Política General

de Seguridad de la Información

Información Pública

Tabla de contenido

Tabla de contenido 2
1. Objetivo 3
2. Alcance 3
3. Vigencia 3
4. Autoridad de emisión, revisión y publicación 3
5. Responsabilidades 4
6. Objetivos de Seguridad de la Organización 4
7. Política General de Seguridad de la Información (Requisito 5.2) 6
8. Medición y control de la implementación de las políticas de Seguridad de la Información. 9
9. Versionado 11
    9.1 Control de Versiones 11

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 o en el entorno operativo de la organización. Adicionalmente, este proceso de revisión considerará

activamente los resultados de las métricas de eficacia, los informes de las auditorías internas y externas, y el estado de la gestión de riesgos, 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.
- **Jefe de Ciberseguridad/DPO:** 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.
- **Colaboradores:** tienen la responsabilidad de cumplir con los lineamientos de estas políticas y reportar cualquier anomalía o sospecha de incidente de seguridad.

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 la Información y la Política de Seguridad de la Información en la Nube.
- Están relacionados directamente con las métricas del SGSI, lo cual permite a su vez medirlos.

- ➔ Contemplan los requisitos de seguridad y privacidad de la información aplicables y los resultados de la apreciación (resultados de los Análisis de Contexto y Requerimientos de Seguridad de las Partes Interesadas) y tratamiento de los riesgos.
- ➔ Son monitoreados, publicados y comunicados según lo establece el Plan de Comunicación del SGSI.
- ➔ 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 actualizados, cuando sea requerido y están disponibles y documentados.

En este sentido Chattigo se propone mantener un estándar de seguridad y privacidad de la información necesario y alineado a sus objetivos anuales corporativos, para ello declara los siguientes objetivos de Seguridad y Privacidad de la Información :

- ➔ **Objetivo 1 Fortalecer y modernizar la infraestructura y postura de seguridad:** Ejecutar controles, adoptar modelos de automatización y protocolos de contingencia que mejoren continuamente la protección de los activos críticos, garanticen la disponibilidad de la información y aseguren la continuidad del negocio frente a situaciones extremas.
- ➔ **Objetivo 2 Asegurar la renovación y mantenimiento del marco normativo:** Lograr la renovación del certificado ISO/IEC 27001:2022 y mantener la vigencia de ISO/IEC 27017 e ISO/IEC 27018, asegurando el cumplimiento continuo de leyes y regulaciones en materia de ciberseguridad y protección de datos personales.
- ➔ **Objetivo 3 Gestionar de forma segura los recursos y activos de información:** Realizar los controles que promuevan el uso adecuado de los activos, gestionen adecuadamente los cambios tecnológicos y aseguren la confidencialidad de la información sensible y de los datos personales.
- ➔ **Objetivo 4 Identificar, evaluar y tratar los riesgos de seguridad:** Mantener un proceso continuo y documentado de gestión de riesgos, considerando nuevos vectores de amenaza, análisis previos y planes de tratamiento, para mantener los riesgos en niveles aceptables.

- **Objetivo 5 Desarrollar y mantener políticas, procesos y prácticas seguras:** Garantizar la actualización y aplicación efectiva de políticas de seguridad, desarrollo seguro y procedimientos clave, alineados con el SGSI, estableciendo lineamientos específicos para que el uso de nuevas tecnologías opere bajo este marco de control, con el fin de generar confianza en los clientes respecto a la seguridad del producto y las funcionalidades adquiridas.
- **Objetivo 6 Promover una cultura organizacional en seguridad y privacidad de la información:** Continuar impulsando la formación, concientización y comunicación interna sobre seguridad de la información y protección de datos en todo el personal, fomentando el cumplimiento de las políticas y el fortalecimiento de la cultura organizacional. Extender comunicaciones hacia Partners y Clientes orientado a la concientización en seguridad de la información, promoviendo la transparencia y asegurando la alineación de controles en toda la cadena de valor."
- **Objetivo 7 Supervisar y medir continuamente el desempeño del SGSI:** Establecer indicadores y métricas claras que permitan monitorear el cumplimiento de los objetivos de seguridad, evaluar su eficacia y asegurar la mejora continua del SGSI y de la protección de las aplicaciones y datos personales en el entorno de nube.

Se determina dentro de la **Metodología de Indicadores de Seguridad de la Información** qué se hará, qué recursos se usarán, quién será el responsable, cuándo y cómo se evaluarán los objetivos y sus métricas.

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 27001:2022, 27017:2015, 27018:2019** 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
- ➔ Gestión de la Inteligencia de Amenazas de Seguridad

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
- ➔ Política de Gestión de Logs
- ➔ Política de Tratamiento de la Información

Específicamente las políticas relacionadas a la **seguridad de la información en la Nube**, **privacidad y protección de Datos Personales**, tiene implementadas:

- ➔ Política de Seguridad de la Información en la Nube
- ➔ Política de Privacidad y Tratamiento de Datos Personales

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.
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
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
Clasificación de la información:	Información Pública

9.1 Control de Versiones

Revisiones del Documento			
Versión	**Fecha aprobación**	**Revisado por**	**Contenido modificación**
1.1	28/03/2024	Comité de Seguridad	Revisión del documento para actualizar en la página web. Aprobado en comité de seguridad Minuta de Comité de Seguridad - #43 (28_03_2024)
1.2	16/05/2025	Comité de Seguridad	*Actualización 6. Objetivos de Seguridad de la Organización, para alinearlos a los objetivos actualizados en la PGSI. *Inclusión en la relación de políticas de seguridad de

			la información, la Gestión de la inteligencia de amenazas de seguridad, en cumplimiento de este nuevo control de la versión 2022 de la Norma. *Inclusión de la referencia a las políticas relacionadas a la seguridad de la información en la Nube y la privacidad de Datos Personales.
1.3	6/03/2026	Daylyn Gonzalez (Analista de Procesos) Comité de Seguridad	* Actualización acápite 6. Objetivos de Seguridad de la Organización (1,2,5,6), para alinearlos a los objetivos actualizados en la PGSI para la etapa de Renovación. *En el acápite 4. Autoridad de emisión, revisión y publicación: Se complemento el 2do párrafo añadiendo en el proceso de revisión para actualizar la política,,, los resultados de las métricas de eficacia, los informes de las auditorías internas y externas, y el estado de la gestión de riesgos. *En el acápite 5 Responsabilidades, se agrega ***Colaboradores:*** *tienen la responsabilidad de cumplir con los lineamientos de estas políticas y reportar cualquier anomalía o sospecha de incidente de seguridad.*