Política de Seguridad Gtd

Versión 1.0

1 Introducción

Gtd es una compañía TIC con más de 40 años de trayectoria y con presencia en Chile, Perú, Colombia y España.

Gtd se compromete a gestionar la seguridad, para ello ha establecido una política general de seguridad, la que es revisada y aprobada por la Gerencia General según corresponda 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.

2 Objetivos

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.

Con objeto de materializar el objetivo antes mencionado se establecen los siguientes objetivos específicos.

a) Definir los **requisitos de seguridad** de la organización que permiten asegurar la confidencialidad, integridad y disponibilidad de los activos de información de Gtd.

b) Establecer e implementar **controles de seguridad**, con el objeto de resguardar los activos de Gtd y garantizar que los objetivos y estrategias del negocio se cumplan, en consideración al alcance definido.

c) Identificar y **cumplir leyes y regulaciones** locales aplicables a seguridad, a fin de minimizar los riesgos e impactos económicos y reputacionales.

d) Monitorear y revisar la gestión de seguridad a intervalos planificados, con el objeto de asegurar la **mejora continua**.

e) Mantener **identificado todos los activos** de información relevantes presentes directa o indirectamente en cada proceso y servicio de la organización, en cada uno de los ámbitos definidos.

f) Realizar las actividades necesarias de **gestión de riesgos** para diseñar e implementar medidas y controles que permitan mitigar los riesgos que sean identificados, sin perder de vista el enfoque de la gestión estratégica de seguridad.

g) Mantener una estructura y un marco **de políticas, normas, estándares, certificaciones** y procedimientos en materia de seguridad, para ser implementados en Gtd.

h) **Capacitar a los empleados** acerca de su responsabilidad en el logro de los objetivos de seguridad fijados por Gtd, y de la incorporación progresiva de buenas prácticas relacionadas con ello.

i) Generar conciencia y establecer una **cultura de seguridad** para nuestros empleados y colaboradores, y promover la comprensión de las responsabilidades individuales relacionadas con el alcance definido.

j) Proveer **seguridad a los elementos informáticos y de comunicaciones** donde se almacene, procese y trasmita información de Gtd y/o de sus clientes y **generar capacidades para responder frente a ataques**.

k) Resguardar los recursos tecnológicos, de comunicaciones e información, por medio de la implementación de medidas de **control de acceso**, de modo de garantizar que tales activos son accesibles por personas, medios y fines autorizados.

l) Fortalecer por medio del desarrollo de políticas, directrices, normas y procedimientos de seguridad, que la confidencialidad, integridad y disponibilidad esté de acuerdo con los niveles de criticidad, clasificación, inversión, y las **necesidades de Gtd y sus clientes**.

m) **Proveer los recursos humanos, técnicos, financieros** necesarios para sustentar esta política. Lo anterior, permitirá dar un marco regulatorio que proporcione principios generales para identificar, proteger, detectar, responder y recuperar los activos frente a los riesgos asociados a la seguridad.

3 Alcance

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

4 Definiciones

Ver anexo.

5 Ámbitos y Dominios

- GOBIERNO Y ORGANIZACIÓN DE LA SEGURIDAD

Para la administración de la seguridad, Gtd, debe contar con un encargado de seguridad 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.

- 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.

- 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.

- 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 es prohibir estrictamente el acceso a menos que sea concedido en forma explícita, y de acuerdo con las necesidades de conocer de las diferentes partes interesadas.

- 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 sensibles.

- 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.

- 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.

- 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 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.

- 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.

- 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.

- 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, con el propósito evaluar el incidente para mitigar los riesgos asociados y responder adecuadamente a estos incidentes en el futuro. Lo anterior de acuerdo con los más altos estándares internacionales tales como NIST y el conjunto de normas ISO 27000.

- 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.

- 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.

6 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.

7 Directrices

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 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 de sus 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 seguridad, 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, constituyen una falta y serán **sancionadas** 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**.

8 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.

9 Referencias

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

- ISO/IEC 27001:2013 Information security management systems
- ISO/IEC 27002:2013 Code of practice for information security controls
- ISO/IEC 31000:2018 Risk Management
- ISO/IEC 27035:2016 Information security incident management
- ISO/IEC 27701:2019 for privacy information management

- ISO/IEC 27017:2015 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) v1.1
- Center for Internet Security CIS Control v7.1
- Payment Card Industry Data Security Standard PCI DSS v3.2.1
- Legislación de Chile, Perú y Colombia:
    - Ley de protección a los datos de carácter personal
    - Ley de propiedad intelectual.
    - Ley de delito informático
- 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

La presente Política de Seguridad Corporativa ha sido revisada por el Comité Táctico de Seguridad y aprobada por el Comité de Seguridad (Estratégico) de Gtd, con fecha 01 de octubre de 2020, fecha a partir de la cual inicia su vigencia. Procederá su revisión al menos una vez al año, pudiendo ser modificada en cualquier momento, de acuerdo con las necesidades, por el Comité de Seguridad (Estratégico) y a sugerencia del Comité Táctico.

10 Anexo

A

Aceptación del riesgo: Decisión de asumir un nivel de riesgo concreto
Análisis de riesgos: Proceso para comprender la naturaleza del riesgo y determinar el nivel de riesgo.

