SEGURIDAD ÉXITO
DE COLOMBIA

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD

CÓDIGO: PLE-PL-16 **VERSIÓN**: 01 **FECHA:** 09/03/2026

---

1. OBJETIVO

Establecer los compromisos, principios, responsabilidades y reglas obligatorias para proteger la información y los recursos tecnológicos de SEGURIDAD ÉXITO DE COLOMBIA LTDA., frente a amenazas internas y externas, accesos no autorizados, pérdida, alteración, divulgación, indisponibilidad o uso inadecuado. La política busca preservar la confidencialidad, integridad y disponibilidad de la información, apoyar la continuidad de las actividades administrativas, operativas y logísticas y fortalecer la seguridad de la cadena de suministro, en concordancia con el SGCS BASC.

2. ALCANCE

Aplica a todos los procesos, sedes, instalaciones, activos de información y recursos tecnológicos de la organización, incluidos equipos de cómputo, servidores, redes, aplicaciones, correo electrónico, almacenamiento local y en la nube, sistemas de respaldo, dispositivos y medios removibles. Es de obligatorio cumplimiento para colaboradores directos y temporales, directivos, practicantes, contratistas, proveedores, asociados de negocio y terceros que administren, procesen, almacenen, transmitan o puedan acceder a información o infraestructura de la empresa.

3. DEFINICIONES

Activo de información: Información, sistema, aplicación, equipo, soporte, red, servicio o recurso que tiene valor para la organización.

Confidencialidad: Propiedad por la cual la información solo está disponible para personas, procesos o entidades autorizadas.

Integridad: Propiedad que busca mantener la exactitud, consistencia y completitud de la información y evitar modificaciones no autorizadas.

Disponibilidad: Propiedad que permite acceder y utilizar la información y los sistemas cuando son requeridos por usuarios autorizados.

Ciberseguridad: Acciones y controles para proteger sistemas, redes, dispositivos y datos frente a amenazas digitales.

Incidente de seguridad: Evento real o sospechado que compromete o puede comprometer la confidencialidad, integridad o disponibilidad de la información o los servicios tecnológicos.

Mínimo privilegio: Asignación a cada usuario únicamente de los permisos necesarios para cumplir sus funciones.

Tercero: Persona u organización externa que presta servicios, suministra bienes o accede a información o recursos de la empresa.

4. DECLARACIÓN DE LA POLÍTICA

La Alta Dirección de SEGURIDAD ÉXITO DE COLOMBIA LTDA. reconoce que la información y la infraestructura tecnológica son activos esenciales para la prestación de sus servicios, la confianza de sus clientes y asociados de negocio y la continuidad de sus procesos. Por lo tanto, se compromete a:

Proteger la información en cualquier medio, formato, ubicación o estado, preservando su confidencialidad, integridad, disponibilidad y privacidad.
Gestionar los riesgos de seguridad de la información y ciberseguridad de acuerdo con el contexto, los procesos, la criticidad de los activos y el rol de la organización en la cadena de suministro.
Proteger los recursos informáticos mediante controles administrativos, físicos y tecnológicos proporcionales a los riesgos identificados.
Prevenir el acceso, uso, divulgación, copia, extracción, alteración, destrucción o pérdida no autorizados de la información.
Cumplir la legislación aplicable, los requisitos BASC, los compromisos contractuales y los acuerdos de confidencialidad.
Promover el uso seguro y responsable de las tecnologías de información y fortalecer la cultura de seguridad mediante inducción, capacitación y sensibilización.
Asignar los recursos y responsabilidades necesarios para implementar, mantener y mejorar los controles de seguridad.
Responder ante incidentes, comunicar oportunamente las amenazas relevantes y recuperar la información y los servicios prioritarios.
Aplicar medidas correctivas y disciplinarias, de acuerdo con los procedimientos internos y la legislación aplicable, frente al incumplimiento de esta política.

5. PRINCIPIOS DE SEGURIDAD

Responsabilidad compartida: Toda persona con acceso a información o tecnología debe protegerla y reportar situaciones sospechosas.
Prevención y resiliencia: Los controles deben prevenir incidentes, facilitar su detección y reducir sus impactos.

