Política

Seguridad de la Información

Público

Objetivo
Definir, establecer y proteger la disponibilidad, integridad y confidencialidad de toda la información relacionada con nuestros servicios.

Alcance
Aplica para todos los empleados, consultores, visitantes, que se involucren en todos los centros de Call Center Services S.A. de C.V.

Departamento y Área
Tecnologías de la Información, Ciberseguridad.

Responsable
Gerente TI.

Creación / Actualización
Analista Ciberseguridad.

Control Documental
Coordinador de Gestión de Procesos.

Revisión
Analista Ciberseguridad.

Autorización
Director de TI.

Última revisión	Inicio vigencia	Versión	Código
Oct20,2025	Oct23,2025	13	E_AIT-002_P

I. Política

Inducción

En Call Center Services International nos comprometemos a proteger los activos de información, garantizando su confidencialidad, integridad y disponibilidad, en cumplimiento con la norma **ISO/IEC 27001**.
Implementamos un **Sistema de Gestión de Seguridad de la Información (SGSI)** que promueve la mejora continua, la gestión de riesgos y la continuidad del negocio para asegurar la resiliencia operativa.

La Alta Dirección respalda explícitamente este sistema, asegurando el cumplimiento legal, regulatorio y contractual, la concienciación del personal y la protección de la información en todas nuestras operaciones, así como el compromiso con la protección del medio ambiente mediante prácticas sostenibles.

NOTA: Esta política es compartida con clientes y proveedores, fomentando una colaboración alineada en la protección de los datos y la entrega de servicios confiables y seguros.

La información se clasificará con base al **Procedimiento de Control de documentos y registros** con la finalidad de entregar información relacionada a las operaciones internas de la Organización y sus clientes (internos / externos), quienes se encuentren fuera del ámbito de acceso controlado.

1. Responsables de la Seguridad de la Información

El equipo de Ciberseguridad (CS), en apoyo con el Departamento de Cumplimiento y el Departamento de Tecnologías de la Información (TI), contará con la responsabilidad de supervisar, controlar, revisar y aplicar la Política de Seguridad de la Información. El uso racional de los recursos de CCSI deberá ser conducido por el Departamento de TI incluyendo, pero no limitándose a las siguientes actividades:

I. Asegurar e implementar a nivel Corporativo que los Colaboradores cumplan con la política.
II. Trabajar en conjunto con los Directores y Gerentes de Operaciones para que su personal a cargo cumpla con la política.
III. Proporcionar seguimiento cuando se revise un reporte de cualquier Colaborador que tenga conocimiento de cualquier violación o sospecha de violación de esta política.
IV. Asegurar que la información se clasifique conforme los lineamientos del **Procedimiento Control de Documentos y Registros.**
V. Validar que los servicios prestados sean diseñados e implementados apegándose al cumplimiento de la Seguridad de la información definidos en este documento.
VI. El Departamento TI tiene la responsabilidad y autoridad primaria sobre todos los componentes de la infraestructura de TI. Todos los dispositivos, aplicaciones, bases de datos y otros componentes deben estar alineados a las políticas de TI de la Organización.
VII. El Equipo de CS revisará y gestionará todas las prácticas del cliente que se desvíen de las directrices de esta política, contactando y compartiendo la aceptación de responsabilidad del cliente antes de cualquier implementación.
VIII. Esta política debe ser reforzada a todos los colaboradores a través de campañas de difusión internas como: Exposiciones por Videollamada, publicaciones en la plataforma GoCCSI, avisos organizacionales, infográficos impresos o cualquier medio de comunicación corporativa oficial cada 6 meses con la finalidad de asegurar el cumplimiento de la misma.

NOTA: Las unidades de negocio o departamentos podrán establecer procedimientos adicionales que resulten relevantes a su operación. Esos procedimientos podrán proveer detalles más específicos y/o restrictivos, siempre y cuando no conflictúen con esta política de seguridad.

2. Uso Aceptable

El uso del Correo Electrónico Corporativo será exclusivo para cuestiones directamente relacionadas el trabajo asignado dentro de la empresa, con total exclusión de cuestiones personales o motivos ajenos al trabajo, con base en lo estipulado en la política de **Cuentas y Acceso a Recursos Digitales**.

Todos los correos corporativos deberán incluir la nota de confidencialidad en la firma del cuerpo del correo de acuerdo a lo establecido en la **Política de Imagen Corporativa**.

Las herramientas y el equipo de Tecnología de la Información proporcionados por CCSI son para uso del negocio. Es por ello que no se permite el uso personal de ningún equipo de cómputo, teléfono o aplicación. Las cuentas y servicios de TI son proveídas únicamente a los empleados activos en la organización.

Las cuentas y servicios de TI serán proveídas únicamente a los empleados activos en la organización.

