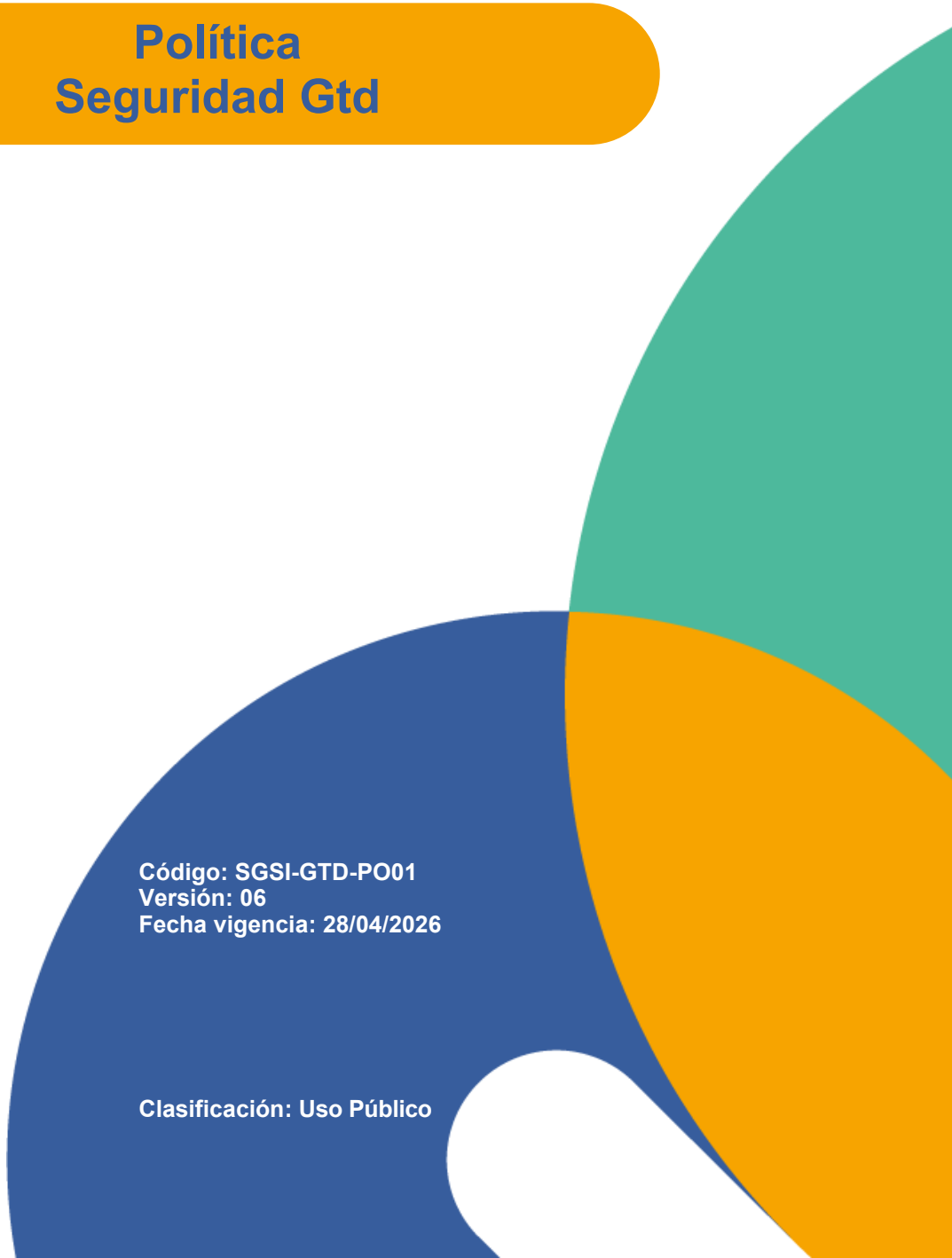
# Política
# Seguridad Gtd



**Código: SGSI-GTD-PO01**
**Versión: 06**
**Fecha vigencia: 28/04/2026**

**Clasificación: Uso Público**

# CONTENIDO

# 1 Identificación del documento

| | |
|---|---|
| **NOMBRE DE LA POLÍTICA** | Política de Seguridad Gtd |
| **IDENTIFICACIÓN DE LA POLÍTICA** | SGSI-GTD-PO01<br>SGSI: Sistema de Gestión de Seguridad de la Información<br>GTD: Documento que aplica para todos los territorios<br>PO: Documento Tipo Política<br>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 27001:2012 – Sistema de Gestión de Seguridad de la Información SGSI |
| ☐ ISO 14001:2015 – Sistema de Gestión Ambiental SGA | ☒ ISO 27701:2025 – Sistema de Gestión de Información de Privacidad SGIP |
| ☐ ISO 45001:2018 – Sistema de Gestión de Seguridad y Salud en el Trabajo SG-SST | ☒ ISO 20000-1:2018 – Sistema de Gestión de Servicio SGS |
| ☒ ISO 22301:2019 – Sistema de Gestión de Continuidad del Negocio SGCN | ☒ ISO 37001:2016 – Sistema de Gestión de Antisoborno SGAS |
| ☐ 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)<br>☐ Empresas (EMP)<br>☐ Mayoristas (MAY)<br>☐ Residencial (RES) | ☒ Corporativo (GTD)<br>☒ Sociedad Gtdata Chile, Perú y Colombia |

# 2 Control de aprobación de la Política

| Versión | Elaborado Por | Fecha | Revisado Por | Fecha | Aprobado por | Fecha |
|---|---|---|---|---|---|---|
| 06 | Paulo Vega Ingeniero Especialista en Seguridad de la Información | 21/04/2026 | Omar Díaz Jefe de Seguridad de la Información | 22/04/2026 | Carlos Marihuán Gerente de Riesgo Corporativo \| CRO & CISO | 28/04/2026 |

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 del sector TIC con más de 46 años de trayectoria, con presencia en Chile, Perú, Colombia, España, Ecuador, México e Italia. En su compromiso con la gestión integral de la Seguridad, Gtd ha establecido una Política General de Seguridad, la cual es revisada y aprobada por el **Chief Information Security Officer (CISO)** en representación del Comité de Seguridad.

