



Política General de Seguridad de la Información

Tabla de contenido

| | |
|---|---|
| Tabla de contenido | 2 |
| 1. Objetivo | 2 |
| 2. Alcance | 3 |
| 3. Vigencia | 3 |
| 4. Autoridad de emisión, revisión y publicación | 3 |
| 5. Responsabilidades | 3 |
| 6. Objetivos de Seguridad de la Organización | 4 |
| 7. Política General de Seguridad de la Información (Requisito 5.2) | 5 |
| 8. Medición y control de la implementación de las políticas de Seguridad de la Información. | 7 |
| 9. Versionado | 8 |
| 9.1 Control de Versiones | 8 |

1. Objetivo

Mostrar un resumen general de las políticas de Seguridad de la Información aprobadas por **Chattigo**, acorde con los objetivos de seguridad de la organización, que muestre el compromiso de Chattigo para satisfacer los requisitos aplicables, relacionados a la seguridad de la información; así como para la mejora continua del sistema de gestión de la seguridad de la información.

2. Alcance

El Resumen General de las políticas de Seguridad de la Información apoya las directivas y lineamientos descritos en: La Política del SGSI (Sistema de Gestión de Seguridad de la Información) y del PSI (Política de Seguridad de la Información), de la organización.

Es de consideración y debe estar disponible para todas las partes interesadas que interactúan con Chattigo.

3. Vigencia

Su vigencia se corresponderá con la fecha de aprobación por la Alta Dirección de la Compañía.

4. Autoridad de emisión, revisión y publicación

Este Resumen General de las políticas de seguridad de la Información ha sido desarrollado por un grupo multidisciplinario de la compañía, aprobado por el **Comité de Seguridad de la Compañía** (CSI) y por la **Alta Dirección**.

Éste documento y todos los documentos que se encuentran dentro del alcance del Sistema de Gestión de Seguridad de la Información (SGSI) se revisará de manera periódica "**anualmente**" o después de cualquier cambio significativo en el alcance, para asegurar su conveniencia, suficiencia, y eficacia continua.

El presente documento deberá ser publicado y comunicado a toda la compañía y disponible a través del sitio web para todas las partes interesadas que interactúan con Chattigo.

5. Responsabilidades

- El **Comité de Seguridad** es el órgano en la compañía de evaluar y aprobar todas las políticas en relación a la Seguridad de la Información.

- **Analista de Seguridad** vela por la implementación y mantención de las políticas de seguridad de la información. Controlar su cumplimiento.
- **Analista de Procesos** revisa la correspondencia y vigencia del presente Resumen General con el Sistema de Gestión de Seguridad de la Información.
- **Alta Dirección** tiene responsabilidad general de la seguridad de la información de toda la organización.

6. Objetivos de Seguridad de la Organización

Chattigo 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.
- 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 actualizables, si es requerido.
- A través del **Plan de Seguridad**, se determina qué se hará, qué recursos se usarán, quién será el responsable y cuándo será completado el Plan de Acciones de Mejora Correctiva, Preventiva y de Mejora.
- Son medidos y obtenidos los resultados de la efectividad de lo desarrollado.

En este sentido Chattigo se propone mantener un estándar de seguridad de la información necesario y alineado para el logro de las ventas proyectadas, la mantención de grandes clientes y adquisición de nuevos clientes, así como la introducción de la compañía en nuevos mercados. Para ello declara los siguientes objetivos de Seguridad:

- **Objetivo 1:** Establecer controles y desarrollar proyectos, que permitan contar con una infraestructura tecnológica cada vez más segura.
- **Objetivo 2:** Implementar y mantener las políticas esenciales de seguridad de la información (en cumplimiento de los requerimientos comprendidos en la Norma ISO 27001) que Chattigo adopta, para protegerse apropiadamente contra amenazas que podrían afectar en alguna medida la confidencialidad, integridad y disponibilidad de la información relevante de los clientes y de la compañía.
- **Objetivo 3:** Gestionar los recursos en seguridad de la información de tal manera que se realice un uso adecuado de los activos de información.
- **Objetivo 4:** Comprender y tratar los riesgos de seguridad de la información que la compañía defina a partir de sus vulnerabilidades, para que permanezcan en niveles aceptables.

