Políticas de SGSI

Versión 1.2.1

Mayo 2024

Índice

1. Objetivo

2. Alcance

3. Vigencia

4. Responsabilidades

5. Autoridad de emisión, revisión y publicación

6. Términos y definiciones

7. Reglas de aplicación al SGSI

- 7.1 Comprender la organización y su contexto
  - 7.1.1 Declaración de Objetivos
  - 7.1.2 Contexto de SGSI
    - Análisis externo
    - Análisis interno
  - 7.1.3 Contexto de Gestión de Riesgos
- 7.2 Comprender las necesidades y expectativas de las partes interesadas
  - 7.2.1 Identificación y Análisis de las Partes Interesadas
  - 7.2.2 Identificación y Análisis de los Requisitos del Negocio de Partes Interesadas
    - Identificación de requisitos de CLIENTES
    - Identificación de requisitos de USUARIOS FINALES
    - Identificación de requisitos de SOCIOS
    - Identificación de requisitos de PROVEEDORES
    - Identificación de requisitos de EMPLEADOS
    - Identificación de requisitos de ASEGURADORAS
    - Identificación de requisitos de administración, legales y regulatorios
  - 7.2.3 Determinar el alcance del sistema de gestión de la seguridad de la información
    - Procesos y servicios
    - Características del negocio

Organización

Ubicación

Activos

Tecnología

7.3 Liderazgo

7.3.1 Liderazgo y compromiso

7.3.2 Política de Seguridad

7.3.3 Roles, responsabilidades y autoridades

7.4 Planificación

7.4.1 Acciones para tratar los riesgos y oportunidades

Evaluación de los riesgos de seguridad de la información

Tratamiento de los riesgos de la seguridad de la información

7.4.2 Objetivos de Seguridad de Información y planificación para alcanzarlos

7.5 Apoyo / Soporte

7.5.1 Recursos

7.5.2 Competencia

7.5.3 Concientización

7.5.4 Comunicación

7.5.5 Documentación de la Información

General

Creación y actualización

Control de la información documentada

7.6 Operación

7.6.1 Planificación y control operacional

7.6.2 Evaluación de los riesgos de seguridad de la información

7.6.3 Tratamiento de los riesgos de seguridad de la información

7.7 Evaluación del desempeño

7.7.1 Monitoreo, medición, análisis y evaluación

7.7.2 Auditorías internas

7.7.3 Revisión por parte de la Dirección

7.8 Mejora

7.8.1 No conformidad y acción correctiva

7.8.2 Mejora continua

8. Versionado

Confeccionado por:

Nombre y rol

Código de documento:

Código

Versión:

v1

Fecha última de actualización:

dd/mm/aaaa

Revisado por:

Nombre y rol

Aprobado por:

Nombre y rol

1. Objetivo

La Dirección de Frogmi, entendiendo la importancia de una adecuada gestión de la información, se ha comprometido con la implementación de un sistema de gestión de seguridad de la información buscando establecer un marco de confianza en el ejercicio de sus servicios con sus clientes y proveedores, todo enmarcado en el cumplimiento de las leyes y en concordancia con la misión y visión de la entidad.

El objetivo de este documento es establecer las políticas, prácticas y lineamientos internos aplicables para el Sistema de Gestión de Seguridad de la Información (de ahora en más SGSI) para Frogmi.

2. Alcance

El siguiente documento alcanza a los procesos y controles definidos para el cumplimiento del Sistema de Gestión de la Seguridad de la Información de toda la organización.

3. Vigencia

Su vigencia será a partir de **24/04/2023**.

4. Responsabilidades

- **CFO:**
  - Aprobar y proporcionar los recursos necesarios para el desarrollo, implementación y cambios de esta política.
  - Garantizar que estas políticas sean conocidas por todos y apoyar a su divulgación, conocimiento y carácter obligatorio.
- **OSI:**
  - Tiene la responsabilidad de supervisar la adecuada ejecución de la presente política.

- Gestionar la capacitación sobre el contenido de la presente política.
- Establecer, documentar y distribuir la presente política.
- Resolver posibles controversias originadas por la política.
- Gestionar los recursos otorgados para la implementación de la política.
- Es el Oficial de Protección de Datos que va a asesorar en leyes de protección de datos y las mejores prácticas.

➔ **Empleados de la organización**:

- Cumplir con los lineamientos de la presente política, apegándose a los procedimientos establecidos. Alertar de inmediato sobre incumplimientos a esta política.

5. Autoridad de emisión, revisión y publicación

Esta Política ha sido desarrollada por Ignacio Abarca, CTO y aprobada por el Comité de Seguridad de la Información.

Se revisará de manera periódica con una frecuencia anual.

6. Términos y definiciones

➔ **Activo de Información:**
Conocimientos o datos que tienen valor para la empresa.

➔ **Seguridad de la Información**:
Preservación de la confidencialidad, integridad y disponibilidad de la información.

