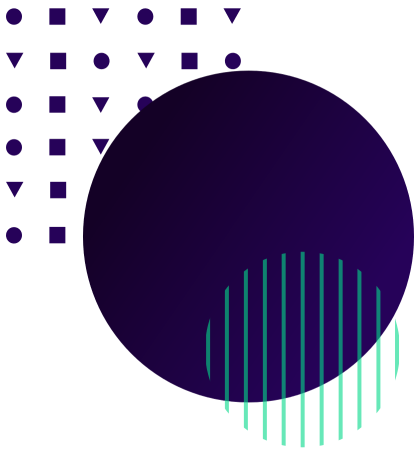
BIOMETRICS



POLÍTICA SISTEMA DE GESTIÓN DE SEGURIDAD DE INFORMACIÓN

Política

V 1.0
15/12/2020

Identificación del Documento

Identificación del documento	PO-03-05 Política sistema de gestión de seguridad de información
Registro(s) relacionado(s)	-
Documento(s) relacionado(s)	Política de Continuidad de Negocios Norma de Continuidad de Negocio y Norma Roles y Responsabilidades del Programa de Gestión de Continuidad del Negocio Política de Seguridad en las Operaciones Política y Manual de Sistema de Gestión de Calidad Norma de Apetito de Riesgo Norma de Gestión de Riesgo en procesos y proyectos.
Responsable de aprobación	Gerente General
Dueño funcional	Seguridad y Acreditaciones
Puesto(s) implicado(s)	Responsable del SGI, OSI, CEO, Gerente General, Líder de Proceso, Responsables de proceso.

Control de Versiones

Motivo:
Cambio del diseño del documento
Actualizar la documentación base para adaptarse a las normas de certificación

Responsable	Versión	Consultados/Revisión	Informados	Aprobación
Ingeniero de Procesos Analista Procesos	1.0	OSI PMO	Gerente de (TI) Gerente BI Gerente de Finanza y Administración Gerente Internacional Gerente I + D	Gerente General
Dic 2020		Dic 2020	Dic 2020	Dic 2020

Información del documento

1. Objetivo:

El propósito de esta Política es definir las directrices de la protección de los activos de la información de todas amenazas, internas o externas, deliberadas o accidentales, mediante la implementación de un Sistema de Gestión de Seguridad de Información.

La implantación de esta política es importante para mantener y demostrar nuestra integridad, confidencialidad y disponibilidad de los activos de la información con nuestros negocios con clientes y proveedores y nuestro personal.

2. Alcance:

Este documento contiene los lineamientos mínimos que debe considerar la TOC para el Sistema de Gestión de Seguridad de Información, de forma de garantizar que la seguridad de la información es gestionada correctamente, haciendo uso de un proceso sistemático, documentado y conocido por toda la organización, desde un enfoque de riesgo empresarial.

La presente política es de aplicación general, comprende a toda la empresa, y considera el involucramiento y compromiso de todo el personal, independientemente de su rango, función o localización, así como de sus proveedores.

3. Referencias:

Los siguientes documentos se consideran como referencia en la presente Política:

• Series ISO 9000, 31000, 20000-1, 27001, 22301.

4. Sistema de Gestión de Seguridad de la Información:

El propósito del SGSI es garantizar que los riesgos de la seguridad de la información sean conocidos, asumidos, gestionados y minimizados por la organización de una forma documentada, sistemática, estructurada, repetible, eficiente y adaptada a los cambios que se produzcan en los riesgos, el entorno y las tecnologías.

Se entiende por información todo aquel conjunto de datos organizados en poder de una entidad que posean valor para la misma, independientemente de la forma en que se guarde o transmita (escrita, en imágenes, oral, impresa en papel, almacenada

electrónicamente, proyectada, enviada por correo, fax o e-mail, transmitida en conversaciones, etc.), de su origen (de la propia organización o de fuentes externas) o de la fecha de elaboración.

La seguridad de la información, consiste en la preservación de su confidencialidad, integridad y disponibilidad, así como de los sistemas implicados en su tratamiento, dentro de la organización. Así pues, estos tres términos constituyen la base de la seguridad de información:

- **Confidencialidad:** la información no se pone a disposición ni se revela a individuos, entidades o procesos no autorizados.

- **Integridad:** mantenimiento de la exactitud y completitud de la información y sus métodos de proceso

- **Disponibilidad:** acceso y utilización de la información y los sistemas de tratamiento de la misma por parte de los individuos, entidades o procesos autorizados cuando lo requieran.

La información, junto a los procesos y sistemas que hacen uso de ella, son activos muy importantes en la organización. La confidencialidad, integridad y disponibilidad de información sensible pueden llegar a ser esenciales para mantener los niveles de competitividad, rentabilidad, conformidad legal e imagen empresarial necesarios para lograr los objetivos de la organización y asegurar beneficios económicos.

.

La organización y sus sistemas de información están expuestos a un número cada vez más elevado de amenazas que, aprovechando cualquiera de las vulnerabilidades existentes, pueden someter a activos críticos de información a diversas formas de fraude, espionaje, sabotaje o vandalismo. Los virus informáticos, el “hacking” o los ataques de denegación de servicio son algunos ejemplos comunes y conocidos, pero también se deben considerar los riesgos de sufrir incidentes de seguridad causados voluntaria o involuntariamente desde dentro de la propia organización o aquellos provocados accidentalmente por catástrofes naturales y fallos técnicos.

El SGSI establece políticas y procedimientos en relación a los objetivos de negocio de la organización, con objeto de mantener un nivel de exposición siempre menor al Apetito de Riesgo que la propia organización ha decidido asumir.