Mínimo privilegio y necesidad de conocer: Los permisos se asignan según las funciones y la necesidad de acceso.
Trazabilidad: Las altas, modificaciones, bajas, accesos privilegiados, incidentes y actividades relevantes deben dejar evidencia verificable.
Proporcionalidad basada en riesgo: La intensidad de los controles se determina según la criticidad del activo y el impacto potencial.
Mejora continua: Los controles se revisan y ajustan a partir de auditorías, incidentes, cambios y resultados de pruebas.

6. LINEAMIENTOS OBLIGATORIOS

6.1 Gestión de activos y clasificación de la información

El área de TI mantendrá actualizado el inventario de activos de información y tecnológicos, con identificación del activo, responsable, ubicación, uso, criticidad y controles aplicables.
La información se clasificará en las categorías definidas por la organización: Confidencial, Clasificada, Compartida y Pública. La clasificación considerará su impacto sobre la confidencialidad, integridad y disponibilidad y los requisitos legales o contractuales.
Los responsables de proceso deben identificar la información que generan, reciben, almacenan o comparten y asegurar que se trate conforme a su clasificación.

6.2 Gestión de identidades, autenticación y control de acceso

Cada usuario tendrá una cuenta individual. Se prohíbe compartir cuentas, contraseñas o credenciales, salvo cuentas técnicas o de servicio formalmente autorizadas, documentadas y controladas.

Las contraseñas deberán ser robustas, mantenerse bajo reserva y cambiarse cuando exista sospecha o evidencia de compromiso, cuando lo exija el sistema o cuando TI lo determine por riesgo. No deben almacenarse en archivos abiertos ni compartirse por canales inseguros.

Los accesos se concederán previa solicitud y aprobación del responsable del proceso y de TI, conforme al rol, nivel de criticidad y principio de mínimo privilegio.

El registro de usuarios debe identificar usuarios internos y externos, sistema al que acceden, nivel de criticidad, permisos y responsable de aprobación. Se revisará al menos semestralmente y cada vez que haya cambios de cargo, funciones o vinculación.

Al terminar la relación laboral, contractual o de servicio, el responsable correspondiente notificará oportunamente a TI para deshabilitar o retirar los accesos, credenciales, sesiones y permisos asociados.

Los privilegios de administrador o superusuario se limitarán a personal autorizado, se documentarán y revisarán semestralmente. Su uso debe ser trazable y justificado.

Se implementará autenticación multifactor para accesos críticos y remotos cuando la plataforma lo permita y de acuerdo con el plan de implementación aprobado por TI. La VPN u otra tecnología segura se habilitará cuando el análisis de riesgo y la necesidad de acceso remoto lo requieran.

6.3 Uso aceptable de equipos, software, correo e internet

Los equipos, cuentas, aplicaciones, redes y servicios corporativos se utilizarán para fines autorizados y relacionados con las actividades de la organización.

Se prohíbe instalar, descargar o ejecutar software no autorizado, sin licencia o de procedencia no confiable. Toda adquisición o instalación deberá contar con aprobación correspondiente y gestión de TI.

Los sistemas operativos y aplicaciones deberán mantenerse licenciados y actualizados. TI verificará el estado de parches y licencias, y administrará las soluciones antimalware corporativas.

Los usuarios deberán abstenerse de abrir archivos, enlaces o adjuntos sospechosos, entregar credenciales, desactivar controles de seguridad o utilizar sitios y servicios que pongan en riesgo la información.

El correo corporativo y las plataformas institucionales deberán utilizarse para las comunicaciones de trabajo. No se deberá transferir información corporativa a cuentas personales ni a servicios de almacenamiento no autorizados.

Las herramientas autorizadas para reuniones y videoconferencias son Google Meet y Microsoft Teams, mediante cuentas corporativas. Cualquier plataforma adicional requiere aprobación de TI.

6.4 Protección de equipos, sesiones y dispositivos

Los usuarios deberán bloquear la sesión al abandonar su puesto de trabajo, incluso por periodos cortos. Los equipos corporativos tienen configurado bloqueo automático por inactividad de cinco (5) minutos, sujeto a verificación por TI.

Se prohíbe dejar equipos desbloqueados o permitir que personas no autorizadas utilicen una sesión abierta.

