Política de seguridad de la información

Políticas corporativas

POL SI 001 • Versión 1.0 • 13 de octubre de 2026

Hummingbird Consulting S.A.S. establece los siguientes criterios para proteger la confidencialidad, integridad y disponibilidad de la información que administra en su operación, consultoría y servicios de software. Aplican a sus administradores, colaboradores, contratistas y proveedores con acceso autorizado.

1 Gobierno y responsabilidad

La representación legal aprueba esta política, asigna recursos y acepta o escala los riesgos que no puedan corregirse de inmediato. La función técnica implementa y mantiene los controles. Toda persona con acceso debe cumplirlos y reportar desviaciones.

Cuando una misma persona desempeñe funciones de dirección y desarrollo, deberá documentar los cambios relevantes y sus verificaciones. Las actividades sensibles se someterán a revisión adicional según el riesgo y la disponibilidad de un tercero competente sujeto a confidencialidad.

2 Clasificación y acceso

La información se clasificará como pública, interna, confidencial o restringida según el daño que pudiera ocasionar su exposición. Los reportes éticos, datos sensibles, credenciales y evidencias de investigaciones requieren acceso especialmente limitado.

Los permisos se asignarán por necesidad de la función, empresa y módulo. Se revisarán ante cambios de rol y retiros. Las cuentas administrativas deben utilizar autenticación reforzada cuando esté disponible. No se compartirán contraseñas ni se enviarán claves de servicio por canales públicos.

La separación entre empresas debe aplicarse en la autorización efectiva de acceso a datos y archivos. Ocultar un botón o una pantalla no constituye por sí mismo un control de autorización.

3 Operación y desarrollo

Los cambios relevantes deben documentarse, revisarse y verificarse antes de pasar a producción, con un mecanismo de reversión razonable. Los entornos de prueba utilizarán datos ficticios o debidamente anonimizados cuando sea posible.

Se aplicarán actualizaciones de seguridad y revisión de dependencias según criticidad. Las comunicaciones utilizarán mecanismos seguros adecuados. Los registros técnicos se limitarán a lo necesario y no deben almacenar contraseñas ni divulgar contenido confidencial innecesario.

Las pruebas de seguridad requieren autorización, alcance y coordinación previa. No se admite acceso a información de otra empresa mediante alteración de enlaces, identificadores o permisos.

4 Archivos y evidencias

Los adjuntos de reportes, contratos y documentos de clientes deben estar sujetos a controles de acceso. Los enlaces que permiten descargar un archivo por su sola posesión se tratarán como información reservada y se limitarán o revocarán cuando corresponda.

Los destinatarios de notificaciones deben ser gestores autorizados. Se evitará enviar por correo el relato completo, datos sensibles o evidencias cuando baste con avisar la existencia de un caso y exigir acceso autorizado al sistema.

5 Respaldo y continuidad

HMB definirá la frecuencia y retención de copias por servicio y riesgo, verificará su ejecución y realizará pruebas de recuperación. Los respaldos deben quedar protegidos frente a acceso indebido y eliminación accidental.

Los tiempos de recuperación, puntos de recuperación y niveles de disponibilidad solo serán compromisos contractuales cuando estén definidos expresamente. El nivel de servicio de un proveedor de nube no se convierte automáticamente en el nivel de servicio de toda la aplicación.

6 Proveedores y trabajo remoto

Los proveedores se evaluarán de acuerdo con el tipo de información y la criticidad del servicio. Se documentarán las condiciones de tratamiento, acceso, ubicación y respuesta a incidentes pertinentes. La subcontratación no elimina las obligaciones de HMB.

Los equipos de trabajo deben contar con bloqueo de pantalla, actualizaciones y medidas de protección apropiadas. Se prohíbe utilizar cuentas personales o herramientas de IA no autorizadas para almacenar o procesar datos confidenciales de clientes.

7 Gestión de incidentes

Las sospechas de acceso indebido, fuga, alteración o pérdida se reportarán a administracion@hmb-sas.com o al +57 322 528 5544. No es necesario demostrar el incidente para comunicar una señal. El reporte debe evitar reenviar información sensible innecesaria.

HMB registrará, clasificará y contendrá el incidente; preservará evidencia; evaluará impacto; coordinará recuperación y acciones correctivas; e informará a clientes, titulares o autoridades cuando exista obligación. Las notificaciones se efectuarán en los plazos legales y contractuales aplicables, con la información disponible y actualizaciones posteriores si son necesarias.

8 Relación con clientes y revisión

Los clientes administran sus usuarios, datos y decisiones de negocio dentro de las funciones contratadas. HMB debe facilitarles instrucciones de uso y soporte y responder por sus obligaciones. Ninguna política traslada automáticamente toda la responsabilidad de seguridad al cliente.

La representación legal revisará esta política al menos anualmente y después de cambios relevantes o incidentes significativos. Los incumplimientos se gestionarán con respeto del debido proceso y de los contratos. Esta política expresa compromisos de gestión y no acredita una certificación de seguridad.

Esta versión entra en vigor con su aprobación y publicación. Contacto: HUMMINGBIRD CONSULTING S.A.S., NIT 901.902.294-8, Avenida 80 No. 28-90, Medellín, Colombia.