia en el Manejo de Datos	Manejo inadecuado de información sensible por parte de empleados, incluyendo almacenamiento inseguro y transmisión no segura de datos.	Medio	Alta	- Capacitar a los empleados en buenas prácticas de manejo de datos - Implementar políticas claras de manejo y protección de datos. - Realizar auditorías regulares de cumplimiento.
Robo de Información Confidencial	Empleados que deliberadamente sustraen información sensible para uso personal o beneficio externo.	Alto	Baja	- Realizar verificaciones de antecedentes al contratar personal. - Implementar monitoreo y registro de actividades de acceso a información sensible.

				- Establecer políticas estrictas y consecuencias claras.
Uso Inapropiado de Recursos	Utilización de los recursos tecnológicos de la institución para fines personales o inapropiados, incluyendo la instalación de software no autorizado.	Medio	Media	- Implementar políticas de uso aceptable de los recursos tecnológicos. - Utilizar software de monitoreo y control de aplicaciones. - Realizar auditorías periódicas de uso.
Filtraciones de Información	Divulgación accidental o intencional de información confidencial a personas no autorizadas, ya sea dentro o fuera de la institución.	Alto	Media	- Establecer políticas de clasificación y manejo de información. - Capacitar a los empleados sobre la importancia de la confidencialidad. - Implementar soluciones de DLP (Data Loss Prevention).
Amenazas Internas por Descontento	Empleados descontentos que podrían intentar dañar los sistemas o robar información como represalia.	Alto	Baja	- Monitorear el comportamiento de los empleados para identificar signos de descontento. - Ofrecer canales de comunicación para quejas y preocupaciones. - Implementar controles de acceso y monitoreo de actividades.

Acciones Generales a Implementar

Evaluación y Monitoreo Continuo:

- Realizar evaluaciones regulares de riesgos internos y auditorías de seguridad.
- Implementar herramientas de monitoreo en tiempo real para detectar actividades sospechosas de empleados.

Capacitación y Concienciación:

- Desarrollar programas de capacitación para todos los empleados sobre las mejores prácticas de seguridad informática y manejo de información.
- Realizar campañas de concienciación sobre la importancia de la seguridad interna y las consecuencias de su incumplimiento.

Políticas y Procedimientos de Seguridad:

- Establecer políticas claras sobre el acceso, uso y manejo de la información y recursos tecnológicos.
- Desarrollar y mantener un plan de respuesta a incidentes de seguridad interna.

Tecnología y Herramientas de Seguridad:

- Implementar soluciones de control de acceso, monitoreo de actividades y prevención de pérdida de datos (DLP).

- Utilizar autenticación multifactor (MFA) y controles de acceso basados en roles (RBAC) para proteger información sensible.

Gestión de Personal:

- Realizar verificaciones de antecedentes y evaluaciones de riesgos al contratar personal.
- Monitorear el comportamiento y desempeño de los empleados para detectar posibles amenazas internas.

Colaboración y Comunicación:

- Fomentar la colaboración entre diferentes departamentos para mejorar la seguridad general.

Mantener una comunicación abierta y transparente con los empleados sobre las políticas de seguridad y sus responsabilidades.

1.2.3 **Amenazas Naturales**: Considerar amenazas naturales, como desastres naturales (inundaciones, incendios, terremotos, etc.), que podrían afectar la disponibilidad y la integridad de los activos de información.

1.3 Evaluación de Vulnerabilidades:

1.3.1 **Análisis de Vulnerabilidades**: Realizar un análisis detallado de los sistemas y redes de la institución para identificar posibles vulnerabilidades de seguridad, como fallos de software, configuraciones inseguras, puertos abiertos, etc.

1.3.2 **Evaluación de Configuraciones de Seguridad**: Revisar las configuraciones de seguridad de los sistemas y aplicaciones para garantizar que estén alineadas con las mejores prácticas de seguridad y cumplimiento de normativas.

1.3.3 **Pruebas de Penetración**: Realizar pruebas de penetración controladas para evaluar la resistencia de los sistemas y redes contra ataques externos e internos y detectar posibles puntos débiles.

1.4 Documentación de Resultados:

1.4.1 **Informe de Evaluación de Riesgos**: Documentar los resultados de la evaluación de riesgos en un informe detallado que incluya una lista de activos críticos, amenazas identificadas, vulnerabilidades encontradas y recomendaciones para mitigar los riesgos.

