LÁBTICA — ESCUELA DIDÁCTICA S.A.S.

POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

Sistema de Gestión de Seguridad de la Información (SGSI)

Código: SGSI-POL-001
Versión: 1.0
Fecha de emisión: Julio de 2026
Clasificación: Uso Interno

Control del documento

Versión	Fecha	Descripción del cambio	Elaboró	Aprobó
1.0	Julio 2026	Emisión inicial del documento maestro de políticas de seguridad de la información	Andrés Sucerquia Osorio Oficial de Seguridad de la Información	Gerencia General

1. Introducción y objetivo

Lábtica (Escuela Didáctica S.A.S.) es una compañía colombiana de tecnología educativa dedicada al diseño de experiencias de aprendizaje, la operación de plataformas LXP en modalidad SaaS multi-tenant (Coloso), el desarrollo de extensiones y plugins para Moodle (incluida la suite didactic), la producción de contenidos e-learning en estándares como SCORM, y servicios de consultoría e infraestructura para clientes corporativos y educativos.

La información es el activo más valioso de Lábtica y de sus clientes. En el desarrollo de sus servicios, Lábtica trata datos personales de estudiantes y colaboradores de sus clientes, contenidos formativos propietarios, credenciales de acceso, información contractual y comercial, y configuraciones de infraestructura crítica. La materialización de un incidente de seguridad podría afectar la confidencialidad, integridad o disponibilidad de dicha información, la continuidad de los servicios y la confianza de los clientes.

El objetivo de este documento es establecer la Política General de Seguridad de la Información y las políticas complementarias que conforman el marco normativo del Sistema de Gestión de Seguridad de la Información (SGSI) de Lábtica, alineado con la norma ISO/IEC 27001:2022 y su Anexo A, y con la legislación colombiana aplicable, en particular la Ley 1581 de 2012 de protección de datos personales y sus decretos reglamentarios.

2. Alcance

Estas políticas aplican a toda la operación de Lábtica, incluyendo de manera enunciativa y no limitativa:

- Plataformas y productos: Coloso (SaaS multi-tenant), suite LXP, plugins y desarrollos a medida sobre Moodle, contenidos SCORM y demás paquetes de contenido e-learning.
- Infraestructura tecnológica propia y administrada: servidores y servicios en la nube (AWS, DigitalOcean y otros proveedores), paneles de administración, instancias Moodle de clientes administradas por Lábtica, herramientas de automatización, mensajería e integración, y entornos de desarrollo, pruebas y producción.
- Información en cualquier formato y medio: digital, impresa, verbal, almacenada, procesada o transmitida.
- Personas: todos los colaboradores de Lábtica, independientemente de su tipo de vinculación (laboral, prestación de servicios, aprendices, practicantes), así como contratistas, proveedores y terceros que accedan a información o sistemas de Lábtica o de sus clientes.
- Procesos: comerciales, de diseño instruccional, desarrollo de software, operación de infraestructura, soporte, administrativos, financieros y de talento humano.

El cumplimiento de estas políticas es obligatorio. Su inobservancia dará lugar a las acciones disciplinarias, contractuales o legales que correspondan, según se describe en el capítulo de cumplimiento.

3. Términos y definiciones

- Activo de información: todo elemento que contenga, procese o transmita información con valor para la organización (datos, software, hardware, servicios, personas, instalaciones).
- Confidencialidad: propiedad por la cual la información no se divulga a personas, entidades o procesos no autorizados.
- Integridad: propiedad de exactitud y completitud de la información y de los métodos de procesamiento.
- Disponibilidad: propiedad de ser accesible y utilizable a demanda por una entidad autorizada.
- Incidente de seguridad de la información: evento o serie de eventos no deseados o inesperados que tienen una probabilidad significativa de comprometer las operaciones o amenazar la seguridad de la información.
- SGSI: Sistema de Gestión de Seguridad de la Información conforme a ISO/IEC 27001.
- Dato personal: cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables (Ley 1581 de 2012).
- Tenant: espacio lógico aislado de un cliente dentro de una plataforma SaaS multi-tenant como Coloso.
- Responsable y Encargado del tratamiento: roles definidos por la Ley 1581 de 2012. Frente a los datos de usuarios finales de las plataformas de sus clientes, Lábtica actúa generalmente como Encargado del tratamiento.