La Política de Contraseñas establece las normas para la creación, distribución, resguardo, terminación y reclamación de los mecanismos de autenticidad de CCSI con base en lo estipulado por la **Política de Contraseñas.**

Toda la Infraestructura de Tecnología ha sido implementada de tal manera que no se encuentre expuesta a la intromisión o ataques aleatorios. Buscando siempre proveer el mantenimiento apropiado a la infraestructura, con referencia a la **Política de Gestión del Cambio.**

Toda papelería, cuadernos, tarjetas, post-it, plumas, lápices, marcadores y artículos similares No están permitidos en el área de operaciones a menos que estén propiamente autorizados por la Alta Dirección mediante la **Carta Responsiva de autorización de excepción al esquema sin papel** y **Aceptación y Conocimiento del Riesgo**. Esto debido a que trabajamos en cumplimiento con el ambiente "Paperless and Clean Desk Policy" tal como lo especifica la **Política Corporativa** y **Política de Información de la Compañía**, que establece lineamientos para la transferencia de información y a su vez garantizar trazabilidad de procesos.

Los empleados deben utilizar el acceso a Internet de la empresa estrictamente para fines relacionados con el trabajo y de una manera responsable que garantice la seguridad y la eficacia. El uso personal debe ser mínimo y no debe interferir con las responsabilidades laborales.

Está estrictamente prohibido acceder, transmitir o descargar contenidos inapropiados, ilegales o de alto riesgo (como juegos de azar, material para adultos o sitios conocidos por su malware). Las redes de invitados se proporcionan para mayor comodidad, pero no deben utilizarse para acceder a sitios web restringidos, de alto riesgo o no relacionados con la empresa, de acuerdo con la **Política de redes inalámbricas**.

3. Controles de Acceso y Confidencialidad de la Información

El equipo de Ciberseguridad colaborará con Capital Humano, Legal y Tecnologías de la Información para garantizar que los controles de acceso, el cumplimiento legal y los procesos de incorporación/separación de personal estén alineados con los requisitos de seguridad establecidos por la organización.

Todo el personal de nuevo ingreso tanto administrativo como operativo, deberá firmar el **Paquete de Inducción** al finalizar su Curso de Inducción y el **Conocimiento Política Seguridad Información**, mediante la cual se comprometen a apegarse y cumplir con las normas y criterios establecidos por CCSI.

Todo el personal que se envíe a trabajar en modalidad de WFH, deberá firmar el formato **Carta de Confidencialidad.**
Todo el personal administrativo de nuevo ingreso debe firmar la **Carta de Confidencialidad,** anexo dentro del **Paquete de Inducción.**

Todo proveedor o contratista deberá firmar la documentación correspondiente para comprometerse a salvaguardar la información a la que tenga acceso, conforme lo indica el procedimiento de **Selección y Evaluación de Proveedores**.
Todos los sistemas deberán tener controles de acceso .

Todo acceso a internet será controlado y monitoreado por los Proxy y Firewalls definidos por el Departamento de TI en CCSI. Cuando un área operativa existente o nueva requiera acceso abierto y/o sin restricciones o filtros de seguridad a internet deberá ser autorizado por el cliente a través del Formato de **Aceptación y Conocimiento del Riesgo.**

Todos los equipos y sistemas de usuario serán gestionados y controlados mediante el procedimiento de **Procedimiento Control de Acceso,** procedimiento de **Procedimiento de Control de Acceso Físico** y **Política de Cuentas y Accesos a Recursos Digitales.**

En caso de que algún proveedor solicite acceso al centro de datos deberá ser registrado mediante nuestro documento **Formato de Registro Acceso a Centro de Datos.** El acceso deberá ser provisto el responsable de la actividad conforme a la **Política de Control de Acceso Físico.**

4. Dispositivos Electrónicos

Todo el equipo de fotografía y cámara de video (portátil o no) está estrictamente prohibido en CCSI, a menos que esté autorizado través del **Formato Permiso para Foto-Video** por Alta Dirección de CCSI establecida en **Organigrama CCSI** y se solicite de acuerdo al **Procedimiento Seguimiento a Dispositivos de Almacenamiento y Electrónicos.**

Todos los equipos externos, como computadoras portátiles y/o dispositivos móviles; deben estar autorizados solicitados como se indica en la política **BYOD Trae tu Propio Dispositivo** y **procedimiento Aprobación de BYOD** mediante BYOD Service Request (https://goccsi.net). Estos registros deberán ser auditables y disponibles en Base de datos en Plataforma Interna de dispositivos aprobados y rechazados.