1.4.2 **Priorización de Riesgos**: Priorizar los riesgos identificados según su impacto potencial en la seguridad de la información y la disponibilidad de recursos para abordarlos.

1.5 Acciones Correctivas y Planificación:

1.5.1 **Desarrollo de Plan de Mitigación**: Desarrollar un plan detallado de mitigación de riesgos que incluya acciones específicas para abordar las vulnerabilidades identificadas y reducir el impacto de las amenazas.

1.5.2 **Asignación de Recursos**: Asignar recursos humanos y financieros necesarios para implementar las acciones correctivas y mejorar la postura de seguridad de la institución.

1.5.3 **Seguimiento y Revisión Continua**: Establecer mecanismos para monitorear y revisar continuamente la efectividad de las medidas de mitigación de riesgos y realizar ajustes según sea necesario.

Matriz de Seguimiento de Implementación.

Actividad	Descripción	Responsable	Fecha de Inicio	Fecha de Finalización	Estado	Observaciones
Identificación de Activos	Listar todos los activos críticos de la institución.	Equipo de IT	01/06/2024	10/06/2024	En progreso	
Identificación de Amenazas y Vulnerabilidades	Evaluar posibles amenazas y vulnerabilidades para cada activo.	Consultor de Seguridad	11/06/2024	30/06/2024	Pendiente	
Evaluación del Impacto y Probabilidad	Asignar niveles de impacto y probabilidad a cada riesgo identificado.	Equipo de Riesgos	01/07/2024	15/07/2024	Pendiente	
Priorización de Riesgos	Clasificar los riesgos según su criticidad y priorizar las acciones.	Consultor de Seguridad	16/07/2024	20/07/2024	Pendiente	

2. Desarrollo de Políticas y Procedimientos

El desarrollo de políticas y procedimientos en ciberseguridad es fundamental para establecer un marco de referencia claro y consistente que guíe las acciones y comportamientos de todos los miembros de la Unidad Educativa Internacional Liceo Iberoamericano en relación con la protección de la información y los sistemas. A continuación, se detallan los pasos necesarios para llevar a cabo este proceso:

2.1 Definición de Objetivos y Alcance:

2.1.1 **Identificación de Objetivos**: Determinar los objetivos generales y específicos que se pretenden alcanzar con la implementación de las políticas y procedimientos de ciberseguridad, como proteger la confidencialidad, integridad y disponibilidad de la información, cumplir con regulaciones legales y normativas, etc.

2.1.2 **Alcance del Marco de Políticas**: Establecer el alcance del marco de políticas, definiendo qué activos de información y sistemas estarán cubiertos,

así como quiénes serán responsables de cumplir con las políticas y procedimientos establecidos.

2.2 **Desarrollo de Políticas:**

2.2.1 **Política de Seguridad de la Información**: Crear una política de seguridad de la información que establezca los principios generales y las directrices para proteger los activos de información de la institución contra amenazas internas y externas.

2.2.2 **Política de Uso Aceptable**: Definir una política de uso aceptable que establezca las reglas y restricciones para el uso apropiado de los recursos informáticos de la institución por parte de estudiantes, profesores y personal.

2.2.3 **Política de Gestión de Contraseñas**: Establecer una política de gestión de contraseñas que defina los requisitos para la creación, almacenamiento y uso seguro de contraseñas para acceder a los sistemas y aplicaciones de la institución.

2.3 Desarrollo de Procedimientos:

2.3.1 **Procedimientos de Gestión de Incidentes**: Desarrollar procedimientos claros y detallados para detectar, reportar, responder y recuperarse de incidentes de seguridad de la información de manera oportuna y efectiva.

2.3.2 **Procedimientos de Control de Acceso**: Establecer procedimientos para administrar y controlar el acceso a los sistemas y datos de la institución, incluyendo la asignación de privilegios de acceso y la revocación de accesos no autorizados.

2.3.3 **Procedimientos de Respuesta a Emergencias**: Crear procedimientos de respuesta a emergencias que definan los roles y responsabilidades del personal en caso de desastres naturales, incumplimientos de seguridad graves u otros eventos que pongan en riesgo la continuidad de las operaciones.

