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

Documento exclusivo de CCSI y entes relacionados autorizados. Consultar versión vigente en SG Oficial.
Prohibido el uso total/parcial del documento sin autorización. Todo abuso será castigado conforme a la ley.

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.

Documento exclusivo de CCSI y entes relacionados autorizados. Consultar versión vigente en SG Oficial.
Prohibido el uso total/parcial del documento sin autorización. Todo abuso será castigado conforme a la ley.

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.**

Documento exclusivo de CCSI y entes relacionados autorizados. Consultar versión vigente en SG Oficial.
Prohibido el uso total/parcial del documento sin autorización. Todo abuso será castigado conforme a la ley.

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.

Documento exclusivo de CCSI y entes relacionados autorizados. Consultar versión vigente en SG Oficial.
Prohibido el uso total/parcial del documento sin autorización. Todo abuso será castigado conforme a la ley.

Policy

Information Security

Public

Objective
Define, establish and protect the availability, integrity and confidentiality of all information related to our services.

Scope
Applies to all employees, consultants, visitors, who are involved in all Call Center Services S.A. de C.V. centers.

Department & Area
Information Technologies, Cybersecurity.

Responsible
IT Manager.

Elaborated by
Cybersecurity Analyst.

Document Control
Process Management Coordinator.

Reviewed by
Cybersecurity Analyst.

Approved by
IT Director.

Last Review	Effective Date	Version	ID
Oct20,2025	Oct23,2025	13	E_AIT-002_P

This document is exclusive to CCSI and authorized entities. Refer to the current version in the Official CCSI MS.
Unauthorized use, in whole or in part, is prohibited and will be penalized by law.

I. Policy

Introduction

At Call Center Services International we are committed to protecting information assets, ensuring their confidentiality, integrity and availability, in line with the **ISO/IEC 27001** standard. We implement an **Information Security Management System (ISMS)** that promotes continuous improvement, risk management and business continuity to ensure operational resilience.

Top Management explicitly endorses this system, ensuring legal, regulatory and contractual compliance, staff awareness and information protection throughout our operations, as well as a commitment to environmental protection through sustainable practices.

This policy is shared with vendors and contractors, fostering an aligned collaboration in data protection and the delivery of reliable and secure services.

NOTE: This policy is shared with clients and suppliers, promoting aligned collaboration in data protection and the delivery of reliable and secure services.

All information will be classified in the **Document Control and Records Procedure** in order to deliver information related to the internal operations of the Organization and its clients (internal / external), who are outside the scope of controlled access.

1. Information Security Responsible

Cybersecurity Team, in support with the Compliance Department and Information Technologies Department (IT), will have the responsibility of supervising, controlling, reviewing and applying the Information Security Policy. The rational use of CCSI resources should be conducted by the IT department including, but not limited to the following activities:

I. Ensure and implement at the Corporate level that employees are informed and comply with the policy.
II. Work altogether with the Operations Directors and Managers so that their personnel in charge can comply with the policy.
III. Provide follow-up when reviewing a report from any employee who becomes aware of any violation or suspected violation of this policy.
IV. Ensure that the information is classified according to the guidelines of **Document Control and Records Procedure.**
V. Validate that services provided are designed and implemented in compliance with the Information Security defined in this document.
VI. IT Department has primary responsibility and authority over all components of the IT infrastructure. All devices, applications, databases and other components must be aligned with the IT policies of the Organization.
VII. The Cybersecurity team shall review and manage all client practices that deviate from the guidelines of this policy, contacting and sharing the client's acceptance of responsibility before any implementation.
VIII. This policy must be reinforced to all collaborators every six months, through the GoCCSI Platform on a regular basis in order to ensure compliance with it.

NOTE: Business units or departments may establish additional procedures that are relevant to their operation. These procedures may provide more specific and / or restrictive details, as long as they do not conflict with this security policy.

2. Acceptable Use

The use of Corporate Email will be exclusive for issues directly related to the work assigned within the company, with total exclusion of personal issues or reasons unrelated to work, according to policy **Accounts and Digital Resources Access**.

All corporate emails must include the confidentiality notice in the signature of the body of the email according to **Corporate Image Policy**.

Information Technology tools and equipment provided by CCSI are for business proposal. For this reason, personal use of any computer, phone or software are not allowed based on with the stipulated on the **Password Policy**.

To ensure process traceability, establish guidelines for the appropriate use of official tools, and consult the protocols for information transfer, the provisions set forth in policy **Company Data** must be taken into account.

IT account and services will be provided by IT Department for only active employees in the Organization.

The Password Policy establishes the rules for the creation, distribution, safeguarding, termination and reclamation of the CCSI authenticity mechanisms based on the provisions of the **Password Policy**.

All the Technology Infrastructure has been implemented in such a way that it is not exposed to intrusion or random attacks. Always seeking to provide the appropriate maintenance to the infrastructure, with reference to the **Change Management Policy.**

All stationery, notebooks, cards, post-its, pens, pencils, markers and similar items are not allowed in the operations area unless properly authorized by the Client troughs **Non-Paper Authorization Waiver** and **Acceptance and Knowledge of Risk Format**. This is because we work in compliance with the **"Paperless and Clean Desk Policy"** environment as specified in **Corporate Policy** and **Company Data**, which establishes guidelines for information transfer and ensures process traceability.

Employees must use the company's internet access strictly for business-related purposes and in a responsible manner that ensures security and efficiency. Personal use should be minimal and must not interfere with work responsibilities. .