C

Ciberseguridad: Enfoque para gestionar los riesgos de seguridad de la información en el ciberespacio para preservar la disponibilidad, integridad, confidencialidad, autenticación y no repudio en este entorno.
Ciberespacio: Espacio virtual conformado por la interacción de personas, software y servicios sobre internet por medio de dispositivos tecnológicos y de redes interconectados.
CSO: director de seguridad, puesto ejecutivo encargado de la gestión de seguridad y protección de todos los activos de la organización.
CISO: director de seguridad de la información, puesto ejecutivo encargado de la gestión y protección de los activos de información.
COBIT: un marco de proceso integral e internacionalmente aceptado para TI que respalda a los ejecutivos, la gerencia de negocios y la gerencia de TI al proporcionar un modelo de gobierno, gestión, control integral de TI.
Controles administrativos: las reglas, procedimientos y prácticas relacionados con la efectividad operativa, la eficiencia y el cumplimiento de las reglamentaciones y políticas de gestión.
Confidencialidad: garantizar que la información es accesible sólo para aquellos autorizados a tener acceso.
Control correctivo: Control que corrige un riesgo, error, omisión o acto deliberado antes de que produzca pérdidas relevantes. Supone que la amenaza ya se ha materializado pero que se corrige.
Control detectivo: Control que detecta la aparición de un riesgo, error, omisión o acto deliberado. Supone que la amenaza ya se ha materializado, pero por sí mismo no la corrige.
Control preventivo: Control que evita que se produzca un riesgo, error, omisión o acto deliberado. Impide que una amenaza llegue siquiera a materializarse.
Control de acceso: Significa garantizar que el acceso a los activos esté autorizado y restringido según los requisitos de negocio y de seguridad.
Conformidad: Cumplimiento de un requisito
Código malicioso: Software destinado a realizar un proceso no autorizado que tendrá un impacto adverso en la confidencialidad, integridad o disponibilidad de un sistema. Un virus, spam o phishing son algunos ejemplos de código malicioso.

D

Derechos de acceso: permisos o privilegios otorgados a usuarios, programas o estaciones de trabajo para crear, cambiar, eliminar o ver datos y archivos dentro de un sistema según lo definido por las reglas establecidas por los propietarios de datos y la política de seguridad de la información.
Disponibilidad: garantizar que la información esté accesible y utilizable cuando lo requiera una entidad autorizada.
Declaración de aplicabilidad: Documento que enumera los controles ISO 27002 aplicados por el SGSI de la organización, tras el resultado de un proceso de evaluación y tratamiento de riesgos.

E

Evento de seguridad de la información: Ocurrencia identificada del estado de un sistema, servicio o red de comunicaciones que indica una posible violación de la política de seguridad de la información o falla de los controles, o una situación previamente desconocida que puede ser relevante para la seguridad.
Estimación de riesgos: Proceso de comparar los resultados del análisis de riesgos con los criterios de riesgo para determinar si el riesgo y/o su magnitud es aceptable o tolerable.
Evaluación de riesgos: Proceso global de identificación, análisis y estimación de riesgos.

G

Gestión de incidentes de seguridad de la información: Procesos para detectar, reportar, evaluar, responder, tratar y aprender de los incidentes de seguridad de la información.
Gestión de riesgos: Actividades coordinadas para dirigir y controlar una organización con respecto al riesgo.
Gobernanza de la seguridad de la información: Sistema mediante el cual las actividades de seguridad de la información de una organización se dirigen y controlan.

I

Identificación de riesgos: Proceso de encontrar, reconocer y describir riesgos.
La identificación de riesgos implica la identificación de las fuentes del riesgo, eventos, sus causas y sus posibles consecuencias. La identificación de riesgos puede involucrar datos históricos, análisis teóricos, opiniones informadas y de expertos, y las necesidades de las partes interesadas.
Impacto: El coste para la empresa de un incidente -de la escala que sea-, que puede o no ser medido en términos estrictamente financieros -p.ej., pérdida de reputación, implicaciones legales, etc.
Incidente de seguridad de la información: Evento único o serie de eventos de seguridad de la información inesperados o no deseados que poseen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información.
Integridad: garantizar la completitud y exactitud de la información.

P

Partes interesadas: Persona u organización que puede afectar a, ser afectada por o percibirse a sí misma como afectada por una decisión o actividad.
Políticas: declaraciones de alto nivel de intención, expectativas y dirección de la alta gerencia.
PDCA: Modelo de proceso basado en un ciclo continuo de las actividades de planificar (establecer el SGSI), realizar (implementar y operar el SGSI), verificar (monitorizar y revisar el SGSI) y actuar (mantener y mejorar el SGSI).

S

Sistema de Gestión de la Seguridad de la Información: Conjunto de elementos interrelacionados o interactuantes (estructura organizativa, políticas, planificación de actividades, responsabilidades, procesos, procedimientos y recursos) que utiliza una organización para establecer una política y unos objetivos de seguridad de la información y alcanzar dichos objetivos, basándose en un enfoque de gestión del riesgo y de mejora continua.

Seguridad Física: consiste en la aplicación de barreras físicas y procedimientos de control ante amenazas que puedan afectar los bienes o activos físicos.
Seguridad Lógica: es una referencia a la protección por el uso de software en una organización, e incluye identificación de usuarios y contraseñas de acceso, autenticación, derechos de acceso y niveles de autoridad. Estas medidas son para asegurar que sólo los usuarios autorizados son capaces de realizar acciones o acceder a información en una red o un equipo concreto.

T

Tratamiento de riesgos: Proceso para modificar el riesgo.

V

Vulnerabilidad: Debilidad en un sistema de información, procedimientos de seguridad del sistema, controles internos o implementación que podría ser explotada o activada por una fuente de amenaza.