2.4 Revisión y Aprobación:

2.4.1 **Revisión por Partes Interesadas**: Solicitar la revisión y comentarios de las partes interesadas relevantes, como el personal de TI, directivos, representantes de padres y estudiantes, para garantizar que las políticas y procedimientos sean comprensibles, adecuados y aceptables para todos.

2.4.2 **Aprobación por la Dirección**: Obtener la aprobación formal de la dirección de la institución para las políticas y procedimientos desarrollados, demostrando su compromiso y respaldo con la seguridad de la información.

2.5 Implementación y Comunicación:

2.5.1 **Implementación de Políticas**: Implementar las políticas y procedimientos aprobados en todos los niveles de la institución, proporcionando orientación y capacitación adecuadas al personal para garantizar su comprensión y cumplimiento.

2.5.2 **Comunicación y Concienciación**: Comunicar de manera efectiva las políticas y procedimientos a todos los miembros de la comunidad educativa, promoviendo la concienciación sobre la importancia de la ciberseguridad y la responsabilidad de todos en su cumplimiento.

Matriz de seguimiento del Desarrollo de Políticas y Procedimientos

Actividad	Descripción	Responsable	Fecha de Inicio	Fecha de Finalización	Estado	Observaciones
Redacción de Políticas de Seguridad	Crear políticas de seguridad claras para el manejo de datos y uso de recursos tecnológicos.	Equipo de Cumplimiento	01/08/2024	30/08/2024	Pendiente	
Desarrollo de Procedimientos	Detallar los procedimientos para la implementación de políticas de seguridad.	Equipo de Cumplimiento	01/09/2024	15/09/2024	Pendiente	
Revisión y Aprobación	Revisar y aprobar las políticas y procedimientos por la dirección de la institución.	Dirección	16/09/2024	30/09/2024	Pendiente	

3. Implementación de Medidas de Seguridad

La implementación de medidas de seguridad es un paso crucial en el fortalecimiento de la postura de ciberseguridad de la Unidad Educativa Internacional Liceo Iberoamericano. Este paso implica la aplicación práctica de controles y tecnologías diseñadas para proteger los activos de información y mitigar los riesgos cibernéticos. A continuación, se detallan los pasos necesarios para llevar a cabo esta implementación:

3.1 Selección de Medidas de Seguridad:

3.1.1 **Evaluación de Riesgos**: Basado en la evaluación de riesgos previamente realizada, identificar las áreas críticas y los activos de información más susceptibles a amenazas y vulnerabilidades.

3.1.2 **Análisis de Requisitos**: Determinar los requisitos específicos de seguridad para cada activo de información y sistema, considerando aspectos como confidencialidad, integridad, disponibilidad y cumplimiento normativo.

3.2 Diseño e Implementación de Controles de Seguridad:

3.2.1 **Firewalls y Seguridad de Red**: Implementar firewalls y soluciones de seguridad de red para monitorear y controlar el tráfico de red, protegiendo así los sistemas contra amenazas externas.

3.2.2 **Antivirus y Antimalware**: Desplegar soluciones antivirus y antimalware en todos los dispositivos y sistemas de la institución para detectar y prevenir la ejecución de software malicioso.

3.2.3 **Autenticación Multifactor (MFA)**: Habilitar la autenticación multifactor en los sistemas críticos y aplicaciones para agregar una capa adicional de seguridad al requerir múltiples formas de autenticación para acceder a los recursos.

3.2.4 **Gestión de Identidades y Accesos (IAM)**: Implementar soluciones de IAM para administrar de manera centralizada los accesos de usuarios, garantizando que solo aquellos autorizados tengan acceso a recursos específicos.

3.2.5 **Cifrado de Datos**: Aplicar cifrado de datos para proteger la confidencialidad de la información almacenada y transmitida, especialmente en dispositivos móviles y comunicaciones en línea.

3.3 Capacitación y Concienciación:

3.3.1 **Programas de Capacitación**: Proporcionar capacitación regular en seguridad de la información para todo el personal, cubriendo temas como mejores prácticas de seguridad, identificación de amenazas y manejo de incidentes.

