Política

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, Irving Lugo.

Creación / Actualización
Analista Ciberseguridad, Aranza Sainz.

Control Documental
Coordinador de Gestión de Procesos, Illya Garcia.

Revisión
Analista Ciberseguridad, Aranza Sainz.

Autorización
Director de TI, Luis Veana.

Última revisión	Inicio vigencia	Versión	Código
Oct20,2025	Oct23,2025	13	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 **PCUGP-001_P 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 **PCUGP-001_P 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 **AIT-018_P 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 **AVMMK-001_P 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 **AIT-001_P 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 **AIT-004_P 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 **FCUGP-026_I Non-paperless Authorization Waiver** y **FIT-051_P 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 **ACHCH-004_P Política Corporativa** y **AIT-012 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 **AIT-030_P 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 **FCHDO-003_P Paquete de Inducción** al finalizar su Curso de Inducción y el **FIT-010_I 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 **FCHAP-022_P Carta de Confidencialidad.**

Todo el personal administrativo de nuevo ingreso debe firmar la **FCHAP-022_P Carta de Confidencialidad,** anexo dentro del **FCHDO-003_P 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 **PFNCO-001_I 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 de **FIT-051_P Aceptación y Conocimiento del Riesgo.**
Todos los equipos y sistemas de usuario serán gestionados y controlados mediante el procedimiento de **PIT-003_P Procedimiento Control de Acceso,** procedimiento de **PIT-004_I Control de Acceso Físico** y **AIT-018_P Cuentas y Accesos a Recursos Digitales.**

En caso de que algún proveedor solicite acceso al centro de datos deberá ser registrado mediante nuestro documento **FIT-030_I Registro Acceso a Centro de Datos.** El acceso deberá ser provisto el responsable de la actividad conforme al **AIT-027_P 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 de **FIT-011_I Permiso para Foto-Video** por Alta Dirección de CCSI establecida en **DCHCH-001_P Organigrama CCSI** y se solicite de acuerdo a **PCUGP-002_P 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 AIT-031_P BYOD Trae tu Propio Dispositivo y procedimiento PIT-052_P Procedimiento Aprobación de BYOD mediante BYOD Service Request (https://goccsi.net). Estos registros deberán ser auditables y disponibles en Base de datos en GoCCSI 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 **FIT-051_P Aceptación y Conocimiento del Riesgo** y por el Director de Operaciones a través de **BYOD Service Request (https://goccsi.net).**

El usuario autorizado deberá firmar **FIT-065_P Carta Responsiva de Aceptación de Usuario para el uso de dispositivo propio**.
El acceso a Internet deberá de ser solicitado de acuerdo a **FIT-051_P 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 **FIT-029_I 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 **ACHCH-004_P 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 de **PCUGP-002_P Seguimiento a Dispositivos de Almacenamiento y Electrónicos**

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 **PIT-028_I 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 **DIT-022_P Acuerdos de Nivel de Servicio.**

6. Incidentes

Todo incidente deberá ser reportado, manejado, gestionado y resuelto apegándose a lo establecido en **PIT-002_I 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 **ACHCH-001_P Reglamento Interior de Trabajo** y **PCHAP-006_P Ciclo Disciplinario.**
b) **Personal Operativo**: Será penalizado de acuerdo a **ACHCH-001_P Reglamento Interior de Trabajo** y **PCHAP-006_P Ciclo Disciplinario.**
c) **Personal de Formación Profesional (Practicantes):** Será penalizado de acuerdo a **ACHCH-001_P Reglamento Interior de Trabajo** y **PCHAP-006_P 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 a **PCHAP-006_P 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 a **PCHAP-006_P 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 **ACHCH-001_P Reglamento Interior de Trabajo**. La reincidencias y gravedad del incumplimiento serán sancionadas conforme a **PCHAP-006_P 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.