Esta Política tiene como propósito dar cumplimiento a los requerimientos específicos en materia de seguridad, en los siguientes ámbitos: seguridad organizacional, infraestructura física, infraestructura tecnológica, ciberseguridad, seguridad de la información, protección de datos y seguridad de los servicios entregados a clientes.

Gtd mantiene un enfoque basado en la gestión oportuna del riesgo, promoviendo la mejora continua de sus prácticas de seguridad y ciberseguridad la cual se alinea con adherir y adoptar estándares internacionales como ISO/IEC 2700:20221, NIST Cybersecurity Framework y PCI DSS para fortalecer su compromiso en proteger la confidencialidad, integridad y disponibilidad de la información como un objetivo estratégico garantizando la protección de sus activos y la confianza de nuestros clientes.

Cumplir con los estándares de seguridad que hoy día demanda el mercado, nos permite satisfacer normas y regulaciones vigentes, resguardar nuestra reputación corporativa y en consecuencia evitar pérdidas económicas e implicancias legales.

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 la integran, con la protección y el resguardo de los activos de información. Este compromiso se extiende al uso adecuado de dichos activos, así como la aplicación de buenas prácticas que garanticen la integridad, confidencialidad y disponibilidad en conformidad con los requisitos de seguridad de la información.

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

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

b. Los bienes físicos tales como instalaciones administrativas, técnicas, centros de datos e infraestructura física de red deben ser protegidos de manera adecuada contra los riesgos de naturaleza, actos deliberados y aquellas amenazas que puedan comprometer la confidencialidad, integridad y disponibilidad de los activos que la albergan y soportan.

c. La información, los sistemas de información y los servicios entregados a clientes a través de las tecnologías e infraestructura de 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 constituye una función esencial para proteger los activos digitales de Gtd y la infraestructura tecnológica que sustenta la entrega de los servicios a los clientes frente a los riesgos y amenazas provenientes del ciberespacio.