3.3.2 **Concienciación del Usuario**: Sensibilizar a los usuarios sobre las amenazas cibernéticas comunes, como el phishing y la ingeniería social, y proporcionar pautas claras sobre cómo reconocer y evitar estas amenazas.

3.4 Monitoreo y Gestión de Incidentes:

3.4.1 **Implementación de Herramientas de Monitoreo**: Desplegar herramientas de monitoreo de seguridad para detectar y responder proactivamente a actividades sospechosas en los sistemas y redes.

3.4.2 **Plan de Respuesta a Incidentes**: Establecer un plan detallado de respuesta a incidentes que defina roles y responsabilidades, procedimientos

de notificación y acciones de recuperación en caso de una brecha de seguridad.

3.5 Actualizaciones y Mantenimiento Continuo:

3.5.1 **Parches y Actualizaciones**: Implementar políticas para garantizar la aplicación oportuna de parches de seguridad y actualizaciones de software en todos los sistemas y dispositivos para remediar vulnerabilidades conocidas.

3.5.2 **Auditorías y Pruebas de Penetración**: Realizar auditorías de seguridad regulares y pruebas de penetración para evaluar la efectividad de las medidas de seguridad implementadas y detectar posibles vulnerabilidades.

Matriz de Implementación de Medidas de Seguridad

Actividad	Descripción	Responsable	Fecha de Inicio	Fecha de Finalización	Estado	Observaciones
Implementación de Firewall	Instalar y configurar firewalls para proteger la red.	Equipo de IT	01/10/2024	15/10/2024	Pendiente	
Actualización de Software y Parches	Asegurar que todos los sistemas y software estén actualizados.	Equipo de IT	16/10/2024	31/10/2024	Pendiente	
Implementación de IDS/IPS	Implementar sistemas de detección y prevención de intrusiones.	Consultor de Seguridad	01/11/2024	15/11/2024	Pendiente	
Configuración de Control de Acceso	Establecer controles de acceso basados en roles y autenticación multifactor.	Equipo de IT	16/11/2024	30/11/2024	Pendiente	

4. Concienciación y Formación

La concienciación y formación en ciberseguridad es esencial para crear una cultura de seguridad en toda la Unidad Educativa Internacional Liceo Iberoamericano. Este paso implica educar y sensibilizar a todos los miembros de la comunidad educativa sobre las amenazas cibernéticas, las mejores prácticas de seguridad y su papel en la protección de la información. A continuación, se detallan los pasos necesarios para llevar a cabo esta concienciación y formación:

4.1 Evaluación de Necesidades:

4.1.1 **Análisis de Audiencia**: Identificar los diferentes grupos dentro de la comunidad educativa, como estudiantes, profesores, personal administrativo y padres, y determinar sus necesidades específicas de formación en ciberseguridad.

4.1.2 **Identificación de Temas Relevantes**: Evaluar las amenazas cibernéticas más comunes y las áreas de vulnerabilidad dentro de la institución para determinar los temas clave que deben abordarse en los programas de concienciación y formación.

4.2 Diseño de Programas de Formación:

4.2.1 **Desarrollo de Contenidos**: Crear materiales de formación claros y accesibles que aborden temas como contraseñas seguras, phishing, seguridad en dispositivos móviles, protección de datos personales y comportamientos seguros en línea.

4.2.2 **Formatos de Formación**: Ofrecer una variedad de formatos de formación, como sesiones presenciales, cursos en línea, videos educativos, carteles informativos y boletines de seguridad, para adaptarse a las preferencias de aprendizaje de la comunidad educativa.

4.3 Implementación de Programas de Concienciación:

4.3.1 **Sesiones de Concienciación**: Organizar sesiones periódicas de concienciación en ciberseguridad para estudiantes, profesores y personal administrativo, donde se presenten y discutan los conceptos clave de seguridad de la información.

4.3.2 **Campañas de Sensibilización**: Lanzar campañas de sensibilización regulares a través de carteles, correos electrónicos, redes sociales y otros canales de comunicación para destacar las amenazas cibernéticas actuales y promover buenas prácticas de seguridad.

4.4 Formación Específica para Roles:

4.4.1 **Formación para Personal de TI**: Proporcionar formación específica en seguridad de la información para el personal de TI, incluyendo temas avanzados como gestión de vulnerabilidades, análisis forense digital y respuesta a incidentes.