4. Política General de Seguridad de la Información

4.1 Declaración de la Dirección

La Gerencia General de Lábtica declara su compromiso con la protección de la confidencialidad, integridad y disponibilidad de la información propia y de sus clientes, como condición esencial para la prestación de servicios de tecnología educativa confiables y para el cumplimiento de las obligaciones contractuales, legales y regulatorias de la compañía.

En consecuencia, la Dirección se compromete a: establecer, implementar, mantener y mejorar continuamente un SGSI alineado con ISO/IEC 27001:2022; asignar los recursos y roles necesarios; gestionar los riesgos de seguridad de la información con base en una metodología formal; asegurar la concienciación y formación del personal; y cumplir la legislación aplicable, en especial la normativa colombiana de protección de datos personales.

4.2 Principios

- La seguridad de la información se gestiona con base en riesgos: los controles se seleccionan y priorizan según el análisis y evaluación de riesgos sobre los activos de información.
- Mínimo privilegio y necesidad de conocer: cada persona accede únicamente a la información y sistemas estrictamente necesarios para sus funciones.
- Segregación de ambientes y funciones: se separan los entornos de desarrollo, pruebas y producción, y las funciones incompatibles entre sí.

- Aislamiento entre clientes: en las plataformas multi-tenant, la información de cada cliente se mantiene lógicamente aislada de la de los demás.
- Seguridad desde el diseño y por defecto: los productos, integraciones y servicios se conciben incorporando requisitos de seguridad y privacidad desde su diseño.
- Responsabilidad individual: toda persona con acceso a información de Lábtica o de sus clientes es responsable de protegerla y de reportar los incidentes o debilidades que detecte.
- Mejora continua: el SGSI se revisa y mejora de forma periódica con base en auditorías, indicadores, incidentes y cambios del contexto.

4.3 Objetivos de seguridad de la información

- Proteger los datos personales y la información confidencial de clientes, estudiantes y colaboradores frente a accesos no autorizados, pérdida o alteración.
- Garantizar la disponibilidad de las plataformas de aprendizaje y servicios administrados de acuerdo con los niveles de servicio pactados con los clientes.
- Cumplir los requisitos contractuales de seguridad exigidos por los clientes en sus procesos de contratación y auditoría.
- Prevenir, detectar y responder oportunamente a incidentes de seguridad, minimizando su impacto.
- Fortalecer la cultura de seguridad de la información en todos los colaboradores.

5. Roles y responsabilidades

La estructura de gobierno de seguridad de la información de Lábtica está conformada por los siguientes roles:

5.1 Gerencia General

- Aprueba la Política General de Seguridad de la Información y sus políticas complementarias.
- Asigna los recursos humanos, técnicos y financieros necesarios para el SGSI.
- Designa formalmente al Director de Tecnología y al Oficial de Seguridad de la Información.
- Preside la revisión por la dirección del SGSI, al menos una vez al año.
- Aprueba los niveles de aceptación de riesgo de la organización.

5.2 Director de Tecnología

- Es el responsable ejecutivo de la seguridad de la infraestructura tecnológica, las plataformas y los procesos de desarrollo de Lábtica.
- Garantiza que la arquitectura de los productos (Coloso, desarrollos Moodle, integraciones) incorpora los controles de seguridad definidos en estas políticas.
- Aprueba los cambios significativos en infraestructura y plataformas de producción, asegurando la aplicación de la gestión de cambios.
- Vela por la implementación técnica de los controles: hardening, cifrado, respaldos, monitoreo, gestión de vulnerabilidades y parches.

- Coordina la respuesta técnica ante incidentes de seguridad y la ejecución de los planes de continuidad y recuperación tecnológica.
- Gestiona la relación de seguridad con proveedores de infraestructura y servicios en la nube.