➔ **Sistema de Gestión de la Seguridad de la Información (SGSI)**:
Parte del sistema de gestión global, basado en un enfoque hacia los riesgos del negocio, cuyo fin es establecer, implementar, operar, hacer seguimiento, revisar, mantener y mejorar la seguridad de la información.

➔ **Riesgo de Seguridad de la Información:**
Posibilidad que una amenaza explote las vulnerabilidades de un activo o de un grupo de activos y por lo tanto cause daño a la Institución.

- **Integridad**:
  Propiedad de salvaguardar que la información no sufra alteraciones conservando su exactitud.

- **Sistema de Gestión**:
  Marco de políticas, procedimientos, guías y recursos asociados para lograrlos objetivos de la Institución.

- **Políticas**:
  Intenciones globales y orientación tal como se expresan formalmente por la Dirección.

- **Acción Preventiva**:
  Acción tomada para eliminar la causa de una no conformidad potencial u otra situación potencial no deseable.

- **Procedimiento**:
  Forma especificada para llevar a cabo una actividad o un proceso.

- **Registro**:
  Documento que presenta resultados obtenidos o proporciona evidencias de actividades desempeñadas.

- **Nivel de Riesgo:**
  Combinación de probabilidad de un evento y sus consecuencias.

- **Aceptación del Riesgo:**
  Decisión de aceptar un riesgo.

- **Análisis del Riesgo:**
  Uso sistemático de la información para identificar fuentes y estimar el riesgo.

- **Gestión del Riesgo:**
  Actividades coordinadas para dirigir y controlar una organización en relación con el riesgo.

7. Reglas de aplicación al SGSI

7.1 Comprender la organización y su contexto

Frogmi ha determinado los objetivos, asuntos internos y externos que son relevantes para su propósito y que intervienen en el logro de los resultados esperados.

7.1.1 Declaración de Objetivos

La organización declara los siguientes objetivos de seguridad de la información alineados a la estrategia establecida en el Plan de Seguridad de la Información de Frogmi.

- ➔ Proteger la información sensible de nuestros clientes que es almacenada por nuestra solución evitando filtraciones o mal uso de esta.
- ➔ Asegurar a nuestros clientes el acceso y gestión de su información de acuerdo a los niveles de servicios declarados.
- ➔ Evitar pérdidas o inconsistencias de la información de nuestros clientes ante fallas de nuestros proveedores de infraestructura o fallas internas en algún componente de nuestra solución.
- ➔ Identificar, gestionar y minimizar los riesgos a través de herramientas como: Revisión de accesos según matriz de accesos, banca de contraseñas, gestión de incidentes de seguridad, etc.
- ➔ Tener una cultura organizacional consciente respecto a la disponibilidad, confidencialidad e integridad de la información, mediante la concientización y capacitación al personal.

7.1.2 Contexto de SGSI

Con el fin de definir los parámetros externos e internos que deben tenerse en cuenta al gestionar el riesgo, se analiza el contexto interno y externo de la organización.

Análisis externo

El contexto externo incluye cualquier cosa fuera de la organización que pueda influir en la forma en que una organización administra su riesgo de seguridad de la información.

Político Política gubernamental	**Económico** Economía y finanzas	**Socioambiental** Cultura y naturaleza	**Tecnológico** Avances e innovación	**Legal** Leyes y regulaciones
Cambios en la Legislación. Cambios en los tratados comerciales. Acuerdos Internacionales.	Ciclo Económico. Financiación. Impuestos.	Patrones de comportamiento relacionados a la tecnología.. Opinión o percepción de los medios de información.	Nuevas tecnologías para el software. Reemplazo y obsolescencia de las tecnologías. Riesgos asociados a la innovación.	Propiedad intelectual. Regulación de sectores. Leyes de protección. Licencias.

Análisis interno

El contexto interno incluye cualquier cosa dentro de la organización que pueda influir en la forma en que una organización administra su riesgo de seguridad de la información.

Fortalezas	**Debilidades**
Personal de TI experimentado. Personal competente y con experiencia.	Procesos poco consolidados. Poca concientización de empleados en temas de Seguridad de la Información.
Oportunidades	**Amenazas**
Adopción de nuevos estándares relacionados al manejo y transmisión de la información. Rápida adaptabilidad debido a la adopción de tecnologías ágiles y en la nube.	Aumento de ataques a los sistemas de grandes empresas en el rubro de nuestros clientes (retail). Mal uso de la solución por parte de los usuarios finales (compartir contraseñas, subir información confidencial, etc). Cambios en la legislación relacionada a la protección de datos en los países donde operamos. Vulnerabilidades en librerías o software de terceros que usa la solución.

7.1.3 Contexto de Gestión de Riesgos

Los lineamientos acerca de esta gestión son considerados en la Metodología de Gestión de Riesgos donde se encuentran las definiciones pertinentes al tema.