- **Objetivo 5:** Implementar/Mejorar procesos, políticas y procedimientos de Desarrollo Seguro que generen confianza en los clientes sobre el producto o funcionalidad que adquieren.
- **Objetivo 6:** Elevar el nivel de formación y concientización sobre Seguridad de la información en todo el personal de la compañía. Establecer una cultura en Seguridad de la Información.
- **Objetivo 7:** Fortalecer la disponibilidad de información de los componentes de los sistemas de gestión de la compañía, mediante la implementación de medidas y protocolos de contingencia que permitan asegurar dentro de los parámetros consensuados con nuestros mandantes y clientes internos la normal operación del negocio en situaciones extremas.
- **Objetivo 8** Viabilizar la supervisión de las medidas implementadas para proteger la información de la compañía.

7. Política General de Seguridad de la Información (Requisito 5.2)

La Seguridad de la Información en **Chattigo Spa** es parte fundamental del negocio para así entregar confianza a nuestros clientes y usuarios sobre el manejo y protección de su información a través de las tecnologías de la información que operamos. La data, con base en nuestra clasificación de la información, es gestionada con los más altos estándares según las mejores prácticas disponibles en el mercado, lo cual es una base para nuestro crecimiento y sustentabilidad organizacional.

La Seguridad de la Información en Chattigo es posible dado el compromiso de la **Alta Dirección** promoviendo una cultura de mejora continua, facilitando los recursos y herramientas necesarias.

La Alta Dirección entiende y atiende la importancia y beneficios de mantenerse en cumplimiento, no solo con los **requerimientos de la norma ISO 27001** y sus mejores prácticas de seguridad, sino además con otros requisitos legales, contractuales y gubernamentales relevantes para el contexto de la organización.

Para el cumplimiento y mantención de este gran compromiso **Chattigo**:

1. Establece, implementa, mantiene y mejora un SGSI siguiendo los lineamientos descritos en las siguientes Políticas:
 - Política del **SGSI**
 - Política de **Seguridad de la Información**
2. Cuenta con un **Comité de Seguridad de la Información**, cuya composición y forma de trabajo se realiza de acuerdo a los lineamientos de la **Política del Comité de Seguridad**.

3. Reconoce la necesidad de corregir y mejorar continuamente el sistema de gestión mediante la aplicación de acciones de mejora continua y acciones correctivas, en correspondencia al **Procedimiento de Acciones Correctivas y de Mejora**.
4. Implementa políticas en cuanto a la Seguridad de la Información que son del conocimiento general para todos los empleados de la organización. En la medida de lo posible y con base al **Plan de Comunicación del SGSI** definido, nuestras partes interesadas clave son informados de nuestros lineamientos y mejores prácticas.

A continuación, se detallan aquellas políticas que proporcionan principios y guía en aspectos específicos de la seguridad de la información

- Política del **SGSI**
- Políticas de **Seguridad de la Información**, que abarca los lineamientos tendientes a:
 - Gestión de Protección de Datos Personales.
 - Gestión de Activos y Clasificación de la Información
 - Gestión de Riesgos
 - Gestión de Accesos y Perfiles
 - Gestión de Seguridad de Entornos, Plataformas y Aplicaciones
 - Gestión de Vulnerabilidades
 - Gestión de Incidentes de seguridad
 - Gestión del Ciclo de Vida, Puesta en Producción y Entornos
 - Gestión de Capital Humano
 - Gestión y Protección del uso de los dispositivos
 - Gestión de Claves y Criptografía
 - Gestión de Respaldo, Recuperación y Continuidad
 - Gestión de Relaciones con Proveedores
 - Gestión de Cumplimiento
 - Gestión con Instituciones de Injerencia en la SI
 - Gestión de la Seguridad Física y Ambiental