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

f. Todo empleado, contratista y proveedor debe acceder únicamente a la información, sistemas y recursos que sean estrictamente necesaria para el desempeño de sus funciones conforme al principio de necesidad de conocer.

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

h. La organización reconoce que la sensibilización, capacitación y formación continua de su personal en las materias de Seguridad y Ciberseguridad son actividades prioritarias, esenciales y permanentes para la gestión eficaz del riesgo y la protección de los activos de información.

i. La organización establece un conjunto de políticas, planes y procedimientos específicos en materias de Seguridad de la Información y Ciberseguridad los cuales constituyen componentes complementarios e integrados de la presente política. Este Marco Normativo proporciona lineamientos de gobierno y operativos para garantizar el cumplimiento de los objetivos de seguridad, la gestión de riesgos y la protección de los activos de información.

j. El Comité de Seguridad es responsable de entregar direccionamiento estratégico en los objetivos de Seguridad y Ciberseguridad teniendo la autoridad para su implementación, control y seguimiento garantizando la mejora continua en esta materia.

k. La organización debe asegurar y velar que las políticas de seguridad de la información sean difundidas de manera efectiva a todas las partes interesadas. Los colaboradores tienen el deber de conocer, comprender y aplicar la presente Políticas de Seguridad.

l. El incumplimiento de las Políticas de Seguridad de la Información y su Marco Normativo será considerado una infracción a las normas Corporativas y que podrá ser sancionada conforme a lo establecido en el reglamento interno de trabajo de Gtd, así como a la normativa legal vigente.

m. La organización se compromete a adherir, adoptar y mantener las mejores prácticas de Seguridad de la Información y Ciberseguridad mediante la implementación de marcos de referencia internacionalmente reconocidos para la Gestión de Riesgos, el cumplimiento normativo y la mejora continua.

n. La organización declara su decisión de cumplir con la legislación, reglamentación y normativa vigente en materias de Seguridad de la Información, Ciberseguridad y Protección de 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 gestión efectiva de la seguridad de la información, Gtd debe establecer y mantener una estructura organizacional de seguridad con roles, responsabilidades y autoridades claramente definidos. Esta estructura incluye la designación de equipos responsables de seguridad y ciberseguridad, quienes lideran las acciones para alcanzar los objetivos establecidos en esta política y garantizar la operatividad del Sistema de Gestión de Seguridad de la Información *(SGSI)*.

### 3.4.2 Seguridad Organizacional y de las Personas

Los colaboradores de Gtd, constituyen el capital humano más valioso de la compañía. Reconociendo que una parte importante de los incidentes de seguridad puede originarse por acciones involuntarias, desconocimiento o descontento de empleados, por ello se deben definir y establecer mecanismos para mitigar estos riesgos. Esto incluye concientización, formación continua, control de acceso y la definición clara de roles, responsabilidades, además del fomento de un ambiente de trabajo seguro y colaborativo para el personal interno y externo.

### 3.4.3 Gestión de Activos

Los activos de información de Gtd, tanto físicos cómo lógicos deben ser identificados e inventariados y gestionados adecuadamente en los términos establecidos por la organización. La gestión del ciclo de vida debe incluir la asignación de responsabilidades, revisión periódica y eliminación segura reduciendo los riesgos asociados. Estos activos son fundamentales para el logro de los objetivos del negocio y la entrega de los servicios de clientes por lo que deben ser clasificados según su criticidad y protegidos mediante controles apropiados que aseguren la protección de su integridad, confidencialidad e integridad.

