Política
Seguridad Gtd

Código: SGSI-GTD-PO01
Versión: 04
Fecha vigencia: 19/06/2024

Clasificación: Uso Público

CONTENIDO

1 Identificación del documento

NOMBRE DE LA POLÍTICA	Política de Seguridad Gtd
IDENTIFICACIÓN DE LA POLÍTICA	SGSI-GTD-PO01 SGSI: Sistema de Gestión de Seguridad de la Información GTD: Documento que aplica para todos los territorios PO: Documento Tipo Política 01: Correlativo
REGISTRO(S) ASOCIADOS	No Aplica
PERÍODO DE REVISIÓN	Revisión anual o cuando se requiera según modificaciones de contexto, eventos o consideraciones internas o externas.

SISTEMA DE GESTION	
Establecer a que Sistema de Gestión aplica la Política	
☐ ISO 9001:2015 – Sistema de Gestión de la Calidad SGC	☒ ISO 27001:2013 – Sistema de Gestión de Seguridad de la Información SGSI
☐ ISO 14001:2015 – Sistema de Gestión Ambiental SGA	☒ ISO 20000-1:2018 – Sistema de Gestión de Servicio SGS
☐ ISO 45001:2018 – Sistema de Gestión de Seguridad y Salud en el Trabajo SG-SST	☐ ISO 37001:2016 – Sistema de Gestión de Antisoborno SGAS
☒ ISO 22301:2019 – Sistema de Gestión de Continuidad del Negocio SGCN	☒ Otro(s): PCI-DSS

DOCUMENTO ESPECIFICO Y APLICABLE A		
PAIS	**SEGMENTO**	**OTROS**
☒ Chile (CHL) | ☒ Perú (PER) | ☒ Colombia (COL) | ☐ Ecuador (ECU) | ☐ España (ESP) | ☐ Italia (ITA) | ☐ México (MEX)	☐ Corporaciones (CORP) ☐ Empresas (EMP) ☐ Mayoristas (MAY)	☒ Corporativo (GTD) ☐ Otro(s): ___

2 Control de aprobación de la Política

Versión	Elaborado Por	Fecha	Revisado Por	Fecha	Aprobado por	Fecha
04	Paulo Vega Ingeniero Gestión de Seguridad	18/06/2024	Omar Díaz Jefe de Seguridad de la Información	19/06/2024	Carlos Marihuán Gerente de Riesgo Corporativo | CRO & CISO	18/06/2024
	Gary Apablaza Ingeniero Gestión de Seguridad	18/06/2024				

La única versión valida de esta Política se encuentra disponible en SharePoint del Sistema de Gestión de Gtd.
No es válida cualquier impresión o copia digital de la misma, para evitar que usuarios mantengan versiones obsoletas.

3 Descripción de la Política

3.1 Introducción

Gtd es una compañía TIC con más de 40 años de trayectoria y con presencia en Chile, Perú, Colombia, España, Ecuador y recientemente México. Gtd se compromete a gestionar la seguridad, para ello ha establecido la política general de seguridad, la que es revisada y aprobada por el CISO (*Chief Information Security Officer*) en representación del Comité de Seguridad con miras a cumplir los requerimientos específicos de seguridad, en cada uno de los siguientes ámbitos: seguridad organizacional, seguridad de la infraestructura física, seguridad de la infraestructura tecnológica, ciberseguridad, seguridad de la información, seguridad de los datos y la seguridad de los servicios provistos a clientes.

Para Gtd proteger la confidencialidad, integridad y disponibilidad de la información es un objetivo estratégico y de alto valor. Cumplir los estándares de seguridad que hoy día demanda el mercado, nos permite proteger los activos de la compañía de amenazas, cumplir normas y regulaciones vigentes, resguardar nuestra reputación corporativa y en consecuencia evitar pérdidas económicas e implicancias legales, respondiendo así a la confianza de nuestros clientes.

Nuestra compañía adhiere a los más altos estándares internacionales vigentes, para ello ha incorporado las mejores prácticas de seguridad basados en ISO 27001, NIST, CIS Controls, PCI entre otros.

Esta política debe ser comunicada a toda la organización y a las principales partes interesadas de Gtd.

