Sistema de Gestión de la Seguridad de la Información (SGSI)

1. SGSI-BTK 27001:2022

Sistema de Gestión de la Seguridad de la Información

Qué es: Norma que establece los requisitos para establecer, implementar, mantener y mejorar un SGSI.

Objetivo: Proteger la confidencialidad, integridad y disponibilidad de la información.

Aspectos clave: Análisis de riesgos, controles, gestión de incidentes, seguridad tecnológica.

Beneficios clave:

- Protección integral de datos biométricos, altamente sensibles, frente a accesos no autorizados, pérdidas, filtraciones o manipulaciones.
- Generación de confianza con clientes (empresas y entidades) al demostrar que se gestionan los datos críticos bajo estándares internacionales de seguridad.
- Cumplimiento normativo con regulaciones locales e internacionales sobre protección de datos e información personal (ej. leyes de protección de datos, Habeas Data).
- Fortalecimiento de la reputación corporativa como proveedor tecnológico confiable y seguro.
- Prevención y gestión de incidentes de ciberseguridad, minimizando impactos económicos, legales y operacionales.

Hito en Biometrika:

Actualmente, este sistema se encuentra oficialmente certificado por un ente acreditado, garantizando que la organización protege la confidencialidad, integridad y disponibilidad de sus activos de información frente a las amenazas actuales.

Ver Certificado ISO/IEC 27001:2022

2. SGPI-BTK 27701:2019

Sistema de Gestión de Privacidad de la Información

Qué es:

Extensión de la ISO 27001 para implementar un Sistema de Gestión de Información Personal (SGPI).

Objetivo:

Garantizar el cumplimiento legal* y ético en el tratamiento de datos personales, incluyendo biométricos.

Aspectos clave:

Consentimiento, derechos del titular, privacidad por diseño, minimización de datos.

Nota. * Atención a Ley O. Protección de Datos Personales (LOPDP).

Beneficios clave:

- Garantiza el cumplimiento de principios de privacidad por diseño y por defecto.
- Permite demostrar que la empresa gestiona datos personales conforme a estándares compatibles con RGPD, LOPD, y otras leyes de protección de datos.
- Proporciona directrices específicas para responsables y encargados del tratamiento de datos biométricos.
- Reduce el riesgo de sanciones legales, demandas o daños reputacionales por un uso inadecuado de datos personales.
- Refuerza la relación con el cliente y el usuario final, mediante la transparencia y control sobre cómo se recopilan, almacenan, procesan y eliminan los datos biométricos.

Hito en Biometrika:

Se ha implementado los controles y directrices de la norma ISO/IEC 27701, en estricto cumplimiento con la Ley de Protección de Datos Personales vigente en Ecuador, demostrando el compromiso de la empresa con la privacidad y el tratamiento ético y legal de la información de sus clientes y colaboradores.

Además, Biometrika cuenta con la definición del Delegado de Protección de Datos Personales, asegurando la garantía y confianza legal de los servicios de Biometrika.

www.biometrika.ec
Av. Shyris N34-328 y Portugal, Edif. Smerald Of. 1401
Quito-Ecuador
Telf. +(593) 25153 033

3. SGCN-BTK 22301:2019

Continuidad del Negocio

Qué es: Norma que proporciona un marco para planificar la resiliencia organizacional y garantizar operaciones continuas ante interrupciones.

Objetivo: Asegurar la disponibilidad y recuperación de servicios críticos.

Aspectos clave: Análisis de impacto (BIA), escenarios de crisis, recuperación ante desastres.

Sus datos son usados exclusivamente para los siguientes fines, determinados por su empleador:

Beneficios clave:

- Asegura la disponibilidad continua de los servicios biométricos, incluso ante fallas tecnológicas, ciberataques, desastres naturales o pandemias.
- Minimiza el tiempo de inactividad de los sistemas de control de acceso y asistencia.
- Mejora la resiliencia organizacional mediante una planificación estratégica para la recuperación rápida de operaciones.
- Refuerza la confianza del cliente al demostrar preparación frente a crisis y compromiso con la continuidad de los servicios.
- Alineación con requisitos de contratación pública o privada, donde la continuidad de los servicios es una exigencia contractual o de aseguradoras.

Hito en Biometrika:

Se han establecido las estrategias y planes de continuidad basados en las mejores prácticas de la norma ISO 22301, asegurando la capacidad de la organización para mantener sus operaciones críticas o recuperarlas en tiempos aceptables ante eventos disruptivos.

4. MODELO INTEGRADO DE GESTIÓN SGSI + SGCN + SGPI

Objetivo general del modelo

Diseñar, implementar y mantener un sistema integrado de gestión que asegure la seguridad, disponibilidad y privacidad de los datos biométricos de los colaboradores de empresas clientes, garantizando el cumplimiento normativo, la resiliencia operativa y la confianza de las partes interesadas.

Enfoque de integración

Los tres sistemas comparten principios clave:

- Gestión basada en riesgos
- Mejora continua (PDCA)
- Participación de la alta dirección
- Gestión documental y control de cambios
- Auditoría interna y revisión por la dirección.

Aspecto clave: Sistema de Gestión de Riesgos

Biometrika cuenta con un modelo integral de gestión de riesgos corporativos alineado con el marco COSO ERM (Enterprise Risk Management), permitiendo a la empresa identificar, evaluar y mitigar proactivamente los riesgos estratégicos y operativos.

BENEFICIOS DEL MODELO INTEGRADO

Beneficios Estratégicos

- Consolidación de la confianza del cliente al demostrar cumplimiento internacional.
- Eficiencia operativa al evitar duplicidad de procesos y documentación.
- Resiliencia organizacional, garantizando que los servicios biométricos estén siempre disponibles.
- Reducción de riesgos legales, reputacionales y técnicos.
- Ventaja competitiva frente a otros proveedores que no cumplen normas internacionales.

Beneficios para el Cliente Final

- Seguridad de sus datos biométricos
- Protección de su privacidad
- Confianza en la continuidad del servicio

Fin Documento