En un nivel inferior, **la política de seguridad de la información** es apoyada por otras normas o procedimientos sobre temas específicos que obligan aún más la aplicación de los controles de seguridad de la información y se estructuran normalmente para tratar las necesidades de determinados grupos dentro de una organización o para cubrir ciertos temas. Para ellos Chattigo tiene implementada además las siguientes políticas:

- Política de Escritorios Limpios
- Política de Tecnología y Operaciones TI
- Política de Desarrollo Seguro
- Política de Backups
- Política de Seguridad por Capas

La implementación de dichas políticas apoyan la **identificación y evaluación de los riesgos de seguridad** a los que está expuesto la compañía, mediante la disposición e implantación de los controles de seguridad en relación a un punto de referencia utilizado para identificar las deficiencias en el diseño e implementación de los sistemas, y el tratamiento de los riesgos mediante la posible identificación de tratamientos adecuados para las vulnerabilidades y amenazas localizadas.

5. Da seguimiento a los **riesgos en seguridad de la información** y se adoptarán medidas relevantes cuando existan cambios que impliquen un nivel de riesgo no aceptable.

Los criterios para la clasificación y la aceptación del riesgo se encuentran referenciados en la política del SGSI.

6. Las situaciones que puedan exponer a la organización a la violación de las leyes y normas legales no serán toleradas.
7. Ejecuta investigación, toma medidas correctivas y elabora informes ante la ocurrencia de **Incidentes de Seguridad**, de acuerdo al Procedimiento establecido para ello. Incluye la ocurrencia de este tipo de eventos a los **Planes de Capacitación y Concientización**.

8. Medición y control de la implementación de las políticas de Seguridad de la Información.

Chattigo a partir de la medición del cumplimiento de los objetivos de seguridad proyectados (mediante indicadores) y a través del seguimiento y mejora de la implementación de las políticas de seguridad referenciadas anteriormente (mediante la revisión sistemática de los controles), garantiza que en la organización:

1. La información estará protegida contra cualquier acceso no autorizado.
2. La confidencialidad de la información, especialmente aquella relacionada con los datos de carácter personal de los empleados y clientes.
3. La integridad de la información se mantendrá en relación a la clasificación de la información (especialmente la de "uso interno").
4. La disponibilidad de la información cumple con los tiempos relevantes para el desarrollo de los procesos críticos de negocio.
5. Se cumplen con los requisitos de las legislaciones y reglamentaciones vigentes, especialmente con la Ley de Protección de Datos.
6. Los planes de continuidad de negocio serán mantenidos, probados y actualizados al menos con carácter anual.

| | | |
|---|--|---|
|  | Resumen General Política de Seguridad de la Información | Código: Chg-ISO27001-051 Versión: 1.0 Pág 8/8 |
|---|--|---|

7. La capacitación en materia de seguridad se cumple y se actualiza suficientemente para todos los empleados.
8. Todos los eventos que tengan relación con la seguridad de la información, reales como supuestos, se comunicarán al responsable de seguridad y serán investigados.

9. Versionado

| | |
|-----------------------------|---|
| Confeccionado por: | Daylyn González Vega (Analista de Procesos) |
| Código de documento: | Chg-ISO27001-051 |
| Versión: | V 1.0 |
| Fecha creación: | 25/04/2023 |
| Revisado por: | David Añasco (Analista de Seguridad) |
| Aprobado por: | Comité de Seguridad de la información |
| Aprobado por: | Alta Dirección |
| Comunicado a: | A toda la compañía |

9.1 Control de Versiones

| Revisiones del Documento | | | |
|--------------------------|------------------|--------------|------------------------|
| Versión | Fecha aprobación | Revisado por | Contenido modificación |
| | | | |