5.3 Oficial de Seguridad de la Información

- Administra el SGSI: elabora, actualiza y divulga las políticas, procedimientos y estándares de seguridad.
- Lidera la identificación, análisis, evaluación y tratamiento de riesgos de seguridad de la información, y mantiene la matriz de riesgos y la declaración de aplicabilidad.
- Gestiona el registro, clasificación, escalamiento y cierre de incidentes de seguridad, incluyendo el reporte a clientes y autoridades cuando aplique.
- Define y ejecuta el plan de concienciación y formación en seguridad para todos los colaboradores.
- Coordina las auditorías internas y externas del SGSI y hace seguimiento a los planes de acción derivados.
- Verifica el cumplimiento de la normativa de protección de datos personales (Ley 1581 de 2012) y atiende los requerimientos de titulares y autoridades en coordinación con la Gerencia.
- Reporta periódicamente a la Gerencia General el estado de la seguridad de la información mediante indicadores.

5.4 Líderes de proyecto y de área

- Actúan como propietarios de los activos de información de sus procesos y proyectos, definiendo su clasificación y los accesos requeridos.
- Garantizan que los requisitos de seguridad de los contratos con clientes se trasladen a los equipos de trabajo y se cumplan durante la ejecución.
- Autorizan y revisan periódicamente los accesos de sus equipos a los sistemas bajo su responsabilidad.

5.5 Colaboradores, contratistas y terceros

- Conocen y cumplen estas políticas y los procedimientos que las desarrollan.
- Protegen las credenciales, equipos e información que se les asignen, y los utilizan exclusivamente para fines laborales autorizados.
- Reportan de inmediato al Oficial de Seguridad cualquier incidente, debilidad o comportamiento anómalo que detecten.
- Suscriben acuerdos de confidencialidad como condición para acceder a información de Lábtica o de sus clientes.

5.6 Comité de Seguridad de la Información

Conformado, como mínimo, por la Gerencia General, el Director de Tecnología y el Oficial de Seguridad de la Información. Se reúne al menos trimestralmente para: revisar el estado de riesgos,

incidentes e indicadores; aprobar excepciones a las políticas; priorizar inversiones en seguridad; y hacer seguimiento a los planes de tratamiento de riesgos y auditorías.

6. Políticas complementarias

Las siguientes políticas desarrollan la Política General y se alinean con los controles del Anexo A de ISO/IEC 27001:2022. Cada política podrá ser detallada mediante procedimientos, estándares e instructivos específicos.

6.1 Política de gestión de activos de información

Controles relacionados: A.5.9 a A.5.11.

- Se mantiene un inventario actualizado de activos de información: plataformas, servidores, servicios en la nube, bases de datos, repositorios de código, dominios, licencias, equipos de cómputo y activos de información documental.
- Todo activo tiene un propietario designado, responsable de su clasificación, protección y revisión de accesos.
- Los equipos y activos asignados deben devolverse al finalizar la vinculación o el contrato, y los accesos asociados se revocan de inmediato.
- El uso de activos de Lábtica para fines personales, comerciales ajenos o ilícitos está prohibido.

6.2 Política de clasificación y manejo de la información

Controles relacionados: A.5.12 a A.5.14.

La información se clasifica en los siguientes niveles:

Nivel	Descripción	Ejemplos
Pública	Puede divulgarse sin restricción	Sitio web, material comercial publicado
Uso Interno	Para colaboradores de Lábtica; su divulgación causa impacto menor	Procedimientos internos, comunicaciones generales
Confidencial	Restringida a roles autorizados; su divulgación causa impacto significativo	Contratos, propuestas comerciales, código fuente, configuraciones
Restringida	Máximo nivel; su divulgación causa impacto grave legal o contractual	Datos personales de estudiantes, credenciales, respaldos de bases de datos de clientes

- Toda información de clientes tratada en el marco de un contrato se considera, como mínimo, Confidencial.
- La información Confidencial y Restringida solo se comparte por canales autorizados y cifrados, con destinatarios autorizados, y nunca por canales personales.

- La transferencia de información a terceros requiere acuerdo de confidencialidad o contrato que incorpore obligaciones de seguridad.

6.3 Política de control de acceso

Controles relacionados: A.5.15 a A.5.18, A.8.2 a A.8.5.