7.2 Comprender las necesidades y expectativas de las partes interesadas

La organización a continuación determina las partes interesadas que son pertinentes para el SGSI y los requisitos de estas partes interesadas que sean pertinentes para la seguridad de la información.

7.2.1 Identificación y Análisis de las Partes Interesadas

Categoría	Interesados detectados
Personal Interno	Gerente General - CEO.
	Miembros del Directorio.
	Comité de Seguridad de Información.
	OSI.
	Jefaturas de los Procesos/Servicios.
	Personal Operativo de los Procesos.
Personas Externas	Clientes.
	Socios comerciales.
	Usuarios finales.
Proveedores	Proveedores de Servicios.

7.2.2 Identificación y Análisis de los Requisitos del Negocio de Partes Interesadas

Identificación de requisitos de CLIENTES

- ➔ Entregar productos y servicios con soporte y mantenimiento:
  - ◆ de acuerdo con los requisitos contractuales,
  - ◆ en caso de interrupciones,
  - ◆ cumpliendo los requisitos legales aplicables,
  - ◆ cumpliendo los requisitos adicionales de la industria aplicables.
- ➔ Protección de datos:
  - ◆ Los productos y servicios protegen adecuadamente los datos de los clientes cumpliendo los requisitos legales y contractuales para los datos sensibles.
- ➔ Cumplir con los requisitos de ISO 27001.

Identificación de requisitos de USUARIOS FINALES

- ➔ Servicios disponibles:
  - ◆ Sistemas de apoyo ante interrupciones.
  - ◆ Mantener servicios de soporte ante interrupciones.
- ➔ Protección de datos:
  - ◆ Los productos y servicios protegen adecuadamente los datos de los usuarios finales cumpliendo los requisitos legales y contractuales para los datos sensibles.

Identificación de requisitos de SOCIOS

Los socios serán empresas que contratan o usan nuestras aplicaciones para dar servicio a usuarios finales o sus clientes:

- ➔ Cumplir con los requisitos de desarrollo de software según los acuerdos firmados.
- ➔ Cumplir con los acuerdos de confidencialidad firmados.
- ➔ Proporcionar información técnica y soporte suficiente que les permita utilizar nuestros servicios de manera segura.

- ➔ Proporcionar la formación necesaria tanto técnica como comercial enfocada a la venta de los productos y servicios.
- ➔ Cumplir los acuerdos contractuales especialmente en los tiempos de entrega acordados.

Identificación de requisitos de PROVEEDORES

- ➔ Cumplir con los acuerdos contractuales.
- ➔ Cumplir con las formas de pago acordadas.
- ➔ Cumplir con los acuerdos de confidencialidad firmados.

Identificación de requisitos de EMPLEADOS

- ➔ Proporcionar un ambiente de trabajo seguro y apropiado.
- ➔ Recibir capacitación y apoyo requeridos.
- ➔ La compañía especifica claramente sus requisitos y expectativas de los trabajadores.
- ➔ Protección de su información personal.
- ➔ La compañía paga justamente por el trabajo.
- ➔ Continuidad del empleo.
- ➔ Oportunidades para el avance y desarrollo profesional.

Identificación de requisitos de ASEGURADORAS

- ➔ Cumplir con los requisitos de la política.
- ➔ Fidelidad en los pagos.
- ➔ Comunicación de cambios en las circunstancias del negocio y del riesgo.

Identificación de requisitos de administración, legales y regulatorios

- ➔ Cumplir con políticas y procedimientos internos de la organización.
- ➔ Cumplir con los requisitos de las leyes de protección de datos.
- ➔ Identificar y cumplir con los requisitos legales propios de cada tipo de negocio emprendido.
- ➔ Información mediante planes de comunicación y procedimientos establecidos para mitigar su impacto.

- Se debe implementar y operar el SGSI y/o sus equivalentes, contar con la aprobación de su documentación y producir los registros requeridos por la norma:
    - ISO/IEC 27001:2013 EDI Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de Seguridad de la Información Requisitos.

7.2.3 Determinar el alcance del sistema de gestión de la seguridad de la información

La información relacionada a los análisis internos y externos (contexto) del SGSI que intervienen y afectan al logro de sus objetivos y que fueron desarrollados en la sección **7.1.2 Contexto de SGSI**. Esta información ha sido usada para definir el alcance respecto a:

- Procesos.
- Características del negocio.
- Organización.
- Ubicación.
- Activos.
- Tecnología.

De manera similar, de la sección **7.2.2. Identificación y Análisis de los Requisitos del Negocio de Partes Interesadas** se tomaron en cuenta los Requisitos de Seguridad de la Información que provienen de los involucrados y afectados por el SGSI para definir el siguiente enunciado de alcance:

El sistema de gestión de Frogmi contempla la infraestructura cloud, los procesos de desarrollo, almacenamiento y eliminación correcta para la protección de información sensible en la entrega de servicios prestados a nuestros clientes. Esta implementación se extiende a las siguientes áreas funcionales: Desarrollo, Operación Comercial e Innovación. Todo esto, de acuerdo con la declaración de aplicabilidad versión 1.1.1, publicada en abril del 2024.