3.2 Política de Seguridad de la información

El objetivo general es declarar el compromiso de Gtd, y las empresas que lo conforman, con la seguridad y resguardo de los activos, su uso y buenas prácticas relacionadas con la mantención de la integridad, confidencialidad y disponibilidad de dichos activos

Gtd asume los siguientes compromisos de actuación en materia de seguridad y privacidad:

a. La seguridad de las personas es el bien más valioso para Gtd.

b. Los bienes físicos como instalaciones administrativas y técnicas, data centers y la infraestructura física de la red deben ser protegidos contra los riesgos de naturaleza, actos deliberados y aquellas amenazas que pongan en riesgo los activos que soportan y contienen.

c. La información, los sistemas de información y los servicios provistos a clientes a través de las tecnologías y la red, son activos valiosos para Gtd y los países donde opera, los que deben ser protegidos contra amenazas o riesgos internos y externos, para resguardar su disponibilidad, integridad y confidencialidad.

d. La ciberseguridad es una función clave para proteger los activos de Gtd y la infraestructura que brinda soporte a la entrega de servicios de clientes ante los riesgos del ciberespacio.

e. La seguridad de los activos de Gtd incluida la información es responsabilidad de todos los empleados, contratistas y proveedores, independientemente del cargo que desempeñan.

f. Todo empleado, contratista y proveedor debe acceder exclusivamente a la información que le sea estrictamente necesaria para cumplir sus funciones.

g. Todo empleado, contratista y proveedor tiene la obligación de notificar cualquier actividad o situación que afecte o pueda afectar la seguridad de los activos de Gtd.

h. La organización reconoce que la sensibilización, capacitación y entrenamiento adecuados a su personal en las materias de ciberseguridad, son tareas prioritarias y recurrentes.

i. Gtd establece un conjunto de políticas, planes y procedimientos de seguridad en materias específicas, las cuales forman parte integral de la presente política.

j. El Comité de Seguridad es responsable de entregar direccionamiento en los temas de seguridad y tiene la autoridad para su implementación, control y seguimiento para garantizar la mejora continua en materias de seguridad.

k. La organización debe velar por la difusión de las políticas de seguridad a todo Gtd.

l. El incumplimiento de las políticas de seguridad constituye una falta que será sancionada en conformidad a lo establecido en el reglamento interno.

m. La organización se adhiere a las mejores prácticas de seguridad, como marcos de referencia internacionales para la gestión de los riesgos de la seguridad y su mejora continua.

n. La organización declara su decisión de cumplir con la legislación y normativa vigente en temas de seguridad y privacidad de los datos.

3.3 Alcance del documento

En base a las necesidades detectadas y en conjunto con los requerimientos de las partes interesadas se han definido los siguientes ámbitos de trabajo:

• Seguridad organizacional
• Seguridad de la infraestructura física
• Seguridad de la infraestructura tecnológica
• Seguridad de la información y los datos propios y de nuestros clientes
• Ciberseguridad
• Seguridad de los servicios provistos a clientes.

3.4 Ámbitos y Dominios

3.4.1 Gobierno y Organización de la Seguridad

Para la administración de la seguridad, Gtd, debe contar con una estructura de seguridad y un encargado dedicado al logro de los objetivos expresados en esta política. Para ello, se define una estructura organizacional y de gobierno, con dependencia funcional y roles claramente establecidos.

3.4.2 Seguridad Organizacional y de las Personas

Los empleados del Gtd, son parte del capital humano más valioso de la compañía. Una parte significativa de los problemas en la seguridad puede ser causado por empleados descuidados, mal informados, o disgustados, por ello se debe definir e implantar mecanismos para mitigar estos riesgos, y apoyar al personal interno y externo relacionado al Gtd, en la creación de un ambiente de trabajo adecuado.

3.4.3 Gestión de Activos

Todos los activos del Gtd deben ser inventariados y controlados de manera apropiada. Esto se aplica a los recursos físicos y lógicos dentro de los ámbitos definidos. Estos recursos son cruciales para el éxito del negocio y se deben proteger por medio de controles apropiados para reducir al mínimo cualquier riesgo que los pueda afectar.

3.4.4 Control de Acceso

Los activos a cargo del Gtd son esenciales para su óptima operación. Por lo tanto, el acceso a todos los activos debe ser concedido de una manera controlada y periódicamente monitoreada. El protocolo definido en este aspecto contempla autenticación robusta y denegar por defecto el acceso a menos que sea concedido en forma explícita, de acuerdo con las necesidades de conocer de las partes interesadas.

3.4.5 Criptografía

La información confidencial de Gtd y sus clientes, se debe resguardar de accesos no autorizados mediante de la implementación de controles criptográficos aplicables a la transmisión y almacenamiento de datos sensible.

