1. Acerca del Documento	
Código:	PL-SGSI-18
Versión:	00
Fecha Inicio:	13/11/2024
Responsable:	Comité de Dirección
Clasificación de Información	Interna

Si usted no es una persona autorizada para conocer el contenido de este documento, desista de su lectura.

En caso de ignorar este aviso estará sujeto a las medidas disciplinarias y legales pertinentes.

2. Control de Aprobaciones		
	Nombre	**Fecha**
Elaboró	CISO	09/08/2023
	AUXILIAR DE SEGURIDAD	09/08/2023
	GERENTE DE CONTINUIDAD	09/08/2023
	DIRECTOR DE CUMPLIMIENTO Y AUDITORIA	09/08/2023
Revisó	DIRECCIÓN DE TI INFRAESTRUCTURA	11/11/2024
Aprobó	COMITÉ DE DIRECCIÓN	13/11/2024

3. Control de Cambios			
Fecha	**Versión**	**Revisión**	**Descripción de la Modificación**
13/11/2024	00	00	Documento de nueva creación

Contenido

4. Objetivo

Establecer un plan de tratamiento de riesgos relacionado con la cláusula 5 Controles Organizacionales en conformidad con los requisitos de la norma ISO/IEC 27001:2022.

5. Alcance

Este proceso aplica para todas las áreas y personal que participan dentro del Sistema de Gestión de Seguridad de la Información de Cibergestión.

6. 5 Controles Organizacionales

Control	5.1 Políticas para la seguridad de la información
Requisito normativo	La política de seguridad de la información y las políticas específicas asociadas deben ser definidas, aprobadas por la dirección, publicadas, comunicadas y reconocidas por el personal pertinente y partes interesadas pertinentes, y revisadas a intervalos planificados y cuando ocurran cambios significativos en la organización
Operación	En cumplimiento con el apartado 5.2 (Política) de la Cláusula 5 (Liderazgo) de la norma, se cuenta con el DN-SGSI-03 Política general del SGSI. También se cuenta con las siguientes políticas para implementar la seguridad de la información en CG: ● PO-SGSI-01 Política de seguridad de la información para proyectos ● PO-SGSI-02 Política de dispositivos móviles ● PO-SGSI-03 Política de Trabajo Remoto ● PO-SGSI-04 Política de control de acceso ● PO-SGSI-05 Política sobre el uso de controles criptográficos ● PO-SGSI-06 Política de pantalla y escritorio limpio ● PR-SGSI-07 Política de segregación y seguridad en la red ● PO-SGSI-08 Política de transferencia de información ● PO-SGSI-09 Política de desarrollo, actualización, mantenimiento y administración de los aplicativos ● PO-SGSI-10 Política de control de acceso físicos ● PO-SGSI-11 Política sobre prevención de pérdida de datos ● PO-SGSI-12 Política de Filtrado Web La comunicación de las políticas se realiza de acuerdo con el PR-SGSI-05 Proceso de capacitación. De acuerdo con lo indicado en el PR-SGSI-01 Proceso de control documental: ● Todos los documentos del Sistema de Gestión de Seguridad de la Información deberán ser revisados por lo menos una vez al año para garantizar su vigencia y aplicación a las necesidades de la organización. En cumplimiento con lo indicado en el apartado 9.3 (Revisión por la dirección) de la cláusula (9 Evaluación del desempeño) de la norma, se cuenta con el PR-SGSI-10 Proceso de revisión por la dirección en la cual se estipulan la revisión de políticas y objetivos del SGSI.
Responsable	CISO - Responsables de procesos

Control	5.2 roles y responsabilidades para seguridad de la información
Requisito normativo	Los roles y responsabilidades de seguridad de la información se deben definir y asignar de acuerdo con las necesidades de la organización.
Operación	La Alta Dirección, aprueba y firma el DN-SGSI-04 Roles y responsabilidades del SGSI. Dentro de cada proceso del SGSI se establecen los roles y responsabilidades para la ejecución de actividades. En los planes de tratamiento del SGSI se indica el responsable de cada control.
Responsable	Comité de Dirección / CISO

Control	5.3 Segregación de tareas
Requisito normativo	Las tareas en conflicto y áreas de responsabilidad se deben segregar.
Operación	Se tiene la LT-SGSI-04 Tabla de segregación de tareas donde se identifican aquellas tareas o actividades que han sido segregadas para evitar acciones no autorizadas.
Responsable	Directores de Área / Proceso Roles y responsabilidaes

Control	5.4 Responsabilidades de Gobierno/Administración
Requisito normativo	La administración debe exigir a todo el personal que aplique la seguridad de la información de acuerdo con la política de seguridad de la información establecida, así como políticas y procedimientos específicos.
Operación	La política del SGSI y las políticas específicas de seguridad de la información son autorizadas y firmadas por los responsables de las áreas correspondientes, así como del comité de dirección. Durante la fase de inducción a los nuevos colaboradores, se les da a conocer el conjunto de políticas de seguridad de la información aplicables. De acuerdo con el proceso de revisión por la dirección, se revisan políticas de seguridad de la información. PR-SGSI-10 Proceso de Revisión por la Direccion PO-SGSI-01 Politica de Seguridad de la Información
Responsable	Recursos humanos - (CISO)