Procesos y servicios

El Sistema de Gestión de Seguridad de la Información aplica a todas las funciones, servicios, actividades y activos de información, de los procesos que forman parte de la Cadena de Valor definido en el Plan Estratégico de Frogmi.

Procesos y/o servicios internos alcanzados	Área	Procesos dependientes/Interferencias
Proceso de Desarrollo	Desarrollo e Innovación	Procesos de Operaciones de TI e Infraestructura Procedimientos de Ventas
Procesos de Operaciones de TI e Infraestructura	Desarrollo e innovación	Proceso de soporte, puesta en marcha y configuración para clientes Proceso de Desarrollo
Proceso de soporte, puesta en marcha y configuración para clientes	Operación comercial y Desarrollo	Procedimientos de Ventas Proceso de Desarrollo
Proceso de capacitación interna.	Operación comercial, Desarrollo e innovación	

Características del negocio

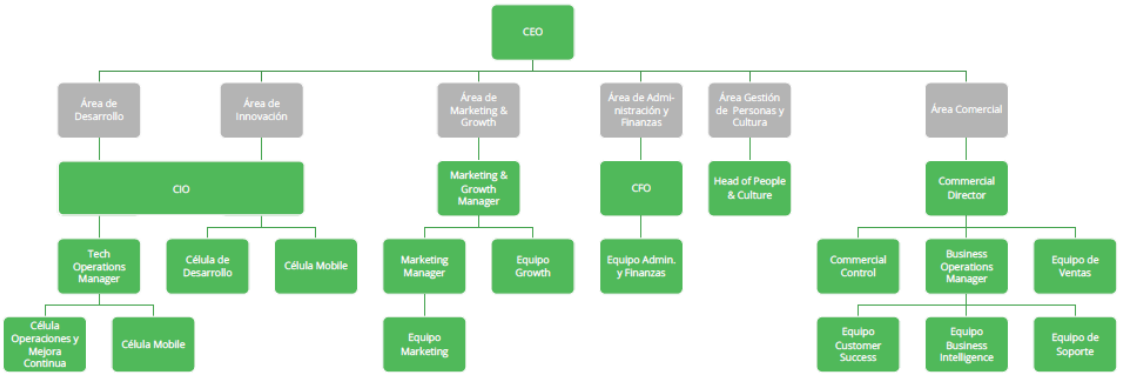
El negocio de Frogmi se encuentra en la industria de retail.

El servicio provisto es el siguiente:

- ➔ Frogmi es una plataforma SaaS que cuenta con interfaz web para definir y priorizar tareas que apoyan la operación en empresas de retail.
- ➔ Frogmi cuenta con aplicaciones móviles para iOS y Android que permiten a los colaboradores de empresas de retail gestionar tareas en terreno.
- ➔ Frogmi cuenta con paneles e información de inteligencia de negocios que ayuda en la gestión y toma de decisiones para la operación de empresas de retail.
- ➔ Frogmi cuenta con una API (Application Programming Interface) que permite que nuestros usuarios puedan integrar sus sistemas con nuestra solución en la medida que lo requieran.

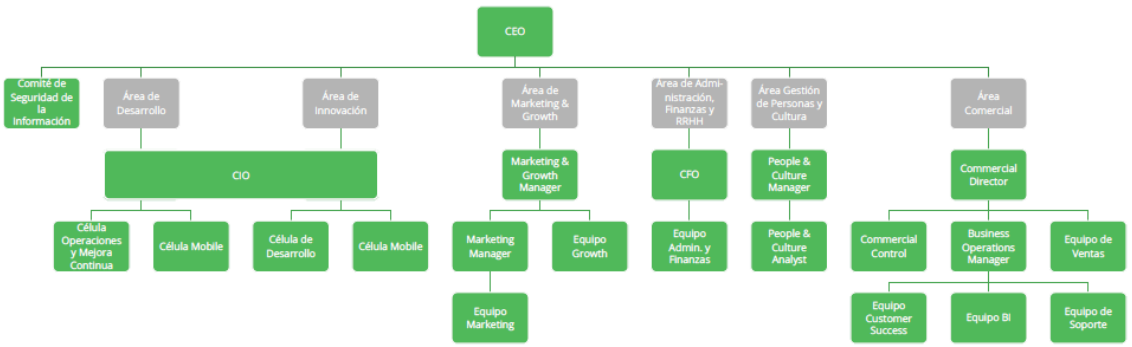
Frogmi cuenta con una estructura que presenta a los distintos órganos y las relaciones que existen entre ellos representado mediante el siguiente organigrama.