II. Documentos y Registros

Una vez transcurrido el periodo de almacenamiento establecido, se procederá a la disposición del documento de acuerdo con su formato: Electrónico - Eliminar el archivo de forma segura, garantizando la completa destrucción de la información / Físico - Triturar y desechar el archivo de manera adecuada para asegurar la destrucción irreversible de la información.

Código	Nombre	Tiempo de Retención	Tipo de Archivo	Ubicación	Responsable
PCUGP-001	Procedimiento Control de Documentos y Registros	Mientras se encuentre vigente	Referencia digital	SP - CU - Procedimientos	Coord. Gestión de Procesos
AVMMK-001	Política de Imagen Corporativa	Mientras se encuentre vigente	Referencia digital	SP - MK - Políticas	Director de Marketing
AIT-001	Política de Contraseñas	Mientras se encuentre vigente	Referencia digital	SP - IT - Políticas	Director de TI
AIT-004	Política de Gestión del Cambio	Mientras se encuentre vigente	Referencia digital	SP - IT - Políticas	Director de TI
FCUGP-026	Non-paperless Authorization Waiver	24 meses	Registro digital	SP - CU - Formatos	Coord. Gestión de Procesos
ACHCH-004	Política Corporativa	Mientras se encuentre vigente	Referencia digital	SP - CH - Políticas	Director de Capital Humano
FCHDO-003	Paquete de Inducción	24 meses	Registro digital	SP - CH - Formatos	Director de Capital Humano
FCHAP-022	Carta de Confidencialidad	24 meses	Registro digital	SP - CH - Formatos	Director de Capital Humano
FIT-010	Conocimiento Política Seguridad Información	24 meses	Registro digital	SP - IT - Formatos	Director de TI
PFNCO-001	Selección y Evaluación de Proveedores	Mientras se encuentre vigente	Referencia digital	SP - FN - Procedimientos	Director de Finanzas
FIT-051	Aceptación y Conocimiento del Riesgo	24 meses	Registro digital	SP - IT - Formatos	Director de TI
PIT-003	Procedimiento Control de Acceso	Mientras se encuentre vigente	Referencia digital	SP - IT - Procedimientos	Director de TI
PIT-004	Control de Acceso Físico	Mientras se encuentre vigente	Referencia digital	SP - IT - Procedimientos	Director de TI
AIT-018	Cuentas y Accesos a Recursos Digitales	Mientras se encuentre vigente	Referencia digital	SP - IT - Políticas	Director de TI
FIT-030	Registro Acceso a Centro de Datos	24 meses	Registro digital	SP - IT - Formatos	Director de TI
AIT-027	Política de Control de Acceso Físico	Mientras se encuentre vigente	Referencia digital	SP - IT - Políticas	Director de TI
FIT-011	Permiso para Foto-Video	Mientras se encuentre vigente	Registro digital	SP - IT - Formatos	Director de TI
DCHCH-001	Organigrama CCSI	Mientras se encuentre vigente	Referencia digital	SP - CH - Documentos	Director de Capital Humano
FIT-051	Aceptación y Conocimiento del Riesgo.	Mientras se encuentre vigente	Referencia digital	SP - IT - Formatos	Gerente de TI
-	BYOD Service Request	Mientras se encuentre vigente	Registro digital	GoCCSI.net	Director de TI
-	Base de datos en GoCCSI de dispositivos aprobados y rechazados	Mientras se encuentre vigente	Registro digital	GoCCSI.net	Director de TI
PIT-052	Procedimiento de Aprobación de BYOD	Mientras se encuentre vigente	Referencia digital	SP - IT - Procedimientos	Director de TI
FIT-065	Carta Responsiva de Aceptación de Usuario para el uso de dispositivo propio	Mientras se encuentre vigente	Registro digital	SP - IT - Formatos	Gerente de TI
FIT-029	Carta Responsiva Equipo de TI	24 meses	Registro digital	SP - IT - Formatos	Director de TI
PIT-028	Procedimiento de Restauración y Copia de Seguridad	Mientras se encuentre vigente	Referencia digital	SP - IT - Procedimientos	Director de TI
DIT-022	Acuerdos de Nivel de Servicio	Mientras se encuentre vigente	Referencia digital	SP - IT - Documentos	Director de TI
PIT-002	Procedimiento Gestión de Incidentes	Mientras se encuentre vigente	Referencia digital	SP - IT - Procedimientos	Director de TI
ACHCH-001	Reglamento Interior de Trabajo	Mientras se encuentre vigente	Referencia digital	SP - CH - Políticas	Director de Capital Humano
PCHAP-006	Ciclo Disciplinario	Mientras se encuentre vigente	Referencia digital	SP - CH - Procedimientos	Director de Capital Humano
AIT-030	Política de redes inalámbricas	Mientras se encuentre vigente	Referencia digital	SP - IT - A - Políticas	Gerente de TI
AVMMK-001	Política de Imagen Corporativa	Mientras se encuentre vigente	Referencia digital	SP - MK - A - Política	Director de Marketing
AIT-012	Información de la Compañía	Mientras se encuentre vigente	Referencia digital	SP - IT - A - Políticas	Gerente de TI
AIT-018	Cuentas y Acceso a Recursos Digitales	Mientras se encuentre vigente	Referencia digital	SP - IT - A - Políticas	Gerente de TI