Accessing, transmitting, or downloading inappropriate, illegal, or high-risk content (such as gambling, adult material, or sites known for malware) is strictly prohibited. Guest networks are provided for convenience but must not be used to access restricted, high-risk, or non-business-related websites according to **Wireless Network Policy**.

3. Access Controls and Information Confidentiality

The Cybersecurity team will collaborate with Human Capital, Legal, and Information Technologies to ensure that access controls, legal compliance, and employee onboarding/offboarding processes are aligned with the security requirements established by the organization.

All new operational or administrative personnel, must sign a **Onboarding Package** and **Information Security Policy Acknowledgement** upon completion of their Induction Course, by means of which they undertake to adhere to and comply with the standards and criteria established by CCSI.

All new administrative and operations personnel must sign out the **Confidentiality Notice**, in addition to **Onboarding Package**.

This document is exclusive to CCSI and authorized entities. Refer to the current version in the Official CCSI MS.
Unauthorized use, in whole or in part, is prohibited and will be penalized by law.

All equipment and user systems will be managed and controlled through the **Access Control Procedure**, **Physical Access Control Procedure** and **Accounts and Digital Resources Access Policy.**

In the event that a provider requests access to the data center, it must be registered through our **Data Center Access Log**. Access must be provided by the activity responsible in accordance to the **Physical Access Control Policy**.

4. Electronics devices

All photography and video camera equipment (handheld or not) is strictly prohibited at CCSI, unless is authorized by Senior Direction of **CCSI by Photo-Video Permission** establishes in **Organization Chart** and requested through **Electronic Storage Device Follow Up.**

All external equipment, such as laptops and/or mobile devices; must be authorized requested as outlined in the **BYOD Bring Your Own Device policy** and **PIT-052_P BYOD Approval Procedure** using **BYOD Service Request (https://goccsi.net).** These records must be auditable and available on **GoCCSI database of approved and rejected devices.**

In the event that the Client's need warrants the use of devices other than those provided by CCSI, it must be authorized by the Client through **Acceptance and Awareness of Risk Format** and by the Operations Director through **BYOD Service Request**

The authorized user must sign **Responsive Letter of User Acceptance for the use of their own device.**

Internet access must be requested in accordance with **Acceptance and Awareness of Risk.**

Mobile devices electrical charging is strictly prohibited within the area of operations, with the exception of previously authorized laptops.

All equipment belonging to the Organization such as laptops, mobile telephony, headset, among others, must have a responsive letter signed by each person responsible of the equipment. Please refer to **IT Responsive Letter.**

All electronic devices with storage capacity are strictly prohibited inside areas like: Operations, Administrative, Training; according to **Corporate Policy**. Devices such as: MP3 players, sound recorders, portable USB memories, electronic pens, portable media devices, smartwatch and similar equipment. These can only be used in common areas and/or rest. During the working day they must be sheltered in their lockers or areas assigned for this purpose.

It is prohibited connect in the CCSI computer equipment any type of electronic storage device.

Information Technologies department are allowed to use and connect only electronic storage devices property of CCSI and only for work related purposes.

CCSI domain or Client / Account domain mail configuration will not be installed on mobile devices unless it is approved by the Client and the service request is created as indicated in **BYOD Approval Process**.

5. Hardware and Software Security Controls

CCSI will maintain an update nightly backup of all the information stored in the Organization's server systems. This includes, but is not limited to, files, spreadsheets, databases used by the Organization, any information required by the authorities, as well as information that needs to be recovered in the event of a disaster. Please refer to the **Backup and Restore Procedure.**

All required changes to IT equipment or software must be approved by IT. Please refer to the **IT Service Level Agreement.**

6. Incidents

All incidents must be reported, handled, managed, and resolved by adhering to the Incident Reporting Procedures. For all IT incidents please refer to **Incident Management Procedure.**

7. Penalties

The Information Security Policy will penalize in accordance with the following:

a) **Administrative Personnel**: Will be penalized according to the **Disciplinary Cycle and RIT Internal Employee Handbook.**
b) **Operational Personnel**: Will be penalized according to the **Disciplinary Cycle and RIT Internal Employee Handbook.**
c) **Professional Training Personnel (Interns)**: Will be penalized according to the **Disciplinary Cycle and RIT Internal Employee Handbook.**
d) **Visitors:** Will be addressed with a verbal warning.
e) **Contractors**: Will be addressed with a verbal warning in case of recurrence, the notice of contract termination will be given.
f) **Vendors:** It will be addressed with a verbal warning in case of recurrence, the notice of contract termination will be given.

Those employees who are reasonably suspected of having compromised the security of the information will be subject to the termination of the contract with the Organization.

Any employee who interferes with or refuses to cooperate with a corporate investigation of a violation of this policy will be subject to disciplinary action, up to and including termination of contract with the Company according to **Disciplinary Cycle**.

In the event that any Supervisor or Manager makes inappropriate use of IT resources, the sanctions mentioned in the **RIT - Internal Employee Handbook** will be applied. If the employee repeats the contract termination may apply according to **Disciplinary Cycle**.

All video and photography material that is published on **Public Websites**, as well as **Emails** without prior authorization, will be held accountable to the owner of the website or publication profile and will be subject to investigation, sanction and / or if the case merits it, contract termination with the Organization.

CCSI will collaborate with the police forces in their investigation efforts in the event of any violation of any state or federal law related to information security. In the event that CCSI suspects a violation of any law, CCSI may request the police forces to investigate the case.

This document is exclusive to CCSI and authorized entities. Refer to the current version in the Official CCSI MS.
Unauthorized use, in whole or in part, is prohibited and will be penalized by law.