The Collace Group Chile SpA

Política de Seguridad de la Información

Código:	POL-SEG-INF-1
Versión:	0.1
Fecha de la versión:	25 de octubre de 2021
Creado por:	Juan Pablo Schele Laso
Aprobado por:	Roberto del Río Cámbara
Nivel de confidencialidad:	Pública

Historial de modificaciones

Fecha	Versión	Creado por	Descripción de la modificación
25-10-2021	0.1	Juan Pablo Schele Laso	Primera versión

Tabla de contenido

1 Introducción

Este documento define la política de seguridad de la información de The Collace Group Chile SpA (TCG en adelante).

Como empresa moderna y con visión de futuro, TCG reconoce en los niveles superiores la necesidad de garantizar que su empresa funcione sin problemas y sin interrupciones en beneficio de sus clientes, accionistas y otras partes interesadas.

Una política de seguridad sólida establece el tono de seguridad para toda la organización e informa a todo el personal qué se espera de ellos. Todo el personal debe conocer los tipos de información confidencial que se conserva y procesa y su responsabilidad de protegerla.

La política está en línea con los requisitos del Estándar Internacional ISO/IEC 27001 para proteger la confidencialidad, integridad y disponibilidad de la información en posesión de TCG.

Esta política se aplica a todos los sistemas, personas y procesos que constituyen los sistemas de información de la organización, incluidos los miembros de la junta, directores, empleados, proveedores y otros terceros que tienen acceso a las plataformas desarrolladas internamente, repositorio de código fuente y de datos de TCG.

Los siguientes documentos de respaldo son relevantes para esta política de seguridad de la información y proporcionan información adicional sobre cómo se aplica:

- Política de protección y retención de datos.
- Política antimalware
- Política de software
- Política de control de acceso
- Política de contraseñas
- Política de gestión de vulnerabilidades técnicas
- Política de mensajería electrónica
- Política de uso aceptable de Internet
- Política de dispositivos móviles
- Política de trabajo remoto
- Política de seguridad de la información para las relaciones con los proveedores de servicios.
- Política de uso aceptable

Política de seguridad de la información

a) Requisitos de seguridad de la información

Se acordará y mantendrá una definición clara de los requerimientos para la seguridad de la información dentro de TCG con los clientes internos del negocio y proveedores externos para que todas las actividades de seguridad de la información se centren en el cumplimiento para proteger los datos confidenciales. Los requisitos legales, reglamentarios y contractuales también serán documentados y aportados al proceso de planificación. Los requisitos específicos con respecto a la seguridad de los sistemas o servicios nuevos o modificados se capturarán como parte de la etapa de diseño de cada proyecto con la intención de que las partes interesadas conozcan de forma correcta la política de seguridad de la información.

Es un principio fundamental del marco de seguridad de la información de TCG que los controles implementados sean impulsados por las necesidades del negocio se comunicarán regularmente a todo el personal, contratistas, proveedores, socios de negocio a través de reuniones de equipo y documentos informativos enviados por correo.

b) Marco para establecer objetivos

Se utilizará un ciclo regular para establecer los objetivos de seguridad de la información, para coincidir con el ciclo de planificación presupuestaria. Esto asegurará que se obtenga la financiación adecuada para las actividades de mejora identificadas. Estos objetivos se basarán en una comprensión clara de las necesidades de negocio, informados por el proceso de revisión de la administración durante el cual se pueden obtener las opiniones de las partes interesadas relevantes.

Los objetivos de seguridad de la información se documentarán durante un período de tiempo acordado, junto con detalles de cómo se lograrán. Estos serán evaluados y monitoreados como parte de las revisiones de la gerencia para asegurar que sigan siendo válidos. Si se requieren modificaciones, éstas se gestionarán a través del proceso de gestión de cambios.

La adopción de estos códigos de práctica proporcionará una garantía adicional a nuestros clientes y ayudará aún más con nuestro cumplimiento.

c) Áreas de política de seguridad de la información

The Collace Group Chile SpA define la política en una amplia variedad de áreas relacionadas con la seguridad de la información que se describen en detalle en un conjunto completo de documentación de políticas que acompaña a esta política general de seguridad de la información.