III. Definiciones

Palabra	Definición
PCR	Lector de tarjetas de proximidad (acrónimo por sus siglas en Inglés).

IV. Indicadores Relacionados

Indicador	Descripción	Frecuencia
-	-	-

V. Autorización

Departamento y Área: Tecnologías de la Información, Ciberseguridad.

Medio de aprobación: Correo electrónico

VI. Control de cambios

Versión	Descripción del Cambio	Vigencia	Solicitante	Creación / Actualización	Control Documental	Autorización
1	Creación.	Jun26,2014	IT Manager, Luis Veana	IT Manager, Luis Veana	IT Manager, Luis Veana	VPO, Jorge Oros
2	Se agregó mención de FIT-028.	Feb19,2015	Andrea Salgado	Andrea Salgado	Andrea Salgado	VPO, Jorge Oros
3	Se agregó mención FIT-030.	Apr01,2016	Andrea Salgado	Andrea Salgado	Andrea Salgado	Director General, José Luis Rosas
4	Se agregó sección 5. Política de Seguridad de la Información - 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. Esto debido a que trabajamos en cumplimiento con el ambiente "Paperless / Escritorio limpio (clean desk)."	May02,2018	Coordinador de Seguridad de la Información, Alejandra Sánchez	Coordinador de InfoSec, Alejandra Sánchez	Coordinador de InfoSec, Alejandra Sánchez	Director General, Gustavo León
5	Samantha Rodríguez y Luis Martínez se agregaron como responsables.	Dec18,2019	Coordinador de Cumplimiento, Samantha Rodríguez	Coordinador de Cumplimiento, Samantha Rodríguez	Coordinador de Cumplimiento, Samantha Rodríguez	Director General, Luis Martínez
6	Se agrega política: - Está prohibido copiar, mover y / o almacenar datos de titulares de tarjetas en discos duros locales y / o medios electrónicos extraíbles.	Aug31,2020	Coordinador de Seguridad de la Información, Alejandra Sánchez	Coordinador de InfoSec, Alejandra Sánchez	Coordinador de InfoSec, Alejandra Sánchez	Director General, Luis Martínez
7	Se realizó revisión y actualización de la política, agregando las siguientes modificaciones: - Se migró a nuevo formato. - Se agregó **esquema visual**. - Se seccionaron las políticas por tópico, agregando los títulos del **1.1** al **1.7** - Se revisó redacción en la política. - Se actualizaron los responsables de control documental y responsables. - Se actualizan títulos de los documentos mencionados en todo la política.	Dec15,2020	Analista de Seguridad de la Información, Aranza Sainz	Coordinador de InfoSec Alejandra Sánchez	Coordinador de InfoSec Alejandra Sánchez	Director General, Luis Martínez
8	La política fue revisada y actualizada, agregando las siguientes modificaciones: - El tercer punto de la sección 1.2 se modificó a "Las cuentas y servicios de TI se proporcionará únicamente a los empleados indicados como activos por Recursos Humanos". - La redacción se modificó en la sección 1.6 mencionando que esto se aplica "para todos los incidentes de TI". - Se revisó redacción y gramática en toda la política.	Apr06,2021	Coordinador de Seguridad de la Información, Alejandra Sánchez	Coordinador de InfoSec, Alejandra Sánchez	Coordinador de InfoSec, Alejandra Sánchez	Consultor Jurídico Interno, Klaudya Hernández