Estructura Organizacional por Áreas Funcionales



frogmi

Estructura Organizacional por Áreas Funcionales ISO 27.001



frogmi

Para un detalle más específico de las relaciones funcionales que existen se cuenta con los descriptivos de los roles y responsabilidades de la empresa.

Ubicación

Las instalaciones donde se desarrollan los procesos alcanzado corresponden a la siguiente ubicación geográfica:

➔ Avenida Apoquindo Nº5950, Oficina 20-125 y 20-124, Las Condes, Santiago, Chile

Activos

Los activos de información de Frogmi dentro del alcance y límites del SGSI están sujetos al proceso de Gestión de Riesgos, por lo que estos son inventariados, clasificados y valorizados en base al procedimiento de Gestión de Riesgos vigente y pueden ser encontrados en el Inventario de Activos que se produce a partir de la ejecución del mencionado procedimiento y teniendo en cuenta los lineamientos de la Gestión de Activos y Clasificación de la Información de la Política de Seguridad de la Información.

Tecnología

Los activos se encuentran a su vez soportados por una estructura tecnológica compleja, la cual cuenta con hardware, software, infraestructura y servicios que permiten procesar, almacenar y transmitir la información del proceso. Los componentes tecnológicos más importantes están listados en el Inventario de Activos vigente.

7.3 Liderazgo

7.3.1 Liderazgo y compromiso

La Alta Gerencia y los miembros del Directorio de Frogmi demuestren su liderazgo y compromiso con el Sistema de Gestión de Seguridad de la Información mediante las siguientes acciones:

➔ Reconociendo y suscribiendo la Política de Seguridad de la Información y la Declaración de Objetivos de Seguridad de la Información, revisando y validando que son compatibles con la Dirección estratégica de la organización.

➔ Asegurando que se realice la integración de los requisitos del sistema de gestión de la información dentro de los procesos de la organización mediante la aprobación de los procedimientos y documentos requisito del SGSI.

➔ Garantizando que los recursos necesarios para el sistema de gestión de la seguridad de la información estén disponibles mediante la aprobación de partidas presupuestarias que ha dispuesto consultorías para la implementación del SGSI y sus controles.

- ➔ Comunicando, mediante los canales que considere pertinente, la aceptación de las políticas y procedimientos de seguridad de la información para la adecuación de la empresa a los requisitos del SGSI.
- ➔ Garantizando que el sistema de seguridad de la información logre sus resultados esperados, mediante las revisiones periódicas del sistema.
- ➔ Dirigiendo, indicando las correcciones que deben hacerse y brindando respaldo al personal para la realización de las medidas para mejorar la efectividad del SGSI.
- ➔ Dando recomendaciones de mejora continua para el SGSI.
- ➔ Brindando apoyo mediante el respaldo a las convocatorias y los cambios requeridos para la operación y mejora del SGSI.

7.3.2 Política de Seguridad

La Política de Seguridad de Información de Frogmi cuenta con las siguientes características:

- ➔ Ha sido revisada y aprobada por la Dirección para garantizar su alineamiento al propósito de la organización.
- ➔ Referencia a los Objetivos de Seguridad de la Información.
- ➔ Reconoce la necesidad de atender los requisitos aplicables a la empresa en temas de Seguridad de Información.
- ➔ Reconoce la necesidad de mejorar y corregir continuamente el SGSI mediante la aplicación de acciones de mejora continua y acciones correctivas.
- ➔ Ha sido difundida al personal de la institución mediante charlas de concientización y comunicada por correo electrónico.
- ➔ El **OSI**, una vez al año, o cuando se produzca algún cambio significativo, propondrá al **Comité de Seguridad de Información** la actualización de la Política de Seguridad de la Información.

7.3.3 Roles, responsabilidades y autoridades

La Dirección de Frogmi ha suscrito el documento Roles y Responsabilidades del SGSI que establece:

- ➔ Todos los roles necesarios para llevar a cabo las actividades requeridas por el estándar ISO/IEC 27001:2013.
- ➔ Las responsabilidades que asume cada uno de los actores involucrados en el SGSI, producto de la asunción de los roles establecidos y especificados.
- ➔ La responsabilidad del **OSI** como encargado de informar sobre el desempeño del SGSI a la Dirección y al resto del personal que se encuentre involucrado o interesado.

En ese sentido, el Plan de Comunicación del SGSI deja evidencia de la comunicación de los resultados del desempeño del SGSI a la Dirección.

7.4 Planificación

7.4.1 Acciones para tratar los riesgos y oportunidades

Frogmi planifica la Gestión de Riesgos del SGSI y oportunidades tomando como base el entendimiento obtenido **7.2 Comprender las necesidades y expectativas de las partes interesadas.** Esta gestión está orientada a:

- ➔ Identificar nuevos controles para garantizar el logro de resultados del SGSI, que se evidencia mediante las mediciones de los controles.
- ➔ Anticiparse a los riesgos para evitar o reducir efectos perniciosos, que se evidencia con el análisis, evaluación y tratamiento de riesgos.
- ➔ Constituir una fuente de robustecimiento del SGSI, apoyando a la mejora continua, que se evidencia durante la implementación de los nuevos controles que se han definido en el Plan de Tratamiento de Riesgos.