Cada una de estas políticas está definida y acordada por una o más personas con competencia en el área relevante y, una vez aprobada formalmente, se comunica a una audiencia apropiada, tanto dentro como fuera de la organización.

La siguiente tabla muestra las políticas individuales dentro del conjunto de documentación y resume el contenido de cada política y el público objetivo de las partes interesadas:

Título de la política	Áreas abordadas	Alcance
Política de retención y protección de datos	Período de retención para tipos de datos específicos, uso de criptografía, selección de medios, recuperación de registros, destrucción y revisión.	Empleados responsables de la creación y gestión de registros.
Política criptográfica	Evaluación de riesgos, selección de técnicas, despliegue, prueba y revisión de criptografía y gestión de claves.	Empleados involucrados en la configuración y gestión del uso de tecnología y técnicas criptográficas.
Política antimalware	Firewalls, antivirus, filtrado de correo no deseado, instalación y escaneo de software, gestión de vulnerabilidades, capacitación de conciencia del usuario, monitoreo y alertas de amenazas, revisiones técnicas y gestión de incidentes de malware.	Empleados responsables de proteger la infraestructura de la organización del malware
Política de control de acceso	Registro y baja de usuarios, provisión de derechos de acceso, acceso externo, revisiones de acceso, responsabilidades del usuario y control de acceso a sistemas y aplicaciones.	Empleados involucrados en la configuración y gestión del control de acceso.
Política de contraseñas	Requisitos de contraseña y lineamientos	Todos los empleados
Política de gestión de vulnerabilidades técnicas	Definición de vulnerabilidad, fuentes de información, parches y actualizaciones, evaluación de vulnerabilidad, fortalecimiento y capacitación de concientización.	Empleados responsables de proteger la infraestructura de la organización del malware
Política de mensajería electrónica	Envío y recepción de mensajes electrónicos, monitoreo de servicios de mensajería electrónica y uso de correo electrónico.	Usuarios de servicios de mensajería electrónica.
Política de uso aceptable de Internet	Uso comercial de Internet, uso personal de Internet, administración de cuentas de Internet, seguridad y monitoreo y usos prohibidos del servicio de Internet.	Usuarios del servicio de internet

Política de dispositivos móviles	Cuidado y seguridad de los dispositivos móviles, como computadoras portátiles, tabletas y teléfonos inteligentes, ya sean proporcionados por la organización o el individuo para uso comercial.	Usuarios de dispositivos móviles proporcionados por la empresa y BYOD (Traiga su propio dispositivo)
Política de trabajo remoto	Consideraciones de seguridad de la información en el trabajo remoto y arreglos, p. ej. seguridad física, seguro y equipamiento	La gerencia y los empleados involucrados en la configuración y el mantenimiento del trabajo remoto
Política de seguridad de la información para relaciones con proveedores de servicios	Due diligence, acuerdos de proveedores de servicios, monitoreo y revisión de servicios, cambios, disputas y finalización de contrato.	Empleados involucrados en la creación y gestión de relaciones con proveedores de servicios.

d) Aplicación de la política de seguridad de la información

Las declaraciones de política formuladas en este documento y en el conjunto de políticas de respaldo enumeradas en la Tabla 1 han sido revisadas y aprobadas por la alta dirección de TCG y deben cumplirse. El incumplimiento por parte de un empleado de estas políticas puede dar lugar a la adopción de medidas disciplinarias de conformidad con el proceso disciplinario de los empleados de la organización.

Las preguntas relacionadas con cualquier política de TCG deben dirigirse en primera instancia al gerente de línea inmediata del empleado.

Validez y gestión de documentos

Este documento es válido hasta el 31 de diciembre de 2022

El propietario de este documento es el oficial de seguridad de la información, que debe verificar, y si es necesario actualizar, el documento por lo menos una vez al año.