3.4.6 Seguridad Física y Ambiental

Las medidas de seguridad físicas deben estar operativas para resguardar la seguridad y la integridad de las personas, edificios y centros de cómputo o datos. Las medidas de protección deben estar de acuerdo con la clasificación de los activos y a la información procesada, almacenada, y manejada internamente.

3.4.7 Administración de Operaciones

La administración de operaciones de recursos y sistemas de información son esenciales para mantener un alto nivel de servicio a los clientes que operan con el Gtd. Por lo tanto, se deben desarrollar e implementar requerimientos de seguridad para mantener el control sobre las operaciones. Con este objeto se deben definir e implementar las métricas de control adecuadas e incorporar sistemas de monitoreo continuo sobre la operación de seguridad. Lo anterior permite identificar, detectar y prevenir oportunamente los riesgos y amenazas de origen interno o externo que pueden comprometer la seguridad, continuidad y/o la ciberseguridad de los servicios.

3.4.8 Administración de Comunicaciones

La administración de las comunicaciones se debe estructurar de modo tal de asegurar que los datos que se transmiten por las redes de Gtd se encuentren adecuadamente protegidos. Para ello se deben establecer controles técnicos y de gestión que garanticen un nivel de segmentación y resguardo acorde a la criticidad de los datos. La infraestructura de telecomunicaciones asociada a la provisión de servicios TIC debe contar con los equipos, sistemas, personas y tecnologías que permitan mantener un alto nivel de seguridad, de los data centers, nodos e infraestructura de comunicaciones.

3.4.9 Desarrollo, Mantención e Implementación de Sistemas

El diseño de la infraestructura y la implementación de aplicaciones de negocios deben cumplir formal y explícitamente todos los requerimientos de seguridad definidos por Gtd. Estos requerimientos deben ser incorporados en cada paso del ciclo de diseño, desarrollo e implementación de productos, servicios y sistemas.

3.4.10 Relación con Proveedores

Se debe asegurar que el proceso de gestión de proveedores incorpora el cumplimiento de los lineamientos de seguridad, con el objeto de garantizar que los servicios brindados por estos cubren las necesidades de la organización en cuanto a la seguridad y resguardo de activos propios y de nuestros clientes.

3.4.11 Respuestas a incidentes

Se debe asegurar que los eventos e incidentes de seguridad sean notificados de forma adecuada y oportuna a los responsables de los activos y las partes interesadas relevantes, con el propósito evaluar el incidente para mitigar los riesgos asociados y responder adecuadamente a estos incidentes en el futuro. Se deben mantener acuerdos de colaboración con instituciones especializadas para responder ante eventos de ciberseguridad. Lo anterior de acuerdo con los más altos estándares internacionales tales como NIST y el conjunto de normas ISO 27000.

3.4.12 Administración de la Continuidad del Negocio

Se debe disponer de un sistema de administración para asegurar la continuidad de la seguridad y la recuperación rápida ante incidentes o interrupciones inesperadas de los servicios. El plan de continuidad del negocio debe incluir procesos y procedimientos de recuperación ante cualquier interrupción del servicio.

Información adicional y el alcance propio de Continuidad se puede encontrar en la Política de Continuidad del Negocio Gtd

3.4.13 Cumplimiento

Gtd debe cumplir con todas las reglas y regulaciones aplicables por la ley, en lo que respecta a resguardo de información. Esto incluye aspectos penales o civiles, estatutos, reglamentos u obligaciones contractuales hechas a nombre del Gtd. Satisfacer los requerimientos de seguridad incorporado en las leyes, así como la protección de la información propia del Gtd y/o datos de colaboradores, clientes y proveedores.

3.5 Roles y Responsabilidades

El Directorio de Gtd mandata a la administración, encabezada por su Gerente General, establecer los lineamientos/directrices generales y asignar los recursos humanos y técnicos adecuados.

Gtd cuenta con una estructura de gobierno y de gestión de la seguridad en base a tres niveles. Un nivel estratégico, un nivel táctico y un nivel operacional y de gestión. En el nivel estratégico se establecen, coordinan y aprueban los lineamientos generales y la estrategia de seguridad, proveyendo los recursos humanos, tecnológicos y financieros requeridos para alcanzar los objetivos de la presente política.

En el nivel táctico se definen, priorizan y evalúan los proyectos, riesgos e iniciativas de seguridad en cada uno de los ámbitos antes mencionados.