4.2 **Formación para Estudiantes**: Integrar la formación en ciberseguridad en el currículo escolar, ofreciendo programas educativos diseñados para enseñar a los estudiantes sobre los riesgos en línea, el uso seguro de la tecnología y la protección de su privacidad en línea.

4.5 Evaluación y Seguimiento:

4.5.1 **Evaluación de la Efectividad**: Realizar evaluaciones periódicas para medir la efectividad de los programas de concienciación y formación en ciberseguridad, utilizando encuestas, cuestionarios y métricas de participación.

4.5.2 **Feedback y Mejora Continua**: Recopilar feedback de los participantes y utilizarlo para mejorar y ajustar los programas de formación en función de las necesidades cambiantes y los comentarios recibidos.

Matriz de seguimiento de Concienciación y Formación

Actividad	Descripción	Responsable	Fecha de Inicio	Fecha de Finalización	Estado	Observaciones
Desarrollo de Programa de Capacitación	Crear un programa de formación sobre ciberseguridad para empleados y estudiantes.	Recursos Humanos	01/12/2024	15/12/2024	Pendiente	
Realización de Talleres y Seminarios	Organizar talleres y seminarios de ciberseguridad periódicamente.	Recursos Humanos	16/12/2024	Continuo	Pendiente	
Simulaciones de Phishing	Realizar simulaciones de ataques de phishing para educar a los usuarios.	Consultor de Seguridad	01/01/2025	Continuo	Pendiente	

5. Auditorías y Evaluaciones Periódicas

Las auditorías y evaluaciones periódicas son elementos cruciales en la gestión efectiva de la ciberseguridad en la Unidad Educativa Internacional Liceo Iberoamericano. Estos procesos garantizan que las medidas de seguridad implementadas sean efectivas, identificando posibles vulnerabilidades y áreas de mejora. A continuación, se detallan los pasos necesarios para llevar a cabo estas auditorías y evaluaciones:

5.1 Planificación de Auditorías y Evaluaciones:

5.1.1 **Definición de Objetivos**: Establecer los objetivos específicos de las auditorías y evaluaciones, como evaluar el cumplimiento normativo, identificar vulnerabilidades en la infraestructura de TI o medir el nivel de concienciación en seguridad.

5.1.2 **Selección de Metodologías**: Elegir las metodologías adecuadas para llevar a cabo las auditorías y evaluaciones, como auditorías internas, pruebas de penetración externas, análisis de vulnerabilidades, revisión de políticas y procedimientos, etc.

5.2 Ejecución de Auditorías y Evaluaciones:

5.2.1 **Auditorías Internas**: Realizar auditorías internas periódicas para evaluar el estado de la ciberseguridad en la institución, revisando el cumplimiento de políticas, controles de acceso, configuraciones de seguridad, registros de auditoría, entre otros.

5.2.2 **Pruebas de Penetración**: Realizar pruebas de penetración externas e internas para identificar y explotar vulnerabilidades en los sistemas y redes de la institución, simulando ataques reales para evaluar la resistencia de las defensas de seguridad.

5.2.3 **Análisis de Vulnerabilidades**: Realizar análisis de vulnerabilidades en sistemas y aplicaciones para identificar posibles puntos débiles que podrían ser explotados por atacantes externos o internos.

5.3 Evaluación de Resultados:

5.3.1 **Análisis de Hallazgos**: Analizar los hallazgos de las auditorías y evaluaciones para identificar áreas de riesgo y puntos críticos que requieran atención inmediata.

5.3.2 **Priorización de Acciones**: Priorizar las acciones correctivas y preventivas basadas en la gravedad de los hallazgos y el impacto potencial en la seguridad de la información de la institución.

5.4 Implementación de Mejoras:

5.4.1 **Desarrollo de Planes de Acción**: Elaborar planes de acción detallados para abordar las vulnerabilidades identificadas y mejorar las defensas de seguridad de la institución.

5.4.2 **Seguimiento y Verificación**: Realizar un seguimiento continuo de la implementación de las acciones correctivas y preventivas para garantizar que se completen según lo planeado y que se logren los resultados esperados.

5.5 Documentación y Reporte:

5.5.1 **Informe de Auditoría**: Preparar informes detallados de auditoría que incluyan los hallazgos, recomendaciones, acciones tomadas y planes de mejora para su revisión por parte de la dirección y otros interesados.