- El acceso a sistemas, plataformas e información se otorga bajo los principios de mínimo privilegio y necesidad de conocer, mediante solicitud aprobada por el líder correspondiente.
- Cada usuario cuenta con una cuenta nominal e intransferible. Las cuentas genéricas o compartidas están prohibidas salvo excepción aprobada por el Oficial de Seguridad, con controles compensatorios.
- Las cuentas privilegiadas (administradores de plataforma, servidores, paneles de infraestructura, consolas cloud) se asignan de forma restrictiva, se usan solo para tareas administrativas y cuentan con autenticación multifactor obligatoria.
- Los accesos se revisan al menos semestralmente, y de inmediato ante cambios de rol o desvinculación. La revocación de accesos por desvinculación se ejecuta el mismo día de la salida.
- El acceso de clientes a sus tenants y plataformas se limita a su propio espacio lógico; el aislamiento entre tenants es un requisito de arquitectura de Coloso y de toda plataforma multi-tenant operada por Lábtica.
- El acceso remoto a infraestructura de producción se realiza únicamente por canales cifrados (SSH con llaves, VPN o equivalente) y desde equipos autorizados.

6.4 Política de contraseñas y autenticación

Controles relacionados: A.5.17, A.8.5.

- Las contraseñas tienen una longitud mínima de 12 caracteres y combinan mayúsculas, minúsculas, números y símbolos; se prohíbe reutilizar contraseñas de servicios personales.
- La autenticación multifactor (MFA) es obligatoria para: correo corporativo, consolas de infraestructura y nube, paneles de administración, repositorios de código, herramientas de automatización y cualquier cuenta con privilegios administrativos.
- Las contraseñas se almacenan y comparten exclusivamente mediante el gestor de contraseñas corporativo aprobado; se prohíbe almacenarlas en texto plano, documentos, chats o correos.
- Las credenciales de servicios, API keys, tokens y secretos de integración se gestionan mediante mecanismos seguros (gestores de secretos o variables de entorno protegidas), nunca se incluyen en el código fuente ni en repositorios, y se rotan ante cualquier sospecha de exposición.
- Las contraseñas por defecto de cualquier sistema o plataforma se cambian antes de su puesta en producción.

6.5 Política de seguridad ligada al personal

Controles relacionados: A.6.1 a A.6.8.

- Previo a la vinculación, se verifican antecedentes y referencias de los candidatos en proporción a la criticidad del rol y conforme a la ley.
- Todo colaborador y contratista suscribe un acuerdo de confidencialidad y una cláusula de aceptación de estas políticas al inicio de su vinculación; las obligaciones de confidencialidad subsisten tras la terminación.
- Todo el personal recibe inducción en seguridad de la información al ingresar y formación de refuerzo al menos una vez al año, incluyendo concienciación sobre phishing e ingeniería social.
- El proceso de desvinculación incluye la devolución de activos, la revocación de accesos y el recordatorio formal de las obligaciones de confidencialidad.
- El incumplimiento de las políticas de seguridad se gestiona a través del proceso disciplinario interno y puede acarrear la terminación del contrato y acciones legales.

6.6 Política de uso aceptable, escritorio y pantalla limpios

Controles relacionados: A.5.10, A.7.7.

- Los recursos tecnológicos se destinan a fines laborales. Se prohíbe instalar software no licenciado o no autorizado, deshabilitar controles de seguridad y conectar dispositivos no autorizados a la infraestructura.
- Las sesiones se bloquean al ausentarse del puesto de trabajo; los equipos se configuran con bloqueo automático.
- La información física Confidencial o Restringida no se deja a la vista en puestos de trabajo, impresoras o salas; se almacena bajo llave y se destruye de forma segura cuando ya no se requiere.
- Se prohíbe el uso de cuentas o servicios personales (correo, mensajería, almacenamiento en la nube) para tratar información de Lábtica o de sus clientes.
- El uso de herramientas de inteligencia artificial de terceros con información Confidencial o Restringida requiere que la herramienta esté aprobada por el Oficial de Seguridad y configurada para no retener ni entrenar con los datos.