La conexión de computadores, celulares, tabletas, memorias USB, discos externos, impresoras u otros periféricos personales está prohibida, salvo autorización expresa de TI y aplicación de controles.

Los periféricos y medios removibles autorizados deberán ser revisados antes de su uso. La información almacenada en ellos deberá protegerse y eliminarse de forma segura cuando ya no sea necesaria.

La red de invitados deberá permanecer segregada de la red interna y será administrada por TI mediante credenciales temporales.

6.5 Seguridad de infraestructura, redes y acceso remoto

Solo TI podrá autorizar la incorporación de equipos a la red corporativa y administrar los componentes de infraestructura tecnológica.

El acceso remoto a equipos y sistemas mediante AnyDesk, TeamViewer u otras herramientas similares está reservado al Responsable de TI. Los accesos excepcionales de terceros o usuarios deberán contar con autorización previa de Gerencia, alcance definido, duración limitada y registro.

Se prohíbe el acceso remoto desde dispositivos personales o no autorizados. TI deberá verificar y bloquear conexiones no autorizadas cuando sean detectadas.

Las credenciales de acceso remoto y de administración se mantendrán bajo control de TI y no se divulgarán a usuarios no autorizados.

Los equipos, servidores, redes y áreas donde se alojan activos tecnológicos deberán contar con controles físicos y de acceso acordes con su criticidad.

6.6 Protección contra malware y gestión de vulnerabilidades

Los equipos corporativos deberán contar con la solución antimalware aprobada por la organización, actualmente Kaspersky según el inventario y las licencias vigentes. TI verificará su actualización, funcionamiento y alertas.

Los sistemas operativos y aplicaciones corporativas deberán recibir actualizaciones y parches de seguridad oportunamente. TI conservará evidencia de las verificaciones y de las acciones realizadas.

TI evaluará la seguridad de hardware, software, redes y aplicaciones al menos una vez al año. La organización podrá mantener una periodicidad semestral como control interno cuando resulte pertinente.
Los hallazgos de vulnerabilidad deberán registrarse, valorarse por riesgo, asignarse a un responsable y contar con acciones correctivas y fechas de seguimiento hasta su cierre.
Las adquisiciones o cambios tecnológicos deberán someterse a revisión de necesidad, aprobación de Gerencia y evaluación de seguridad por TI antes de su puesta en operación.

6.7 Copias de seguridad, recuperación y continuidad
La información sensible y crítica deberá contar con copias de seguridad periódicas, protegidas contra acceso, modificación o eliminación no autorizados.

La organización dispone de respaldos locales en servidor para la aplicación Helisa y archivos de usuarios, y de respaldos externos de correos y documentación mediante el proveedor Davinci/Google Drive, de acuerdo con los servicios y contratos vigentes.

TI administrará los respaldos locales y verificará la ejecución de las copias. Los accesos a respaldos estarán restringidos y protegidos mediante credenciales seguras.
Se realizarán pruebas de restauración al menos una vez al año y se documentarán los resultados, tiempos de recuperación, desviaciones y acciones de mejora.

La recuperación de sistemas e información priorizará los activos según su criticidad y se coordinará con el programa de continuidad del negocio.

6.8 Monitoreo, registros e investigación de incumplimientos
TI establecerá controles para identificar y revisar accesos no autorizados, actividad inusual, incumplimientos de las políticas y posibles manipulaciones o alteraciones no autorizadas de datos comerciales.
Se conservarán, según la disponibilidad de las plataformas y los requisitos aplicables, registros de accesos, cambios, eventos de seguridad, administración de cuentas, antivirus y respaldos.
Los hallazgos e incidentes deberán documentarse, analizarse y escalarse al responsable del proceso, SIG y Gerencia, según su impacto.
Los registros de auditoría se consultarán únicamente por personal autorizado y se protegerán contra alteración o eliminación no autorizada.

6.9 Gestión y comunicación de amenazas e incidentes
Todo colaborador o tercero deberá reportar inmediatamente a TI y/o a su jefe inmediato cualquier pérdida de equipo, correo sospechoso, malware, acceso irregular, divulgación accidental, alteración de información o indisponibilidad de sistemas.

