China Three Gorges Latam

POLÍTICA DE PROTECCIÓN DE DATOS

CTGL-LC-PO-006

Approved: ECM 39th 20241025

Version 1
10-25-2024

Contents

Capítulo 1 Disposiciones generales

1. Introducción

El presente documento contiene la Política de Seguridad de la Información (la "Política") aplicable para: i) CTG Colombia Holding S.A.S; ii), Talasa Conexión S.A.S E.S.P; y iii) Talasa ProjectCo S.A.S. E.S.P (en adelante las "Empresas", o las "Compañías"), en la cual se desarrollan las directrices y principios aplicables a las operaciones de las Compañías en el manejo de información personal y no personal. Este documento tiene por objeto definir las organizaciones, las responsabilidades generales, las obligaciones de los empleados y terceros, con el fin de mitigar los riesgos que se generen en relación con la administración de información de las Compañías.

Las Compañías son conscientes de las amenazas que enfrenta la información hoy en día, así como de las consecuencias derivadas de no implementar medidas de seguridad de la información apropiadas. Teniendo en cuenta lo anterior, la presente Política, tiene como finalidad desarrollar el Sistema de Gestión de Seguridad de la Información – SGSI de las Compañías y cumplir con los estándares establecidos por la normativa aplicable.

2. Alcance

La presente Política es de aplicación obligatoria, para todos los empleados de las Compañías y los terceros (proveedores y contratistas) que presten sus servicios o tengan algún tipo de relación con las Compañías (en adelante, el "Personal"). La Política estará vigente a partir de su publicación.

Capítulo 2 Principios

La presente Política desarrolla sus objetivos mediante el cumplimiento de los siguientes principios, que también serán aplicables a los demás documentos y procedimientos implementados al interior de las Compañías, y los cuales se complementan con los principios generales del tratamiento de datos personales establecidos en la normatividad aplicable y en la Política de Procesamiento de Datos de las Compañías:

1. Principio de confidencialidad

Se refiere al conjunto de procedimientos y medidas tecnológicas y humanas implementados por parte de las Compañías para mantener la información segura y evitar su acceso, modificación, consulta o supresión de forma no autorizada. En la práctica, se trata de la implementación de controles para regular y evitar el acceso a los datos por parte de personal o terceros no autorizados.

2. Principio de integridad

Consiste en garantizar que la información que es utilizada por las Compañías no ha sido manipulada o alterada por un individuo que no está autorizado para tal efecto y, por lo tanto, sean confiables. Para ese efecto, se deberán implementar los sistemas necesarios para asegurar que la información almacenada en los sistemas de la compañía cumple con este principio y no se guardarán copias no autorizadas de la información.

3. Principio de accesibilidad o disponibilidad

Se refiere a que los sistemas, aplicaciones y datos estarán disponibles cuando los miembros del Personal de las Compañías o terceros autorizados los requieran. Para ello, se contará con sistemas que aseguren la preservación de los sistemas y el acceso oportuno a la información.

4. Principio de calidad de la a información

Se refiere a que la información sujeta a ser usada por parte de las Compañías debe ser veraz, completa, exacta, actualizada, comprobable y comprensible. Se prohíbe el uso de información o datos que sean parciales, incompletos, fraccionados o que induzcan a error.

5. Principio de Seguridad

Consiste en que la información de las Compañías se deberá manejar con las medidas técnicas, humanas y administrativas que sean necesarias para otorgar seguridad a los registros y de esa forma mitigar los riesgos asociados a su uso.

6. Principio de Minimización de la información

Se refiere a que, para efectos de eficiencia en el manejo de la información requerida, se disminuirá, en la medida que resulte pertinente y sin afectar las operaciones y procesos de las Compañías, la cantidad de datos recogidos y se limitará su uso en factores como, la autorización dada por los titulares, las finalidades informadas a estos, el tiempo de retención de los datos, la cantidad de personas con acceso a la información y las operaciones para las cuales se utilizarán los datos.