Para los riesgos y oportunidades identificados, la empresa establece:

- ➔ Las acciones para manejarlas.

- ➔ La forma en que se implementarán en los procesos mediante Plan de Tratamiento de Riesgos.

- ➔ La forma en que serán medidas en cuanto a su efectividad.

Evaluación de los riesgos de seguridad de la información

Frogmi dispone de la realización de una evaluación de riesgos, que considera:

- ➔ Definir los criterios de aceptación y de evaluación de los riesgos.

- ➔ Establecer una metodología objetiva para la evaluación de los riesgos que arroje resultados consistentes.

- ➔ Identificar riesgos de seguridad de la información (asociados a pérdida de confidencialidad, integridad y disponibilidad) y sus causantes, dentro del alcance del SGSI.

- ➔ Analizar los riesgos (consecuencias del impacto, probabilidad, nivel de riesgo).

- ➔ Evaluar los riesgos, comparando los resultados del análisis con los criterios y priorizándolos.

Estas actividades se encuentran documentadas en la Metodología de Gestión de Riesgos y en los registros asociados:

- ➔ Inventario de activos de Información.

- ➔ Análisis de riesgos.

- ➔ Evaluación de riesgos.

Tratamiento de los riesgos de la seguridad de la información

Frogmi establece el tratamiento de los riesgos de seguridad de la Información considerando:

- ➔ Tomar los resultados de la evaluación de riesgos para seleccionar opciones de tratamiento.

- ➔ Determinar los controles para implementar la opción seleccionada.

- ➔ Asociar los controles a los listados en el Anexo A de la norma ISO/IEC 27001:2013 y/o otras normas, legislaciones y/o regulaciones a las que esté sujeta, para verificar que no existan omisiones.

- ➔ Elaborar la Declaración de Aplicabilidad, que especifica los controles requeridos/excluidos y el sustento de su inclusión/exclusión.
- ➔ Proponer el Plan de Tratamiento de Riesgos.
- ➔ Obtener la aprobación de los poseedores de riesgos del Acta de Aceptación del Plan de Tratamiento de Riesgos y los Riesgos Residuales.

Estas actividades se encuentran documentadas en la Metodología de Gestión de Riesgos y en los registros producidos como resultado del proceso:

- ➔ Plan de Tratamiento de Riesgos.
- ➔ Declaración de Aplicabilidad.
- ➔ Acta de Aceptación del Plan de Tratamiento de Riesgos y los Riesgos Residuales.

7.4.2 Objetivos de Seguridad de Información y planificación para alcanzarlos

Frogmi establece sus Objetivos de Seguridad, bajo un enfoque de alto nivel, pero estrechamente relacionado a los objetivos institucionales. Estos objetivos:

- ➔ Son consistentes con la Política de Seguridad de Información y son referenciados desde ella.
- ➔ Están relacionados directamente con las métricas del SGSI, lo cual permite a su vez medirlos.
- ➔ Sus actualizaciones toman en cuenta los resultados de los Análisis de Contexto y Requerimientos de Seguridad de las Partes Interesadas y de los resultados de ejecución de la Metodología de Gestión de Riesgos.
- ➔ Son publicadas y comunicadas conjuntamente con la Política de Seguridad de Información, según lo establece el Plan de Comunicación del SGSI.
- ➔ Son actualizables, si es requerido.
- ➔ Se determina qué se hará, qué recursos se usarán, quién será el responsable y cuándo será completado el Plan de Tratamiento de Acciones Correctivas y de Mejora.
- ➔ Son medidos y obtenidos los resultados de la efectividad de lo desarrollado

7.5 Apoyo / Soporte

7.5.1 Recursos

Frogmi elabora una vez al año el Presupuesto Anual, en el que también se consideran los recursos requeridos para el establecimiento, implementación, mantenimiento y mejora continua del SGSI. Dicho Presupuesto es aprobado por la Alta Gerencia.

Asimismo, se garantiza la participación de los recursos humanos necesarios para el SGSI, mediante decisión del **Comité de Seguridad de Información**.

Se dispone de los recursos de infraestructura tecnológica y física (si corresponde), que han sido establecidas en el apartado **7.2.3 Determinar el alcance del sistema de gestión de la seguridad de la información** de este documento.