TI evaluará la criticidad del evento, aplicará medidas de contención y recuperación, conservará evidencias y coordinará la investigación con SIG y Gerencia.
Cuando una amenaza o incidente pueda afectar a procesos, clientes, proveedores, asociados de negocio o autoridades, se comunicará oportunamente a las partes interesadas correspondientes, de acuerdo con los requisitos legales y contractuales.
Las comunicaciones sobre incidentes deberán ser autorizadas por la Gerencia o el responsable designado. Los usuarios no deberán divulgar información del incidente por canales no autorizados.

6.10 Proveedores, terceros y asociados de negocio

Los terceros que accedan a información o infraestructura deberán contar con autorización, acceso limitado y acuerdos de confidencialidad y seguridad cuando corresponda.
Los proveedores críticos de tecnología deberán identificarse y evaluarse considerando su impacto sobre la confidencialidad, integridad y disponibilidad de los sistemas y la información.
Los accesos de soporte técnico externo deberán ser temporales, supervisados, autorizados y registrados. Al finalizar el servicio se retirarán los permisos concedidos.
Los requisitos de seguridad aplicables deberán incorporarse en contratos, acuerdos de servicio o compromisos documentados.

6.11 Inventario, mantenimiento y disposición final de equipos

TI mantendrá actualizado el inventario de computadores, servidores, dispositivos de red, medios y demás equipos que hagan parte de la infraestructura informática.
El inventario se actualizará por adquisición, asignación, traslado, cambio, devolución o retiro de activos y se verificará periódicamente.
Antes de dar de baja o entregar un equipo, se deberá proteger, respaldar cuando aplique y eliminar de forma segura la información contenida. La baja se documentará mediante el acta correspondiente.
Los residuos de aparatos eléctricos y electrónicos se entregarán a gestores autorizados, conservando actas o certificados de disposición final conforme a la legislación aplicable.

6.12 Capacitación, sensibilización y simulacros

Los colaboradores y terceros, según su nivel de acceso, recibirán orientación sobre clasificación de información, manejo de credenciales, uso aceptable, phishing, protección de datos, reporte de incidentes y uso seguro de plataformas.
TI y SIG coordinarán ejercicios prácticos y simulacros para evaluar la eficacia de los controles. Se podrán realizar simulaciones controladas de phishing y ejercicios de restauración de copias de seguridad.

Cada ejercicio deberá contar con objetivo, alcance, participantes, resultados, lecciones aprendidas y plan de acción cuando se identifiquen oportunidades de mejora.

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDA

CÓDIGO: PLE-PL-16 **VERSIÓN**: 01 **FECHA:** 09/03/2026

6.13 Revisión y actualización de la política

Esta política y los procedimientos asociados se revisarán como mínimo una vez al año por TI y SIG, y de manera extraordinaria ante cambios tecnológicos, organizacionales, legales, contractuales, incidentes relevantes o materialización de riesgos.

Las modificaciones serán elaboradas por TI, revisadas por SIG y aprobadas por la Gerencia General antes de su divulgación.

Se conservará el historial de versiones, fechas, responsables y descripción de cambios.

7. DISPOSICIONES FINALES

La política será divulgada a todos los colaboradores y puesta a disposición de las partes interesadas pertinentes. Su conocimiento y cumplimiento serán obligatorios para quienes tengan acceso a información o recursos tecnológicos de SEGURIDAD ÉXITO DE COLOMBIA LTDA. La divulgación deberá dejar evidencia mediante comunicaciones, inducciones, capacitaciones o aceptación documentada.

8. INCUMPLIMIENTO

El incumplimiento de esta política podrá dar lugar a la suspensión o revocación de accesos, medidas administrativas, acciones correctivas o medidas disciplinarias conforme al Reglamento Interno de Trabajo, los contratos, los procedimientos de la organización y la legislación aplicable. Cuando corresponda, se informará a las autoridades o partes interesadas pertinentes. Toda actuación deberá quedar documentada y respetar el debido proceso.

9. APROBACIÓN

Para constancia se firma por la Representante Legal de SEGURIDAD Y VIGILANCIA ÉXITO DE COLOMBIA LTDA.

Martha Beatriz Naranjo Estupiñán
Representante Legal