Capítulo 3 Marco normativo

- Constitución Política de Colombia: Artículo 15.
- Ley 527 de 1999: Por la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales y se establecen las entidades de certificación y se dictan otras disposiciones.
- Ley 1266 de 2008: Por la cual se dictan las disposiciones generales del Hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones.
- Ley 1581 de 2012: Por la cual se dictan disposiciones generales para la protección de datos personales.
- Decreto 1377 de 2013: Por el cual se reglamenta parcialmente la Ley 1581 de 2012.
- Título V de la Circular Única de la Superintendencia de Industria y Comercio
- Decreto 886 de 2014: Por el cual se reglamenta el Registro Nacional de Bases de Datos.
- Decreto 1074 de 2015: Por medio del cual se expide el Decreto Reglamentario del Sector Comercio, Industria y Turismo. Reglamenta parcialmente la Ley 1581 de 2012 e imparte instrucciones sobre el Registro Nacional de Bases de Datos. Artículos 25 y 26.
- Decreto 1078 de 2015: Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones.
- CONPES 3701 de 2011. Lineamientos de Política para Ciberseguridad y Ciberdefensa.
- CONPES 3854 de 2016. Política Nacional de Seguridad digital.

- Norma Técnica Colombiana NTC-ISO/IEC 27001

Capítulo 4 Seguridad de la información

1. Lineamientos Generales de Seguridad y Confidencialidad de la Información

Las Compañías han establecido los siguientes lineamientos principales o pilares para mantener la seguridad y confidencialidad de su información:

- Identificar, de manera oportuna, potenciales riesgos a los sistemas de seguridad de la información de las Compañías.
- Buscar el desarrollo continuo del Sistema de Gestión de Seguridad de la Información, de las Compañías, innovando en los controles físicos y tecnológicos.
- Concientizar al Personal en el cuidado y mantenimiento de la seguridad de la información.
- Socializar con todo el Personal la presente Política, así como las reglas, procedimientos y documentos complementarios en materia de seguridad de la información.

2. Medidas específicas de seguridad y privacidad de la información adoptadas por las Compañías

- **Clasificación de la Información de las Compañías**: Las Compañías han definido los siguientes parámetros para clasificar su información:
- **Información Pública:** es aquella información que ha sido declarada de conocimiento público y que se encuentra disponible en fuentes de acceso público sin ningún tipo de restricción. Esta información puede ser entregada a terceros, funcionarios o cualquier persona sin ocasionar daños a terceros ni a los procesos de negocio.
- **Información de Uso Interno:** es aquella información que es utilizada por las Compañías para realizar las labores asignadas y que no puede ser compartida con terceros sin autorización del propietario del activo.
- **Información Confidencial:** información que es utilizada solo por unos miembros específicos del Personal de las Compañías para realizar sus labores y que no puede ser accedida o conocida por otras áreas o empleados de las Compañías. La información personal de cualquier titular, respecto de la cual las Compañías actúen en calidad de responsables del tratamiento, se considerará Información Confidencial.

Capítulo 5 Gestión de los activos de la compañía

Las Compañías administrarán y resguardarán los activos de información que contienen bases de datos con información personal, considerados como activos clave, de acuerdo con las tablas de retención documental. A estos activos se le ha asignado un responsable, encargado de su gestión conforme a las necesidades de la empresa, para garantizar la confidencialidad y seguridad de la información.

Además, se han establecido controles para asegurar que estos activos sean utilizados de acuerdo con esta Política, y en caso de un cambio de responsable, se realizará la entrega formal al área correspondiente, quien verificará el estado de la información.

Capítulo 6 Organización interna

Procedimientos y reglas en materia de seguridad de la información adoptados por las Compañías en relación con su organización interna:

- Las Compañías cuentan con un área de Tecnología de la Información
- Las Compañías, por medio de sus áreas internas, mantendrán contacto permanente con el Personal involucrado en asuntos de seguridad y privacidad de la información, con el fin de desarrollar y actualizar el Sistema de Gestión de la Información de las Compañías.
- Los activos de información de las Compañías sólo podrán ser administrados por la persona o área a cargo de estos, de conformidad con los lineamientos establecidos, reduciendo así potenciales riesgos o modificaciones intencionales o accidentales de la información contenida en los mismos.
- Las Compañías realizaran capacitaciones sobre seguridad de la información para todos los empleados.