5.5.2 **Registro de Auditoría**: Mantener registros detallados de todas las auditorías y evaluaciones realizadas, incluyendo fechas, participantes, metodologías utilizadas, hallazgos y acciones tomadas.

Matriz de seguimiento de Auditorías y Evaluaciones Periódicas

Actividad	Descripción	Responsable	Fecha de Inicio	Fecha de Finalización	Estado	Observaciones
Auditorías de Seguridad	Realizar auditorías de seguridad internas y externas.	Auditor Interno	01/02/2025	Continuo	Pendiente	
Evaluaciones de Cumplimiento	Evaluar el cumplimiento de políticas y procedimientos de seguridad.	Auditor Interno	01/02/2025	Continuo	Pendiente	
Informes de Auditoría	Generar informes detallados de las auditorías y evaluaciones realizadas.	Auditor Interno	01/02/2025	Continuo	Pendiente	

6. Plan de Continuidad del Negocio

El Plan de Continuidad del Negocio (BCP, por sus siglas en inglés) es esencial para garantizar que la Unidad Educativa Internacional Liceo Iberoamericano pueda mantener sus operaciones críticas y minimizar el impacto de interrupciones inesperadas, como incidentes de seguridad cibernética, desastres naturales o fallas en la infraestructura. A continuación, se detallan los pasos necesarios para desarrollar este plan:

6.1 Evaluación de Impacto en el Negocio (BIA):

6.1.1 **Identificación de Procesos Críticos**: Determinar los procesos y funciones críticas de la institución que deben mantenerse operativas durante una interrupción, como la enseñanza, la administración académica, la comunicación con padres y la gestión de recursos humanos.

6.1.2 **Análisis de Impacto**: Evaluar el impacto potencial de la interrupción de estos procesos críticos en términos de pérdida financiera, daño a la reputación, incumplimiento de regulaciones, interrupción del aprendizaje, entre otros factores.

6.2 Desarrollo de Estrategias de Continuidad:

6.2.1 Identificación de Medidas de Mitigación: Identificar medidas de mitigación para reducir la probabilidad de interrupciones, como la implementación de redundancia de sistemas, copias de seguridad periódicas, políticas de seguridad robustas y sistemas de detección y respuesta a incidentes.

6.2.2 Desarrollo de Planes de Respuesta: Crear planes detallados de respuesta a incidentes y continuidad del negocio que establezcan roles y responsabilidades, procedimientos de notificación, protocolos de recuperación de datos y sistemas, y estrategias de comunicación con partes interesadas.

6.3 Implementación y Pruebas:

6.3.1 **Implementación de Medidas de Mitigación**: Implementar las medidas de mitigación identificadas en los sistemas y procesos de la institución, asegurando que estén correctamente configuradas y operativas.

6.3.2 **Simulacros y Ejercicios**: Realizar simulacros y ejercicios periódicos de respuesta a incidentes y continuidad del negocio para entrenar al personal en la ejecución de los planes y mejorar la preparación para situaciones reales de crisis.

6.4 Mantenimiento y Actualización:

6.4.1 **Revisión y Mejora Continua**: Revisar y actualizar regularmente el Plan de Continuidad del Negocio para reflejar cambios en el entorno operativo, la infraestructura de TI y las amenazas emergentes, asegurando su relevancia y efectividad a lo largo del tiempo.

6.4.2 **Capacitación del Personal**: Proporcionar capacitación continua al personal sobre sus roles y responsabilidades en la ejecución del BCP, asegurando que estén preparados y competentes para responder eficazmente a situaciones de crisis.

6.5 Coordinación con Partes Interesadas:

6.5.1 **Comunicación y Coordinación**: Mantener una comunicación abierta y efectiva con todas las partes interesadas, incluyendo personal, estudiantes, padres, autoridades educativas y proveedores, durante la planificación, ejecución y recuperación de incidentes.

6.5.2 **Colaboración Externa**: Establecer relaciones de colaboración con organizaciones externas, como agencias gubernamentales, servicios de emergencia y otras instituciones educativas, para facilitar la coordinación y el intercambio de recursos en situaciones de crisis.