6.7 Política de teletrabajo y dispositivos móviles

Controles relacionados: A.6.7, A.7.9, A.8.1.

- El trabajo remoto se realiza desde redes confiables; se prohíbe operar infraestructura de producción desde redes WiFi públicas sin VPN.
- Los equipos utilizados para el trabajo cuentan con: cifrado de disco, antimalware, bloqueo de pantalla, actualizaciones automáticas y sesión de usuario personal separada.
- La pérdida o robo de un dispositivo con información o accesos corporativos se reporta de inmediato como incidente de seguridad para revocar sesiones y credenciales.
- El uso de equipos personales (BYOD) para acceder a información Confidencial o Restringida requiere autorización y el cumplimiento de los mismos controles mínimos.

6.8 Política de copias de respaldo

Controles relacionados: A.8.13.

- Toda plataforma de producción (Coloso, instancias Moodle administradas, bases de datos, servicios de automatización e integración, repositorios) cuenta con un esquema de respaldo documentado que define alcance, frecuencia, retención y ubicación.
- Los respaldos de producción se realizan al menos diariamente, se almacenan cifrados y al menos una copia se mantiene en una ubicación o proveedor distinto al del entorno productivo.
- Se realizan pruebas de restauración al menos semestralmente por plataforma crítica, dejando evidencia del resultado.
- La retención de respaldos respeta los compromisos contractuales con cada cliente y la normativa aplicable; al terminar un contrato, los datos del cliente se devuelven o eliminan de forma segura y certificada según lo pactado.

6.9 Política de criptografía

Controles relacionados: A.8.24.

- Toda comunicación de las plataformas con usuarios finales y entre servicios se cifra en tránsito mediante TLS 1.2 o superior, con certificados vigentes y renovación automatizada.
- Los datos Restringidos (datos personales, credenciales, respaldos) se cifran en reposo utilizando algoritmos estándar de la industria.
- Las contraseñas de usuarios en las plataformas se almacenan únicamente mediante funciones hash robustas con sal; nunca en texto plano ni con cifrado reversible.
- Las llaves y certificados se gestionan de forma centralizada; su custodia corresponde al equipo de infraestructura bajo supervisión del Director de Tecnología.

6.10 Política de seguridad en la nube y con proveedores

Controles relacionados: A.5.19 a A.5.23.

- Antes de contratar un proveedor que trate información de Lábtica o de sus clientes (nube, APIs de mensajería, herramientas SaaS), se evalúan sus condiciones de seguridad, privacidad y ubicación de los datos.
- Los contratos con proveedores incluyen obligaciones de confidencialidad, seguridad, notificación de incidentes y tratamiento de datos personales conforme a la Ley 1581 de 2012.
- Se aplica el modelo de responsabilidad compartida: Lábtica configura y opera de forma segura los servicios cloud contratados (hardening, control de acceso, cifrado, monitoreo), sin asumir que la seguridad es responsabilidad exclusiva del proveedor.
- La lista de proveedores críticos se revisa al menos anualmente, evaluando su desempeño en seguridad y continuidad.

6.11 Política de desarrollo seguro

Controles relacionados: A.8.25 a A.8.31.

- El ciclo de desarrollo de Coloso, plugins Moodle e integraciones incorpora requisitos de seguridad desde el diseño, incluyendo autenticación, autorización, validación de entradas, protección contra las vulnerabilidades del OWASP Top 10 y aislamiento multi-tenant.
- Los entornos de desarrollo, pruebas y producción están separados. Se prohíbe usar datos personales reales de clientes en entornos de desarrollo o pruebas; cuando sea indispensable, los datos se anonimizan o enmascaran.
- Todo el código se gestiona en repositorios con control de versiones y acceso controlado; los cambios a producción pasan por revisión de código y pruebas.
- Se prohíbe incluir secretos, credenciales o llaves en el código fuente.
- Las dependencias y librerías de terceros (incluidos plugins Moodle de la comunidad) se evalúan antes de su adopción y se mantienen actualizadas frente a vulnerabilidades conocidas.