En el nivel operacional y de gestión se implementan, controlan y supervisan los indicadores principales de la seguridad que permiten visualizar oportunamente los riesgos y amenazas en cada uno de los ámbitos de la política, de manera de responder adecuadamente ante incidentes de seguridad.

Todos los empleados y colaboradores de Gtd participan y colaboran activa y responsablemente, cada uno desde su función específica, en la mantención de la seguridad de la compañía.

3.6 Política de Cumplimiento

La adecuada implementación y articulación de esta Política debe ser auditada periódicamente tanto en sus alcances técnicos u organizacionales. Los hallazgos detectados deben ser informados a las áreas respectivas para su pronta solución.

Infracciones al cumplimiento de esta Política serán tratadas de acuerdo con el Reglamento Interno de trabajo y de acuerdo con las definiciones del Manual de Buenas Prácticas Empresariales o Código de Ética.

4 Referencias

La presente política se sustenta considerando la aplicación de las mejores prácticas de seguridad:

- Norma ISO 27001:2022- Sistemas de Gestión Seguridad Información -Requisitos
- ISO/IEC 27002:2022 Code of practice for information security controls
- ISO/IEC 31000:2018 Risk Management
- ISO/IEC 27035:2023 Information security incident management
- ISO/IEC 27701:2022 for privacy information management
- ISO/IEC 27017:2021 Code of practice for information security controls based on ISO/IEC 27002 for cloud services
- ISO/IEC 27018:2019 Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors
- NIST Cybersecurity Framework (CSF) v2.0
- Center for Internet Security CIS Control v8.0
- Payment Card Industry Data Security Standard PCI DSS v4.0
- Legislación de Chile, Perú y Colombia:
    - Ley de protección a los datos de carácter personal
    - Ley de propiedad intelectual.
    - Ley de delitos informáticos
    - Ley marco de ciberseguridad (Prestadores de servicios esenciales y/o operadores de importancia vital)
    - Legislación de Chile: Descrita en Matriz de requisitos legales, reglamentario y Otros (MRL)
- Reglamentos y normativas emanadas por entidades regulatorias locales.
- Reglamento Interno de Orden, Higiene y Seguridad de Gtd.
- Manual de Buenas Prácticas Empresariales o Código de Ética de Gtd.
- Manual de Prevención de Delitos de Gtd.

5 Control de versiones

Historial de versiones:

Versión	Vigente a partir de:	Responsable del Cambio	Detalle de los cambios
01	01/10/2020	Carlos Marihuán Subgerente de Seguridad y Continuidad de Negocios	Versión inicial.
01	05/10/2021	Carlos Marihuán Subgerente de Seguridad y Continuidad de Negocios	Revisión anual efectuada a la política, continúa vigente, no requiere cambios. Validada en Comité Táctico de Seguridad el 5 de octubre 2021.

Versión	Vigente a partir de:	Responsable del Cambio	Detalle de los cambios
02	08/07/2022	Carlos Marihuán Subgerente de Seguridad y Continuidad de Negocios	Se modifica el formato de la Política y se asigna un nuevo código al documento.
03	09/05/2023	Carlos Marihuán Gerente de Riesgo Corporativo | CRO & CISO	Se revisa la política y se cambia el orden el 3.6 Directrices pasa al 3.2 y se 3.5 de Roles y Responsable por Responsabilidades. Se elimina el 3.2 objetivos del documento y el ítem 9 definiciones. Se actualiza cargo de Subgerente de Seguridad y Continuidad de Negocios por Gerente de Riesgo Corporativo | CRO & CISO. Se actualiza y usa la v02 de la plantilla del documento.
04	18/06/2024	Paulo Vega Ingeniero Gestión de Seguridad.	Se revisa idoneidad y adecuación del documento, se incorporan mejoras y cambios regulatorios. Se actualiza el formato a la versión 03 de la plantilla del documento.
	19/06/2024	Omar Díaz Jefe de Seguridad de la Información	Se revisa idoneidad y adecuación del documento, no requiere cambios. Se actualizan las fechas de normas de referencias.

Nota: Se registran la fecha y resultados de las revisiones y cuando estas generan una actualización y cambio a la política se asigna una nueva versión al documento, de lo contrario solo se registra la fecha de revisión y reporta que no se identificó cambio alguno manteniendo la misma versión. El responsable de la Revisión comunica por correo electrónico al gestor documental del área de Sistemas de Gestión el resultado de esta revisión para la gestión de control documental.