Matriz de Seguimiento del Plan de Continuidad del Negocio

Actividad	Descripción	Responsable	Fecha de Inicio	Fecha de Finalización	Estado	Observaciones
Desarrollo del Plan de Continuidad	Crear un plan de continuidad del negocio que contemple incidentes de ciberseguridad.	Equipo de Continuidad	01/03/2025	31/03/2025	Pendiente	
Pruebas del Plan	Realizar simulacros y pruebas del plan de continuidad.	Equipo de Continuidad	01/04/2025	15/04/2025	Pendiente	
Revisión y Actualización del Plan	Revisar y actualizar el plan de continuidad periódicamente.	Equipo de Continuidad	16/04/2025	Continuo	Pendiente	

7. Colaboración y Coordinación

La colaboración y coordinación son fundamentales en la gestión de la ciberseguridad de la Unidad Educativa Internacional Liceo Iberoamericano. La participación activa de todos los miembros de la comunidad educativa, así como la cooperación con entidades externas, fortalecerá la postura de seguridad de la institución. A continuación, se detallan los pasos necesarios para promover la colaboración y coordinación en el plan de ciberseguridad:

7.1 Establecimiento de Comités de Seguridad:

7.1.1 **Comité Interno de Seguridad**: Crear un comité interno de seguridad que incluya representantes de diferentes departamentos y áreas de la institución, con el objetivo de coordinar esfuerzos, compartir información y tomar decisiones relacionadas con la ciberseguridad.

7.1.2 **Participación de Interesados**: Involucrar a todos los niveles de la organización, incluyendo directivos, personal docente, administrativo, estudiantes y padres, en las actividades de seguridad cibernética para fomentar una cultura de seguridad compartida.

7.2 Colaboración Externa:

7.2.1 **Redes de Colaboración**: Participar en redes de colaboración con otras instituciones educativas, organizaciones gubernamentales, proveedores de servicios de seguridad y grupos de la industria para intercambiar información, mejores prácticas y recursos.

7.2.2 Coordinación con Autoridades: Establecer canales de comunicación y coordinación con las autoridades locales, regionales y nacionales encargadas

de la ciberseguridad para recibir orientación, asistencia y apoyo en la gestión de incidentes y la prevención de amenazas.

7.3 Desarrollo de Protocolos de Comunicación:

7.3.1 **Plan de Comunicación de Incidentes**: Elaborar un plan de comunicación de incidentes que establezca los procedimientos para la notificación, respuesta y divulgación de incidentes de seguridad cibernética tanto interna como externamente, garantizando una respuesta rápida y eficaz.

7.3.2 **Canal de Denuncia de Seguridad**: Implementar un canal de denuncia de seguridad donde los miembros de la comunidad educativa puedan informar de manera confidencial sobre posibles incidentes de seguridad, vulnerabilidades o comportamientos sospechosos.

7.4 Ejercicio de Simulacros y Pruebas:

7.4.1 **Simulacros de Incidentes**: Realizar ejercicios periódicos de simulacros de incidentes de seguridad cibernética para probar la efectividad de los planes de respuesta, identificar áreas de mejora y aumentar la preparación del personal para situaciones reales.

7.4.2 **Pruebas de Coordinación**: Coordinar ejercicios de prueba de coordinación con otras instituciones y entidades externas para evaluar la capacidad de colaboración y respuesta conjunta en caso de incidentes de seguridad cibernética a gran escala.

7.5 Capacitación y Sensibilización:

7.5.1 **Programas de Formación**: Ofrecer programas de formación en seguridad cibernética para todos los miembros de la comunidad educativa, incluyendo entrenamiento sobre reconocimiento de amenazas, buenas prácticas de seguridad y uso seguro de la tecnología.

7.5.2 **Campañas de Sensibilización**: Lanzar campañas periódicas de sensibilización en seguridad cibernética dirigidas a estudiantes, padres y personal, para aumentar la conciencia sobre los riesgos cibernéticos y promover comportamientos seguros en línea.