6.12 Política de gestión de vulnerabilidades y actualizaciones

Controles relacionados: A.8.8.

- Los sistemas operativos, plataformas (Moodle y sus plugins, servicios de integración) y componentes de infraestructura se mantienen en versiones soportadas y con parches de seguridad al día.
- Las vulnerabilidades críticas con explotación conocida se corrigen o mitigan en un plazo máximo de 72 horas; las altas, en 15 días; las medias y bajas, según priorización de riesgo.
- Se realizan análisis de vulnerabilidades periódicos sobre las plataformas expuestas a Internet, y pruebas de penetración cuando los contratos con clientes lo requieran o ante cambios mayores de arquitectura.
- Los hallazgos de auditorías y pruebas de seguridad se gestionan mediante planes de remediación con responsables y fechas.

6.13 Política de registro, monitoreo y gestión de capacidad

Controles relacionados: A.8.15 a A.8.17, A.8.6.

- Las plataformas y servidores de producción generan registros (logs) de eventos de seguridad: autenticaciones, accesos administrativos, cambios de configuración y errores relevantes.
- Los registros se protegen contra alteración, se conservan al menos 12 meses (o el plazo contractual mayor) y su acceso está restringido.
- Se monitorea la disponibilidad, el desempeño y la capacidad de las plataformas críticas, con alertas que permitan actuar antes de una indisponibilidad.
- Los relojes de los sistemas se sincronizan mediante NTP para garantizar la trazabilidad de los eventos.

6.14 Política de gestión de cambios

Controles relacionados: A.8.32.

- Todo cambio sobre plataformas o infraestructura de producción (actualizaciones de Moodle, despliegues de Coloso, cambios de configuración, migraciones) se planifica, se prueba, se aprueba y se documenta, incluyendo el plan de reversa.
- Los cambios mayores se ejecutan en ventanas de mantenimiento acordadas con los clientes cuando puedan afectar la disponibilidad.
- Los cambios de emergencia se documentan y aprueban retroactivamente en un plazo máximo de 5 días hábiles.

6.15 Política de gestión de incidentes de seguridad

Controles relacionados: A.5.24 a A.5.28, A.6.8.

- Todo colaborador o tercero reporta de inmediato al Oficial de Seguridad de la Información cualquier incidente, sospecha o debilidad de seguridad, a través del canal definido para ello.
- Los incidentes se registran, clasifican por severidad, contienen, erradican y documentan; las lecciones aprendidas alimentan la mejora del SGSI.
- Cuando un incidente afecte información de un cliente, se le notifica de forma oportuna conforme a los plazos contractuales pactados, con la información disponible sobre alcance, impacto y medidas adoptadas.
- Los incidentes que afecten datos personales se evalúan frente a la obligación de reporte a la Superintendencia de Industria y Comercio y de comunicación a los titulares, conforme a la normativa vigente.
- Se preserva la evidencia de los incidentes de forma que soporte investigaciones internas, contractuales o legales.

6.16 Política de continuidad del negocio y recuperación ante desastres

Controles relacionados: A.5.29, A.5.30, A.8.14.

- Lábtica mantiene un Plan de Continuidad de Negocio que identifica los procesos y plataformas críticos, sus tiempos objetivo de recuperación (RTO) y puntos objetivo de recuperación (RPO), y las estrategias de recuperación tecnológica.
- Las plataformas críticas cuentan con mecanismos de recuperación basados en respaldos verificados, redundancia o infraestructura alternativa, según su criticidad y los compromisos con los clientes.
- El plan se prueba al menos una vez al año mediante ejercicios o simulacros, y se actualiza ante cambios significativos de infraestructura o servicios.

6.17 Política de protección de datos personales y privacidad

Controles relacionados: A.5.34. Marco legal: Ley 1581 de 2012, Decreto 1377 de 2013 y demás normas concordantes.

- Lábtica trata los datos personales conforme a los principios de legalidad, finalidad, libertad, veracidad, transparencia, acceso restringido, seguridad y confidencialidad.