En caso de que la necesidad del Cliente amerite el uso de dispositivos ajenos a los proporcionados por CCSI, deberá ser autorizado por el Cliente mediante **Formato Aceptación y Conocimiento del Riesgo** y por el Director de Operaciones a través de **BYOD Service Request.**

El usuario autorizado deberá firmar **Formato Carta Responsiva de Aceptación de Usuario para el uso de dispositivo propio**.
El acceso a Internet deberá de ser solicitado de acuerdo a **Formato Aceptación y Conocimiento del Riesgo.**
La carga eléctrica de dispositivos móviles está estrictamente prohibida dentro del área de operaciones, a excepción de laptops previamente autorizadas.

Todo equipo perteneciente a la Organización como laptops, telefonía móvil, auricular, entre otros, debe contar con **Formato Carta Responsiva Equipo de TI** firmada por cada responsable del equipo.

Todos los dispositivos electrónicos no autorizados con capacidad de almacenamiento (tales como: reproductores MP3, grabadoras de sonido, memorias USB portátiles, bolígrafos electrónicos, dispositivos multimedia portátiles, relojes inteligentes y equipos similares) están estrictamente prohibidos dentro de las instalaciones operativas, administrativas, de entrenamiento y/o áreas de actividades laborales de CCSI de acuerdo a la **Política Corporativa**.

Estos únicamente podrán ser usados en áreas comunes y/o de descanso. Durante la jornada laboral deberán ser resguardados en sus lockers o áreas asignadas para este fin.

Está prohibido conectar en los equipos de cómputo de CCSI cualquier dispositivo electrónico de almacenamiento.

El departamento de Tecnologías de la Información está autorizado a utilizar y conectar únicamente dispositivos de almacenamiento electrónico propiedad de CCSI y sólo para fines relacionados con el trabajo

La configuración de correo del dominio CCSI o del dominio Cliente / Cuenta no se instalará en dispositivos móviles a menos que sea aprobada por el cliente y la solicitud de servicio sea autorizada a través del **Procedimiento de Aprobación BYOD**

5. Controles de Seguridad en Hardware y Software

CCSI mantendrá una copia de seguridad actualizada de toda la información resguardada en los sistemas de servidores de la Organización. Esto incluye, pero no se limita, a los archivos, hojas de cálculo, bases de datos utilizadas por la Organización, cualquier información requerida por las autoridades, así como información que se requiera recuperar en caso de algún desastre como se indica en el **Procedimiento de Restauración y Copia de Seguridad.**

Todos los cambios requeridos al equipo o software de TI deberán ser aprobados por TI.
Los cambios a los Niveles de Servicio, se realizan de acuerdo a **Acuerdos de Nivel de Servicio.**

6. Incidentes

Todo incidente deberá ser reportado, manejado, gestionado y resuelto apegándose a lo establecido en el **Procedimiento Gestión de Incidentes.**

7. Penalizaciones

La Política de la Seguridad de la Información penalizara de acuerdo con lo siguiente:

a) **Personal Administrativo**: Será penalizado de acuerdo a **Reglamento Interior de Trabajo** y **Ciclo Disciplinario.**
b) **Personal Operativo**: Será penalizado de acuerdo a **Reglamento Interior de Trabajo** y **Ciclo Disciplinario.**
c) **Personal de Formación Profesional (Practicantes):** Será penalizado de acuerdo a **Reglamento Interior de Trabajo** y **Ciclo Disciplinario.**

d) **Visitantes**: Se abordará con una advertencia verbal.
e) **Contratistas:** Se abordará con una advertencia verbal en caso de reincidir se dará el aviso de recisión de contrato**.**
f) **Proveedores**: Se abordará con una advertencia verbal en caso de reincidir se dará el aviso de recisión de contrato.

Aquellos empleados de los que razonablemente se sospeche haber comprometido la seguridad de la información estarán sujetos a la terminación de contrato con la Compañía, de acuerdo al **Ciclo Disciplinario**.

Cualquier empleado que interfiera o se rehúse a cooperar con una investigación corporativa de alguna falta a la política será sujeto a acciones disciplinarias, hasta e incluyendo la terminación de contrato con la Organización, de acuerdo al **Ciclo Disciplinario**.

En caso de que algún Supervisor o Gerente haga uso inadecuado de los recursos de TI se aplicaran las sanciones mencionadas en el **Reglamento Interior de Trabajo**. La reincidencias y gravedad del incumplimiento serán sancionadas conforme a **Ciclo Disciplinario**.

Todo el material de video y fotografía que se encuentre publicado en **Sitios Web Públicos**, así como **Correos Electrónicos** sin previa autorización, se le pedirá cuentas al dueño del perfil del sitio web o publicación y será sujeto a investigación, sanción y/o si el caso lo amerita, terminación de contrato con la Organización.

CCSI colaborará con las fuerzas policiacas en sus esfuerzos de investigación en caso de existir alguna violación de alguna ley estatal o federal relacionado con la seguridad de la información. En caso de que CCSI sospeche de alguna violación de alguna ley, CCSI podrá solicitar a las fuerzas policiacas la investigación del caso.