ESTRUCTURA DEL SGSI
El SGSI está formado por:
Políticas
1. Política de Sistema de Gestión de Seguridad de Información
2. Política de Gestión de Activos de Información
3. Política de Gestión de Seguridad de Información en las Operaciones
4. Política de Control de Accesos
5. Política de Seguridad de Información en Recursos Humanos
6. Política de Seguridad Lógica
7. Política de Seguridad Física y del Entorno
8. Política de Seguridad de Redes
9. Política de Cumplimiento y Protección de datos Personales
10. Política de Conexión Remota
11. Política de Criptografía
12. Política de Dispositivos Móviles y BYOD
13. Política de Relación con Proveedores
14. Política de Adquisición, Desarrollo y mantención de Sistemas
15. Política de Correo Electrónico, Uso de Internet y Transferencias de Información

Procedimientos
1. Procedimiento de Gestión de Activos de Información
2. Procedimiento de Seguridad en el Desarrollo y procesos de soporte
3. Procedimiento de Requisitos de Seguridad
4. Procedimiento de Seguridad en las Comunicaciones
5. Procedimiento de Gestión del cambio
6. Procedimiento de Seguridad de las Operaciones y Respaldos
7. Procedimiento de Seguridad en los Equipos
8. Procedimiento de Criptografía
9. Procedimiento de Gestión de Áreas Seguras
10. Procedimiento de Organización para la Seguridad de Información
11. Procedimiento de Gestión de Infraestructura
12. Procedimiento de Evaluación de Activos de Información
13. Procedimiento de Control de Accesos
14. Procedimiento de Cumplimiento
15. Procedimiento de Gestión de Incidentes, Problemas y Vulnerabilidades

Declaración de Aplicabilidad: (SOA -Statement of Applicability-, en sus siglas en inglés); documento que contiene los objetivos de control y los controles contemplados por el SGSI, basado en los resultados de los procesos de evaluación y tratamiento de riesgos, justificando inclusiones y exclusiones.

La evaluación de riesgos de Seguridad de Información se realizará utilizando los criterios de la Política de Riesgos y el Procedimiento de Evaluación de Riesgos y Oportunidades.

5. Roles y Responsabilidades:

5.1. Directorio, CEO, Gerente General

1. Aprobar las políticas del Sistema de Gestión de Seguridad de Información.
2. Asignar recursos al SGSI en todas sus fases.
3. Aprobar los criterios de aceptación de riesgos y sus correspondientes niveles.
4. Asegurar que se realizan auditorías internas.
5. Velar por el establecimiento, implementación, operación, monitoreo, control, revisión, mantenimiento y mejora continua del SGSI.

5.2. Comité de Riesgo

1. Aprobar el establecimiento de objetivos y planes del SGSI.
2. Aprobar roles y responsabilidades de seguridad de la información.
3. Supervisar la implementación, operación, monitoreo, revisión, mantención y mejora del SGSI.
4. Supervisar que los procedimientos de seguridad de la información apoyan los requerimientos de negocio.
5. Asegurar que todo el personal relevante esté consciente de la importancia de sus actividades de seguridad de la información y de cómo contribuye a la consecución de los objetivos del SGSI.

5.3. Gerente de Riesgo

1. Desarrollar y mantener las Políticas del Sistema de Gestión de Seguridad de Información.
2. Reportar la implementación, operación, monitoreo, revisión, mantención y mejora del SGSI.
3. Supervisar que los procedimientos de seguridad de la información apoyan los requerimientos de negocio.
4. Comunicar a la organización tanto la importancia de lograr los objetivos de seguridad de la información y de cumplir con la política de seguridad, como sus responsabilidades legales y la necesidad de mejora continua.

5.4. Oficial de Seguridad de Información (OSI)

1. Administrar y coordinar diariamente el Sistema de Gestión de Seguridad Información.
2. Desarrollar el Plan de Seguridad de la Información.

3. Ejecutar la evaluación de riesgos en seguridad de la información que abarque toda la organización.
4. Desarrollar los procedimientos de seguridad que fortalezcan las políticas de seguridad informática.
5. Guiar a la administración de la organización ante incidentes de seguridad mediante un Plan de Responder y atender notificaciones de incidentes y problemas.
6. Crear y mantener una base de datos para el registro de incidentes en la red, la cual debe poder ser accedida por los miembros del grupo de seguridad.
7. Coordinar la realización periódica de auditorías a las prácticas de seguridad informática, así como, dar seguimiento al corto plazo de las recomendaciones que hayan resultado
8. Ser el punto de referencia para todos los procesos de seguridad y ser capaz de guiar y aconsejar a los usuarios de la institución sobre cómo desarrollar procedimientos para la protección de los recursos de software y hardware.
9. Evaluar la eficacia de las acciones realizadas.
10. Proveer resultados de auditorías y revisiones del SGSI.
11. Proveer técnicas, productos o procedimientos que pudieran ser útiles para mejorar el rendimiento y eficacia del SGSI.
12. Realizar seguimiento y proveer información sobre el estado de acciones preventivas y correctivas.
13. Supervisar la gestión de vulnerabilidades o amenazas que no fueran tratadas adecuadamente en evaluaciones de riesgos anteriores.
14. Resultados de las mediciones de eficacia.

5.5. Gerencia de Operaciones

1. Implementar políticas y procedimientos del SGSI que corresponda.
2. Monitorear y controlar la implementación de las políticas y procedimientos del SGSI que corresponda.
3. Crear, desarrollar e implementar planes de acción para corregir desviaciones a las políticas y procedimientos del SGSI que corresponda.
4. Realizar seguimiento a las acciones correctivas que correspondan.
5. Informar resultados de la implementación, monitoreo, control y seguimientos a planes de acción al OSI.