- Cuando Lábtica opera plataformas por cuenta de sus clientes, actúa como Encargado del tratamiento: trata los datos únicamente según las instrucciones del cliente Responsable, y los contratos incorporan las obligaciones correspondientes.
- Se aplica minimización de datos: las plataformas y formularios solo recogen los datos necesarios para la finalidad educativa o contractual.
- Los titulares pueden ejercer sus derechos de conocer, actualizar, rectificar y suprimir sus datos a través de los canales definidos en la Política de Tratamiento de Datos Personales de Lábtica, que complementa este documento.
- Las integraciones de mensajería y notificaciones (correo, WhatsApp u otros canales) se implementan con el consentimiento requerido y con proveedores que ofrezcan garantías adecuadas de protección de datos.
- Al finalizar la relación contractual, los datos personales se devuelven o suprimen de forma segura según lo pactado con cada cliente.

6.18 Política de seguridad física y ambiental

Controles relacionados: A.7.1 a A.7.14.

- La infraestructura de producción de Lábtica reside en centros de datos de proveedores cloud que cuentan con certificaciones reconocidas de seguridad física (por ejemplo, ISO 27001 o SOC 2 del proveedor).
- En las instalaciones de Lábtica, el acceso físico se controla y los visitantes son acompañados; los equipos se protegen contra robo, y los medios de almacenamiento se destruyen de forma segura al final de su vida útil.
- Los equipos portátiles no se dejan desatendidos en lugares públicos ni en vehículos.

6.19 Política de transferencia de información

Controles relacionados: A.5.14.

- La información Confidencial o Restringida se transmite únicamente por canales corporativos cifrados y aprobados; se prohíbe el envío de credenciales o datos personales masivos por correo o mensajería sin protección adicional.
- Los intercambios recurrentes de información con clientes (por ejemplo, cargues de usuarios, integraciones con sistemas académicos o CRM) se realizan mediante interfaces seguras: APIs autenticadas, SFTP o mecanismos equivalentes.
- Las entregas de información a clientes al cierre de proyectos se registran y se realizan a los contactos autorizados por el cliente.

7. Cumplimiento

- El cumplimiento de estas políticas es condición de la vinculación laboral o contractual con Lábtica.
- El incumplimiento se gestiona según su gravedad a través del reglamento interno de trabajo, las cláusulas contractuales y, cuando corresponda, las acciones legales pertinentes.

- El Oficial de Seguridad de la Información verifica periódicamente el cumplimiento mediante revisiones, indicadores y auditorías internas, y reporta los resultados al Comité de Seguridad.
- Lábtica atiende los requerimientos de auditoría de seguridad de sus clientes conforme a lo pactado contractualmente.

8. Excepciones

Toda excepción a estas políticas debe solicitarse formalmente al Oficial de Seguridad de la Información, indicando la justificación, el alcance, la duración y los controles compensatorios propuestos. Las excepciones son aprobadas por el Comité de Seguridad de la Información, se documentan en un registro de excepciones y tienen una vigencia máxima de un año, renovable previa revisión.

9. Revisión y actualización

Este documento se revisa al menos una vez al año, y adicionalmente ante cambios significativos en la organización, la tecnología, la legislación, los contratos con clientes o como resultado de incidentes y auditorías. Las modificaciones son propuestas por el Oficial de Seguridad de la Información y aprobadas por la Gerencia General, dejando constancia en el control de versiones.

10. Referencias normativas

- ISO/IEC 27001:2022 — Seguridad de la información, ciberseguridad y protección de la privacidad. Requisitos.
- ISO/IEC 27002:2022 — Controles de seguridad de la información.
- Ley 1581 de 2012 y Decreto 1377 de 2013 — Protección de datos personales (Colombia).
- Ley 1273 de 2009 — Delitos informáticos (Colombia).
- Circulares y guías de la Superintendencia de Industria y Comercio aplicables al tratamiento de datos personales.
- Requisitos contractuales de seguridad de la información pactados con los clientes de Lábtica.

SEBASTIAN ROZO CADAVID
Director Ejecutivo
Cel. +57 300 780 0962

ANDRÉS SUCERQUIA OSORIO
Director de tecnología
Cel. +57 316 876 5086