Matriz de Seguimiento de Colaboración y Coordinación

Actividad	Descripción	Responsable	Fecha de Inicio	Fecha de Finalización	Estado	Observaciones
Establecimiento de Alianzas	Crear alianzas con otras instituciones y organismos de ciberseguridad.	Dirección	01/05/2025	Continuo	Pendiente	

Participación en Redes de Información	Participar en redes de intercambio de información sobre amenazas y mejores prácticas.	Dirección	01/05/2025	Continuo	Pendiente	
Coordinación con Entidades Externas	Coordinar con autoridades y entidades externas para mejorar la respuesta a incidentes.	Dirección	01/05/2025	Continuo	Pendiente	

8. Mejora Continua

La mejora continua es un proceso fundamental en la gestión de la ciberseguridad de la Unidad Educativa Internacional Liceo Iberoamericano. A través de la retroalimentación, la evaluación constante y la implementación de mejoras, la institución puede adaptarse a los cambios en el panorama de amenazas y fortalecer su postura de seguridad de manera proactiva. A continuación, se detallan los pasos necesarios para promover la mejora continua en el plan de ciberseguridad:

8.1 Recopilación y Análisis de Datos:

8.1.1 **Evaluación de Incidentes**: Realizar un análisis exhaustivo de los incidentes de seguridad cibernética ocurridos en la institución, identificando las causas subyacentes, las lecciones aprendidas y las áreas de mejora.

8.1.2 **Métricas de Rendimiento**: Definir métricas de rendimiento y objetivos de seguridad cibernética que puedan medirse y evaluarse periódicamente para evaluar el cumplimiento y la efectividad de las medidas de seguridad implementadas.

8.2 Retroalimentación y Participación:

8.2.1 Encuestas y Evaluaciones: Solicitar retroalimentación regular de los diferentes grupos de interés, incluyendo personal, estudiantes, padres y proveedores, sobre su percepción de la seguridad cibernética y sugerencias para mejorarla.

8.2.2 **Participación Activa**: Fomentar la participación activa de todos los miembros de la comunidad educativa en el proceso de mejora continua, alentando la presentación de ideas, comentarios y propuestas de mejora relacionadas con la seguridad cibernética.

8.3 Revisión y Actualización de Políticas:

8.3.1 **Revisión Periódica**: Realizar revisiones periódicas de las políticas y procedimientos de seguridad cibernética de la institución para garantizar su relevancia, eficacia y alineación con las mejores prácticas y estándares de la industria.

8.3.2 **Actualización oportuna**: Actualizar las políticas y procedimientos de seguridad cibernética en respuesta a cambios en el entorno operativo, nuevas amenazas o vulnerabilidades identificadas, y lecciones aprendidas de incidentes previos.

8.4 Capacitación y Desarrollo:

8.4.1 **Programas de Formación Continua**: Ofrecer programas de formación continua en seguridad cibernética para todo el personal de la institución, asegurando que estén al tanto de las últimas tendencias, tecnologías y mejores prácticas en el campo de la ciberseguridad.

8.4.2 **Desarrollo Profesional**: Apoyar el desarrollo profesional del personal en el ámbito de la seguridad cibernética, proporcionando oportunidades de capacitación, certificación y participación en conferencias y eventos de la industria.

8.5 Implementación de Mejoras:

8.5.1 **Planes de Acción Correctiva**: Desarrollar planes de acción correctiva para abordar las áreas de mejora identificadas durante el proceso de mejora continua, asignando responsabilidades, plazos y recursos necesarios para su implementación.

8.5.2 **Seguimiento y Evaluación**: Realizar un seguimiento continuo de la implementación de las mejoras planificadas y evaluar su efectividad en la mejora de la seguridad cibernética de la institución, ajustando los enfoques según sea necesario.

Matriz de Seguimiento de Mejora Continua

Actividad	Descripción	Responsable	Fecha de Inicio	Fecha de Finalización	Estado	Observaciones
Revisión Periódica de Políticas	Revisar y actualizar las políticas de seguridad periódicamente.	Equipo de Cumplimiento	01/06/2025	Continuo	Pendiente	
Incorporación de Nuevas Tecnologías	Evaluar e incorporar nuevas tecnologías de ciberseguridad.	Equipo de IT	01/06/2025	Continuo	Pendiente	
Retroalimentación y Mejora	Recopilar retroalimentación de usuarios y	Dirección	01/06/2025	Continuo	Pendiente	

	ajustar las estrategias de seguridad.					

GRUPO ACADEMICO ISTRA