Capítulo 7 Seguridad de los datos personales

Las Compañías se preocupan por el adecuado manejo de la información y datos asociados a las personas naturales relacionadas con su operación, incluyendo sus empleados, inversionistas, proveedores y otros terceros relacionados con las Compañías. Para ese efecto, han establecido una Política de Tratamiento de la Información o Política de procesamiento de datos en concordancia con los mandatos legales de la Ley 1581 de 2012 y las normas complementarias. Estos documentos son aplicables a todas las operaciones de tratamiento a las que se sometan los datos contenidos en las bases de datos bajo control de las Compañías.

Adicionalmente, las Compañías seguirán los siguientes parámetros en relación con el tratamiento de Datos Personales, con el fin de garantizar la confidencialidad y seguridad de sus bases de datos físicas o automatizadas:

- Dar estricto cumplimiento a la ley 1581 de 2012, su decreto reglamentario 1377 de 2013 y demás normativa de protección de Datos Personales en Colombia.
- Solicitar el consentimiento previo, expreso, e informado de los titulares para el tratamiento de datos.
- Garantizar el ejercicio de los derechos de los titulares de los datos, responder a sus consultas y reclamos de manera oportuna y efectiva, entregando la información pormenorizada del tratamiento realizado.
- Notificar a las autoridades aplicables, dentro del plazo previsto en la regulación vigente, cuando se esté ante un posible incidente de seguridad de datos personales.
- Capacitar a todos los miembros del Personal en relación con el adecuado tratamiento de los datos personales en cumplimiento de la normativa aplicable.

Las Compañías han implementado controles específicos de seguridad para proteger los Datos Personales, tales como controles de acceso mediante usuario y contraseña a las aplicaciones en donde se encuentran las bases de datos o activos de información (Data Room y/o SharePoint), lo que hace que los usuarios que no se encuentren autorizados para ingresar a una aplicación, no lo puedan realizar.

Capítulo 8 Recursos humanos

Las Compañías han definido los siguientes controles dirigidos específicamente a sus miembros de recursos humanos, en relación con la seguridad de la información:

1. **Vinculación de personal**

- Las Compañías han definido una lista de verificación de antecedentes del Personal a contratar.
- Los miembros del Personal deben firmar acuerdos de confidencialidad y no divulgación de la información reservada de las Compañías, y, hacerlos vinculantes.
- Todos los nuevos miembros del Personal son capacitados y se les permite conocer de manera permanente la presente Política.

2. **Desvinculación de personal**

- Cualquier novedad de desvinculación debe ser notificada de inmediato al departamento administrativo, con el fin de que este último proceda con la inactivación de todos los equipos, sistemas, accesos y/o permisos asignados al colaborador.
- Se creará una copia de respaldo del buzón de correo electrónico una vez se dé por terminada la vinculación con las Compañías.
- Se deben inactivar todos los accesos a los sistemas de información.
- Se debe solicitar la devolución cualquier distintivo de autenticación, que lo acredita como miembro del Personal de las Compañías.

Capítulo 9 Gestión de medios

Aunque las Compañías cuenten con herramientas que le permiten realizar un escaneo para todos los medios removibles que se conecten a un equipo de las Compañías, en la actualidad la responsabilidad de este escaneo está en cabeza de cada miembro del Personal de las Compañías, el cual debe adoptar medidas suficientes para la protección de la información de las Compañías contenida en medios removibles. En caso de que configure un acceso no autorizado o fraudulento a los mismos, y/o se extravíe, los miembros del Personal deben notificar de inmediato al departamento administrativo de las Compañías.

Capítulo 10 Gestión de incidentes de seguridad

Las Compañías han implementado gestión de los incidentes de seguridad de la información que puedan presentarse. Para ello cuenta con los siguientes parámetros:

- Definición de incidente de seguridad: Un incidente de seguridad de la información se define como un acceso, intento de acceso, uso, divulgación, modificación o destrucción no autorizada de información (personal o no); un impedimento en la operación normal de las redes, sistemas o recursos informáticos; o una violación a una medida de seguridad implementada por las Compañías.
- Notificación del incidente: La notificación de los incidentes permite responder a los mismos en forma sistemática, minimizar su ocurrencia, facilitar una recuperación rápida y eficiente de las actividades minimizando la pérdida de información y la interrupción de los servicios,

además de manejar correctamente los aspectos legales que pudieran surgir durante este proceso.