9	La política fue revisada y actualizada, agregando las siguientes modificaciones: - La política debe ser reforzada con los empleados cada seis meses. - Se renombró la Política de Dispositivos Móviles a Política de Dispositivos Electrónicos en la sección 1.4 punto 4.	May27,2021	Coordinador de Seguridad de la Información, Alejandra Sánchez	Coordinador de InfoSec, Alejandra Sánchez	Coordinador de InfoSec, Alejandra Sánchez	Consultor Jurídico Interno, Klaudya Hernández
10	Se cambio el nombre y modificación de contenido en el punto 1.2 Uso Aceptable	Aug11,2022	Director de TI, Luis Veana	Coordinador de InfoSec, Alejandra Sánchez	Coordinador de InfoSec, Alejandra Sánchez	Asesor Jurídico Interno, Klaudya Hernandez.
11	- Se realizan actualizaciones de los nombres responsables del área. Revisión General de la Política y se añaden los siguientes cambios: - Se refieren formatos de nueva creación que apoyan en salvaguardar la confidencialidad de la información. - Se revisan documentos referidos. - Se modifica la periodicidad de reforzamiento de la política. - Se complementa la sección 4 "Dispositivos electrónicos" con los formatos de control de dispositivos establecidos en PCUGP-002_P Seguimiento a Dispositivos de Almacenamiento y Electrónicos. - "FIT-020_I Tabla Clasificación Información de TI" cambia ID por "DIT-028_I Tabla Clasificación Información de TI"	Aug16,2023	Gerente IT, Irving Lugo	Analista InfoSec, Aranza Sainz / Ingeniero de Procesos, Uriel Romero.	Ingeniero de Procesos, Uriel Romero.	Asesor Jurídico Interno, Klaudya Hernandez.
12	Revisión general del documento: - Actualización de la introducción del documento. - Actualización de la nomenclatura del documento. - Actualización del documento al formato vigente. - Actualización de los nombres de la documentación referida en el documento. - Actualización de la **sección II. "Documentos y registros"**.	Aug09,2024	Director de TI, Luis Veana	Analista InfoSec, Aranza Sainz / Coordinador Cumplimiento y CA, Diana Pulido.	Coordinador Cumplimiento y CA, Diana Pulido.	Asesor Jurídico Interno, Klaudya Hernandez.

V. Autorización

Departamento y Área: Tecnologías de la Información, Ciberseguridad.

Medio de aprobación: Correo electrónico

VI. Control de cambios

Versión	Descripción del Cambio	Vigencia	Solicitante	Creación / Actualización	Control Documental	Autorización
13	Revisión general del documento: - Actualización en la introducción del documento. - Añadida referencia de PCUGP-001_P Control de documentos y registros en Introducción. - Añadida referencia de FIT-051_P Aceptación y Conocimiento del Riesgo, en la sección 3. - Integración de la AIT-030_P Política de redes inalámbricas en sección 2. - Actualizado el nombre del equipo de «Seguridad de la Información (INFOSEC)» a «Ciberseguridad (CS)».□	Oct23,2025	Gerente de TI, Irving Lugo.	Analista Ciberseguridad, Aranza Sainz.	Coordinador de Gestión de Procesos, Illya Garcia.	Director de TI, Luis Veana.