7.5.2 Competencia

Frogmi dispone lo siguiente:

- ➔ Ha determinado las competencias necesarias de las personas que operan y asumen funciones específicas dentro del SGSI, las cuales han sido definidas en el documento Roles y Responsabilidades del SGSI.
- ➔ Se ha asegurado el cumplimiento de estas competencias mediante la capacitación y concientización del personal, lo que se ha documentado en el Plan de Capacitación y Concientización en Seguridad.
- ➔ Este plan puede ser actualizado si se detectan deficiencias en el conocimiento del personal, de manera que se programan capacitaciones adicionales. Para identificarlas se cuenta con métricas que evalúan el know how adquirido.

7.5.3 Concientización

Las charlas de concientización realizadas son realizadas, según lo especificado en el Plan de Capacitación y Concientización de Seguridad:

- ➔ Difusión de la Política de Seguridad de Información mediante envío de dicho documento por correo electrónico, como una comunicación formal a todo el personal de la empresa.
    - ◆ Cabe resaltar que la política forma parte de los temas tratados en las charlas de sensibilización y concientización.

- ➔ Importancia de las acciones del personal para la efectividad del SGSI.
- ➔ Beneficios de las mejoras en el desempeño del SGSI.
- ➔ Las implicancias de la empresa acerca de una no conformidad sobre el SGSI.

Cada charla de capacitación y concientización programada cuenta con la Lista de Asistencia de Capacitación.

7.5.4 Comunicación

Las comunicaciones internas y externas del SGSI son planificadas y controladas mediante el Plan de Comunicaciones, documento que es actualizado conforme se avanza con la operación del sistema, éste define:

- ➔ Comunicación,
- ➔ Emisor,
- ➔ Destinatarios,
- ➔ Fecha de emisión,
- ➔ Procesos afectados,
- ➔ Estado.

7.5.5 Documentación de la Información

General

El SGSI cuenta con:

- ➔ Los documentos y registros que son requisito de la norma.
- ➔ Documentos que sin ser requisito de la norma son usados por Frogmi para asegurar la efectividad del SGSI (reglamentación interna, políticas específicas de seguridad de información, documentación de controles de seguridad de información).

Creación y actualización

Frogmi dispone para la creación y actualización de sus documentos del SGSI:

- ➔ La identificación y descripción del documento: título, fecha de elaboración, autor, código.
- ➔ Definición de formatos para los documentos y registros, ya sean en medio electrónico o físico.
- ➔ La especificación de quiénes elaboran, revisan y aprueban los documentos.
- ➔ Los documentos pasan por un proceso de creación/mejora, actualización, aprobación y difusión entrando así en vigencia.

Control de la información documentada

La documentación del SGSI de Frogmi es controlada y garantiza su disponibilidad e idoneidad. Adicionalmente se vela por su adecuada protección.

Esto se logra a través de la aplicación de actividades de control:

- ➔ Distribución restringida, acceso controlado, mecanismos de recuperación y restricciones de uso.
- ➔ Condiciones adecuadas de almacenamiento y conservación.
- ➔ Control de cambios sobre los documentos, retención y disposición.
- ➔ Junto con el documento enviado de acuerdo al plan de comunicación, se podrá consultar por disponibilidad y acceso al OSI o comité de la información.

7.6 Operación

7.6.1 Planificación y control operacional

En el punto **7.4.1 Acciones para tratar los riesgos y oportunidades** de este documento se especifican los procedimientos y actividades que se llevan a cabo para planificar, implementar y controlar el proceso de Gestión de Riesgos.

Para todos los casos indicados anteriormente se cuenta con procedimientos documentados que a su vez generan registros que son evidencia de las actividades realizadas.

7.6.2 Evaluación de los riesgos de seguridad de la información

La frecuencia y condiciones para la realización de las Gestiones de Riesgo son especificadas en la Metodología Gestión de Riesgos del SGSI.

Los resultados de la Evaluación de Riesgos se encuentran documentados y dejan registros que evidencian su realización.

7.6.3 Tratamiento de los riesgos de seguridad de la información

La empresa propone e implementa el Plan de Tratamiento de Riesgos, según lo dispone la Metodología de Gestión de Riesgos del SGSI.

Las actividades del Tratamiento de Riesgos dejan registros que evidencian su realización.

7.7 Evaluación del desempeño

7.7.1 Monitoreo, medición, análisis y evaluación

Frogmi mide y evalúa la efectividad del SGSI, para lo cual determina:

- ➔ Aquello que requiere ser monitoreado y medido: procesos y controles de la seguridad de información.
- ➔ Los métodos aplicados para monitorear, medir, analizar y evaluarlos, para obtener resultados válidos.
- ➔ Cuándo se llevarán a cabo el monitoreo y las mediciones.
- ➔ Quién es el responsable de las mediciones.
- ➔ Cuándo se analizarán y evaluarán los resultados del monitoreo y de las mediciones.
- ➔ Quién es el responsable del análisis y evaluación de los resultados.

Las actividades descritas anteriormente se ejecutan según lo dispone la Metodología de Indicadores de Seguridad de la Información.