### 3.4.4 Control de Acceso

Los activos gestionados por Gtd son críticos para la operación segura y eficiente de la organización. En consecuencia, el acceso a estos activos debe estar estrictamente controlado, autorizado previamente y sujeto a seguimiento o monitoreo. El acceso debe ser otorgado únicamente bajo el principio de necesidad de conocer y en función de la responsabilidad especifica de cada parte interesada, por defecto el acceso debe ser negado hasta que se justifique y apruebe su necesidad de conocer. Asimismo, deben aplicarse mecanismos de autenticación robusta y gestionar los privilegios de acceso de manera que se limite el uso de activos al mínimo necesario reduciendo los riesgos de accesos no autorizados o indebidos.

### 3.4.5 Criptografía y Enmascaramiento

La información de Gtd y sus clientes, se debe resguardar de accesos no autorizados evaluando la sensibilidad de la información para la utilización de técnicas de criptografía o enmascaramiento aplicables a la transmisión, almacenamiento y limitación de información de datos sensible.

### 3.4.6 Seguridad Física y Ambiental

Las medidas de seguridad físicas deben implementarse y mantenerse operativas para proteger la integridad de las personas, las instalaciones, la infraestructura de red, TI y los centros de procesamiento de datos. Estas medidas deben ser proporcionales y estar de acuerdo al nivel de sensibilidad de los activos físicos y de la información que estos contienen alineado con su clasificación. La protección debe incluir las salvaguardas necesarias frente a las amenazas internas y externas que garanticen un entorno seguro para la operación continua del negocio.

### 3.4.7 Administración de Operaciones

La administración eficaz de operaciones y recursos tecnológicos de los sistemas de información son esenciales con el fin de mantener la calidad y continuidad de los servicios de los clientes que operan con Gtd. Para mantener el control y la seguridad en las operaciones se deben establecer e implementar requisitos de seguridad específicos así cómo métricas de control adecuadas que permitan evaluar el desempeño de los procesos críticos. Asimismo, se deben incorporar sistemas de monitoreo continuo sobre la operación de los sistemas de información e infraestructura tecnológica con el fin de identificar, proteger, detectar, responder y recuperarse oportunamente frente a los riesgos y amenazas ya sea de origen interno o externo que pueden comprometer la seguridad, la continuidad operacional o la ciberseguridad asegurando la entrega y la calidad de los servicios a los clientes de Gtd.

### 3.4.8 Administración de Comunicaciones

La administración de las comunicaciones se debe estructurar de modo tal de garantizar que los datos transmitidos a través de las redes de Gtd y terceros estén adecuadamente protegidos frente a accesos no autorizados, alteración o perdida. Para ello se deben implementar y establecer controles técnicos y de gestión que aseguren una segmentación efectiva de la red y un nivel de protección proporcional a la criticidad de la información procesada.
La infraestructura de telecomunicaciones utilizada para a la entrega de servicios TIC debe estar respaldada por equipos, sistemas, procesos, personal capacitado y tecnologías que permitan mantener un alto nivel de seguridad, de los centros de datos, nodos e infraestructura de red asegurando la integridad, confidencialidad y la disponibilidad de las comunicaciones.

### 3.4.9 Desarrollo, Mantención e Implementación de Sistemas

El diseño de la infraestructura tecnológica y la implementación de aplicaciones de negocios deben cumplir, de manera formal y documentada con todos los requerimientos de seguridad establecidos por Gtd. Estos requerimientos deben ser integrados desde las etapas iniciales del ciclo de vida incluyendo análisis, desarrollo, pruebas, implementación y mantenimiento asegurando que los productos, servicios y sistemas se construyan bajo los principios de seguridad en su defecto. La incorporación temprana de controles de seguridad permite mitigar oportunamente riesgos, reducir vulnerabilidades y garantizar que los sistemas implementados cumplan con los niveles de seguridad exigidos por la organización y las normativas vigentes.

### 3.4.10 Relación con Proveedores

Se debe asegurar que el proceso de gestión de proveedores incluya de manera explícita los requisitos de seguridad de la información y/o ciberseguridad , con el objetivo de garantizar que los servicios entregados por terceros cumplen con los lineamientos de seguridad definidos por Gtd. Estos deben incluir el resguardo de los activos propios y de clientes, así como el cumplimiento de las políticas internas, los estándares de seguridad aplicables y los compromisos contractuales y normativos. En los acuerdos con proveedores deben establecerse proporcionalmente al nivel de riesgo considerando mecanismos de evaluación, monitoreo y revisión de desempeño en seguridad.