- Proceso de notificación: Un usuario, tercero o contratista que sospeche sobre la materialización de un incidente de seguridad deberá notificarlo al primer punto de contacto definido por las Compañías, que en este caso es la dirección administrativa, a través de cualquier canal de comunicación (Correo electrónico).
  En el primer punto se analizará si el incidente reportado corresponde a un incidente de seguridad de la información o está relacionado con requerimientos propios de la infraestructura de TI (o incidentes que no son susceptibles de reporte ante las autoridades competentes). En caso de sospechar la ocurrencia de un incidente de seguridad sobre datos personales se notificará de inmediato al departamento legal y a los asesores externos y en conjunto se llevará a cabo un análisis preliminar para determinar el alcance de este y si es del caso, notificar a la Superintendencia de Industria y Comercio dentro de los plazos establecidos por la ley.
- Contención: esta actividad busca la detección del incidente con el fin de que no se propague y puedan generar más daños a la información o a la arquitectura de TI. Para facilitar esta tarea las Compañías deben poseer una estrategia de contención previamente definida para poder tomar decisiones, por ejemplo: apagar sistema, desconectar red, deshabilitar servicios.
- Estrategia de contención: La estrategia de contención varía según el tipo de incidente y los criterios deben estar bien documentados para facilitar la rápida y eficaz toma de decisiones. Algunos criterios que pueden ser tomados como base son:
  - Criterios Forenses
  - Daño potencial y hurto de activos
  - Necesidades para la preservación de evidencia
  - Disponibilidad del servicio
  - Tiempo y recursos para implementar la estrategia
  - Efectividad de la estrategia para contener el incidente (parcial o total)
  - Duración de la solución
- Erradicación y Recuperación: Después de que el incidente ha sido contenido se debe realizar una erradicación y eliminación de cualquier rastro dejado por el incidente como código malicioso y posteriormente se procede a la recuperación a través de la restauración de los sistemas y/o servicios afectados para lo cual el administrador de TI o quien haga sus veces deben restablecer la funcionalidad de los sistemas afectados, y realizar un endurecimiento del sistema que permita prevenir incidentes similares en el futuro.

Capítulo 11 Controles de vulnerabilidad

Las Compañías realizan una revisión de vulnerabilidades a los sistemas de información de las Compañías y han adoptado las siguientes medidas específicas para controlar vulnerabilidades técnicas:

- Las Compañías monitorean que el SharePoint y herramientas corporativas sean usada por los miembros del personal para el desempeño laboral, o para el desarrollo de las funciones, actividades y obligaciones acordadas o contratadas.
- Las Compañías llevan un control de los permisos otorgados a proveedores externos, cuando los mismos deban acceder a los sistemas de las Compañías o a la infraestructura tecnológica.
- Cada área de las Compañías que tengan relaciones con proveedores externos que potencialmente conozcan información de las Compañías, debe solicitar el acompañamiento

constante del departamento administrativo de las Compañías con el fin de dar a conocer la presente Política.

Capítulo 12 Controles de acceso

Las Compañías comprenden la necesidad actual de implementar controles de acceso a sus sistemas de información que brinden una protección efectiva y dinámica, teniendo en cuenta los riesgos asociados, por lo que han implementado las siguientes medidas:

- Las Compañías suministran el acceso a sus redes a todos los miembros del Personal, gestionan los cambios de contraseña, actualización de permisos y accesos a las redes y los diferentes aplicativos. Adicionalmente actualizan los accesos a las aplicaciones y sitios web para evitar que tengan acceso a páginas prohibidas o que sean víctimas de actividades como el Phishing o similares.
- Las Compañías solicitan la modificación periódicamente de la contraseña de la red inalámbrica de las Compañías, en especial la relacionada con la red de visitantes.
- Las Compañías cuentan con autenticador de doble factor, que permita la confirmación de la persona que accede a las herramientas de las Compañías, evitando el acceso de personas no autorizadas
- Las Compañías generan estrategias de centralización de la autenticación y administran el acceso de todos los usuarios a través del correo electrónico corporativo, de modo que cuando se bloquee el acceso al sistema centralizado también se bloquea para las plataformas que usan el correo corporativo.