7.7.2 Auditorías internas

Frogmi lleva a cabo a intervalos planificados auditorías internas para determinar que el SGSI:

- ➔ Cumpla con los requerimientos de su SGSI y con los lineamientos del estándar ISO/IEC 27001:2013. Contempla, adicionalmente, otras regulaciones y/o normativas que la empresa esté sujeta.
- ➔ Se encuentra implementado y se mantiene de manera efectiva.

Ambos puntos son realizados según se dispone en el Plan de Auditoría Interna De igual forma, la empresa establece que:

- ➔ Planifica, establece, implementa y mantiene un programa o programas de auditoría (frecuencia, métodos, responsabilidades, requisitos de planificación y reporte) tomando en cuenta la importancia de los procesos involucrados y los resultados de auditorías previas.
- ➔ Define los criterios y alcance de la auditoría en el Plan de Auditoría Interna.
- ➔ Selecciona auditores objetivos e imparciales.
- ➔ Comunica los resultados de las auditorías a los jefes involucrados y Alta Gerencia dejando registro de ello en el Plan de Comunicaciones.
- ➔ Se mantienen registros que evidencian la planificación y ejecución de la Auditoría en el:
    - ◆ Programa Anual de Auditoría Interna.
    - ◆ Plan de Auditoría Interna.
    - ◆ Cronograma de Auditoría Interna.
    - ◆ Acta de Reunión de Comité.
    - ◆ Auditoría Interna.
    - ◆ Informe de Auditoría Interna.

Frogmi establece los siguientes lineamientos que deberá cumplir la persona o empresa que realice la auditoría interna:

- ➔ El auditor interno o empresa deberán mostrar que cuentan con experiencia y conocimiento para realizar auditorías de seguridad de la información (Si es factible deberán proporcionar los certificados que lo comprueben)
- ➔ El auditor interno o empresa deberá saber aplicar sus conocimientos sobre auditorías de seguridad de la información en cualquier proceso de la organización para verificar el cumplimiento de su sistema de gestión.
- ➔ El auditor deberá demostrar independencia de las funciones o procesos sobre los que se realizará la auditoría.
- ➔ El auditor interno o la empresa deberá tener un buen conocimiento de los requisitos y procesos involucrados en la auditoría de certificación.

7.7.3 Revisión por parte de la Dirección

La Alta Gerencia y los miembros del Directorio que conforman a Frogmi, realizan una revisión anual del SGSI para garantizar su disponibilidad, adecuación y efectividad. Esta revisión comprende:

- ➔ El estado de las acciones generadas por revisiones de la Dirección previas.
- ➔ Cambios significativos internos y externos, relevantes para el SGSI.
- ➔ El desempeño de la Seguridad de Información en la empresa:
  - ◆ No conformidades y acciones correctivas.
  - ◆ Resultados de métricas e indicadores.
  - ◆ Resultados de auditoría.
- ➔ Grado de cumplimiento de los objetivos del SGSI.
- ➔ Retroalimentación de las partes interesadas.
- ➔ Los resultados de la Gestión de Riesgos del SGSI y el estado del Plan de Tratamiento de Riesgos.
- ➔ Oportunidades de Mejora Continua.

Todos estos elementos son preparados y presentados a la Dirección mediante Informes, y los resultados de la revisión conllevan a la emisión de acciones correctivas y de mejora.

Producto de la revisión, se cuenta con evidencias documentadas de su realización en el Acta de Revisión por la Dirección, donde se indican los resultados y acciones definidas durante la misma.

7.8 Mejora

7.8.1 No conformidad y acción correctiva

Al presentarse una no conformidad, la empresa dispone:

- ➔ Reaccionar frente a la misma, disponiendo la acción para controlarla, corregirla y atender las consecuencias de ésta.
- ➔ Considerar si es necesario y posible eliminar la causa de la no conformidad, mediante: su revisión, determinación de las causas de la no conformidad y verificación de no conformidades similares.
- ➔ Implementar las acciones planeadas.
- ➔ Revisar la efectividad de las acciones realizadas.
- ➔ Realizar cambios sobre el SGSI, si es requerido.

El manejo de estas condiciones para las acciones correctivas se encuentra especificado en el Procedimiento de Acciones Correctivas y de Mejora. Estas acciones son acordes y proporcionales a las no conformidades que las originaron.

Asimismo, se mantiene registro de las correcciones realizadas.

7.8.2 Mejora continua

Para realizar acciones de mejora continua sobre la idoneidad, adecuación y efectividad del SGSI, Frogmi establece los lineamientos de Mejora Continua del SGSI mencionados anteriormente.

8. Versionado

Elaborado por:	Commercial Control Analyst
Código de documento:	SGSI_01_04_POL_SGSI
Versión:	1.2.1
Fecha última de actualización:	24/04/2023, 09/05/2024
Revisado por:	Head of People & Culture
Aprobado por:	Comité de Seguridad de la Información