### 3.4.11 Respuestas a incidentes

Se debe garantizar que todos los eventos e incidentes de ciberseguridad sean notificados de manera oportuna y precisa en los canales definidos por Gtd y de partes interesadas relevantes. El objetivo es permitir una pronta evaluación, efectiva de los incidente, mitigar los riesgos asociados y fortalecer la capacidad de respuesta ante futuros incidentes. La organización debe mantener acuerdos de colaboración con entidades especializadas para responder ante eventos de ciberseguridad. Lo anterior de acuerdo con los más altos estándares internacionales tales como NIST, PCI DSS y el conjunto de normas ISO 27000 asegurando un enfoque estructurado, coordinado y de mejora continua.

En conformidad a lo establecido en la ley marco de ciberseguridad de Chile, los ciberincidentes que afecten las redes y sistemas que soportan los servicios esenciales estipulados en la ley, deben ser reportados al CSIRT de la Agencia Nacional de Ciberseguridad, dentro de los plazos legales establecidos. Del mismo modo se debe dar cumplimiento a las obligaciones establecidas por ley para los operadores de importancia vital (OIV) de ser requerido.

### 3.4.12 Administración de la Continuidad del Negocio

La compañía debe contar con un sistema formal de gestión para asegurar la continuidad de la seguridad de la información y la recuperación oportuna frente incidentes, desastres o interrupciones inesperadas de los servicios. El plan de continuidad del negocio y el plan de recuperación debe incluir a las personas, los procesos, procedimientos documentados, roles definidos y mecanismos de prueba definidos que permitan garantizar la redundancia de las operaciones y los procesos críticos del negocio dentro de los tiempos establecidos con el fin de minimizar el impacto sobre los activos de información y la entrega de los servicios de los clientes de Gtd.

*Información adicional 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, táctico y operativo de gestión.

En el nivel estratégico se establecen los objetivos estratégicos, se coordina y aprueban los lineamientos generales de Seguridad. Proveyendo los recursos humanos, tecnológicos y financieros requeridos para cumplir con 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 ejecutan e implementan los controles definidos, se monitorean y supervisan los indicadores principales de la seguridad que permiten identificar oportunamente los riesgos y amenazas en cada uno de los ámbitos establecidos de esta Política con el propósito de responder oportuna y adecuadamente ante eventos e incidentes de seguridad.

Todos los empleados de Gtd deben participan, colaborar activa y responsablemente desde su rol y 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 27701:2025 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 v4.1*
- *Legislación de Chile, Perú y Colombia:*
    - *Ley de protección a los datos de carácter personal*
    - *Ley de propiedad intelectual.*
    - *Ley de delitos informáticos*
    - *Ley 21 663 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. |

| Versión | Vigente a partir de: | Responsable del Cambio | Detalle de los cambios |
|---|---|---|---|
| 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. |
| 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.<br>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.<br>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. |
| 05 | 10/06/2025 | Paulo Vega Ingeniero Gestión de Seguridad. | Se realizaron ajustes integrales en la redacción de la política fortaleciendo la alineación con los estándares de seguridad, ordenado la redacción, incorporado el ciclo de vida de activos, resaltando los principios clave de seguridad y estableciendo roles y responsabilidades con mayor precisión vinculando en todo el contenido del documento a la ciberseguridad, la gestión de riesgos y la entrega de servicios. |
| 06 | 28/04/2026 | Paulo Vega Especialista en Seguridad de la Información | Se incorpora en la tabla de sistemas de gestión el estándar **ISO/IEC 27701:2025 – Sistema de Gestión de Información de Privacidad (SGIP)**. Asimismo, se actualiza la tabla de aplicabilidad, incorporando las sociedades **GTDATA Perú, Colombia y Chile** y se incorpora el segmento Residencial **(RES).** |

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.