Capítulo 13 Controles sobre los usuarios

Las Compañías han definido las siguientes herramientas con el fin de controlar la creación y uso de cuentas de usuario:

- Las Compañías otorgarán a los usuarios, los accesos solicitados y autorizados por el jefe inmediato, director del área o supervisor del contrato en caso de ser un contratista.
- Los usuarios creados para miembros del Personal no pueden tener permisos de administrador.
- El usuario y la contraseña asignados a los miembros del Personal son personales e intransferibles.
- Una vez finalizado el contrato laboral a un empleado de las Compañías, el funcionario de recursos humanos o supervisor del contrato debe notificar dicha circunstancia al departamento correspondiente, quien debe garantizar que los accesos y las cuentas de correo quedan cerrados al finalizar el contrato.

Capítulo 14 Controles de seguridad físicos

Las Compañías han implementado las siguientes medidas para proteger sus activos y/o la información almacenada en equipos físicos dentro del perímetro de las Compañías:

- Las Compañías cuentan con sistema de control de acceso a las instalaciones de las Compañías.
- El personal de vigilancia del edificio donde se encuentran ubicadas las instalaciones establece los mecanismos para inspeccionar y examinar los elementos que ingresen visitantes.

Capítulo 15 Controles de seguridad físicos

Las Compañías han definido un esquema para realización de copias de respaldo y restauración de la información de las Compañías de manera segura, permitiendo el respaldo de seguridad de la información de correo electrónico y el correcto almacenamiento de la información corporativo, por el tiempo de retención pertinente.

Capítulo 16 Acceso a la información remota

Las Compañías han implementado los siguientes controles para proteger la seguridad de su información, cuando los miembros de su Personal realicen labores de forma remota:

Las Compañías cuentan con herramientas tecnológicas, tales como DataRoom y SharePoint, para acceder de manera remota a los equipos asignados a los miembros del Personal con el fin de analizar su funcionamiento y garantizar la seguridad de la información y brindar un soporte remoto a estos usuarios.

Toda información gestionada por las Compañías, y que sea accedida remotamente debe ser utilizada solamente para el cumplimiento de las funciones del cargo o de las obligaciones contractuales del mismo

Capítulo 17 Revisión de la seguridad de la información

Las Compañías han definido revisar de manera constante sus medidas de seguridad de la información de la siguiente manera:

- Las Compañías realizarán auditorías internas de manera periódica para comprobar el correcto funcionamiento del Sistema de Gestión de Seguridad de la Información en cuanto a los controles, políticas y procedimientos para la seguridad de la información.
- Los líderes de los procesos deben asegurar que todas las herramientas de seguridad dentro de su área de responsabilidad se realicen correctamente, con el fin de cumplir las políticas y normas de seguridad; en caso de incumplimiento se evaluarán y propondrán acciones correctivas.
- Las Compañías realizarán revisiones del cumplimiento de la presente Política, y, adicionalmente, vinculará a la dirección general de las Compañías con el fin de determinar si los documentos relacionados como la Política de procesamiento de la información están siendo efectivamente implementados por todos los miembros del Personal.

De igual forma las Compañía han establecido la política CTGL-AD-IT-PO-001 Cybersecurity incident emergency managemen con el fin de establecer los lineamientos de seguridad tecnológica

Capítulo 18 Conformidad normativa

Las Compañías deben velar por la identificación, documentación y cumplimiento de la legislación relacionada con la Seguridad de la Información. El departamento administrativo, con el apoyo de los diferentes miembros debe identificar, documentar y mantener actualizados los requisitos legales, reglamentarios o contractuales aplicables a las Compañías y relacionados con seguridad de la

información. Sin excepción, todos los miembros del Personal deberán conocer y adoptar la presente Política, así como las responsabilidades con motivo del ejercicio de sus funciones.

Capítulo 19 Disposiciones suplementarias

Esta Política se prepara de acuerdo con los procedimientos involucrados en la operación cotidiana de las Compañías, que se encuentra en constante cambio, Por este motivo, la Política está sujeta a cambios y ajustes que se irán efectuando conforme sea requerido con la inclusión de nuevos procesos, herramientas y ajustes en las operaciones de las Compañías. Es obligación de todos los miembros del Personal de las Compañías, mantenerse actualizados con esta Política y los procesos asociados a la misma para así desempeñar sus labores de forma adecuada.

Esta política ha sido revisada por el departamento legal y finalmente aprobada por el Comité ejecutivo