Control	5.5 Contacto con autoridades
Requisito normativo	La organización debe establecer y mantener contacto con las autoridades pertinentes.
Operación	Se cuenta con un LT-SGSI-05 Directorio de contactos con autoridades, que incluye: ● Dependencia/Autoridad ● Número de contacto ● Dirección Esta información, además de encontrarse disponible en el repositorio de documentos del SGSI, se encuentra disponible en la recepción para consulta de todos los colaboradores en un caso de emergencia.
Responsable	Dirección Jurídica Dirección de RH Dirección de Finanzas
Control	5.6 Contacto con grupos especiales de interés

Requisito normativo	La organización debe establecer y mantener contacto con grupos de interés especial u otros foros especializados en seguridad y asociaciones profesionales.
Operación	Se cuenta con un LT-SGSI-06 Directorio de grupos de especial interés, que incluye: ● Empresa/Asociación/Dependencia/Autoridad ● Sitio de contacto o consulta Esta información se encuentra disponible en el repositorio de documentos del SGSI para consulta de todos los colaboradores en un caso de emergencia.
Responsable	CISO - Dirección Jurídica

Control	5.7 Inteligencia de amenazas
Requisito normativo	La información relacionada con las amenazas a la seguridad de la información debe recopilarse y analizarse para producir inteligencia sobre amenazas.
Operación	El documento PR-SGSI-15 PROCESO DE GESTIÓN DE VULNERABILIDADES detalla las acciones para la atención de distintas vulnerabilidades, las cuales comienzan con estar al tanto de diferentes fuentes de información y contar con alertamientos internos y externos sobre las diferentes amenazas existentes, para planificar su atención y remediación
Responsable	CISO - Infraestructura - Desarrollo

Control	5.8 Seguridad de la información en la gestión de proyectos
Requisito normativo	La seguridad de la información debe integrarse en la gestión de proyectos.
Operación	Se cuenta con una PO-SGSI-01 Política de seguridad de la información para proyectos que establece, entre otros, lineamientos respecto: Evaluación de riesgos relacionados con seguridad de la información. Considerar mecanismos de control para proteger la disponibilidad, integridad y confidencialidad en la administración de proyectos. Gestión de cambios. Se cuenta con la PO-SGSI-09 Política de Desarrollo, Actualización, Mantenimiento y Administración de los Aplicativos donde se establecen los apartados: ● **De desarrollo seguro** marca los requerimientos de análisis y requisitos de seguridad para el desarrollo de software (entorno, aplicación e información) ● **Principios de ingeniería para la seguridad de la información** apoya las especificaciones de requisitos de seguridad a nivel de aplicación e infraestructura. ● **De los Controles de Seguridad en la Arquitectura del Aplicativo** define lineamientos que soportan la seguridad en la arquitectura de las aplicaciones, así como la capacidad de escalamiento. También define las características de seguridad de la información en reposo (contraseñas: algoritmo criptográfico de hash SHA-256) así como la de tránsito (protocolos criptográficos TLS y SSL). ● **Del Monitoreo de Desempeño y Seguridad de Servidores y el aplicativo** monitorea y registra la actividad en el servidor y los aplicativos.
Responsable	Dirección de Desarrollo - Gerencia de Desarrollo - CISO

Control	5.9 Inventario de información y otros activos asociados
Requisito normativo	Se debe desarrollar y mantener un inventario de información y otros activos asociados, incluidos los propietarios.
Operación	Se cuenta con el archivo FO-SGSI-01 VALORACIÓN Y TRATAMIENTO DE RIESGOS, en cuya pestaña *Valoración de activos* se cuenta con un inventario de activos de información y sus activos asociados. Se cuenta con PR-SGSI-22 Proceso de inventario de hardware y software Se cuenta con LT-SGSI-10 Inventario de hardware y software_AAAAMMDD, donde se registra la información técnica de los equipos y periféricos de la organización.
Responsable	Gerencia de infraestructura - CISO

Control	5.10 Uso aceptable de la información y otros activos asociados
Requisito normativo	Deben identificarse, documentarse y aplicarse normas para el uso aceptable y procedimientos para el manejo de la información y otros activos asociados.
Operación	Se cuenta con diversas políticas para el manejo y cuidado de los activos como equipo de cómputo, laptops, equipo móvil, redes, sistemas, aplicaciones, información física o electrónica y uso adecuado de las instalaciones. Las políticas son: ● PO-SGSI-02 Política de dispositivos móviles. ● PO-SGSI-03 Política de Trabajo Remoto. ● PO-SGSI-08 Política de transferencia de información. ● Se cuenta con responsivas firmadas por los colaboradores (FO-SGSI-02 Carta responsiva de equipo), dónde se dan por enterados de la verificación de los equipos para revisar el cumplimiento de estas políticas. De acuerdo con la política de clasificación de la información que se encuentra en el MN-SGSI-02 Manual de documentos, todos los procedimientos, manuales y formatos del SGSI cuentan con una sección donde se etiqueta la información. Adicionalmente la organización cuenta con procedimientos y políticas para: ● PR-SGSI-17 Proceso de altas bajas y cambios TI infraestructura donde se indican actividades para devolución de activos y retiro de accesos. ● PO-SGSI-05 Política sobre el Uso de Controles Criptográficos.
Responsable	Gerencia de Infraestructura - CISO

Control	5.11 Devolución de activos
Requisito normativo	El personal y otras partes interesadas, según corresponda, deben devolver todos los activos de la organización en su posesión al cambiar o terminar su empleo, contrato o acuerdo.
Operación	En el PR-SGSI-07 Proceso de baja de personal, se establece una actividad para la devolución de activos. Se cuenta con el PR-SGSI-17 Proceso de altas bajas y cambios TI infraestructura, mediante el cual se indica la devolución de equipo asignado. En la PO-SGSI-03 Política de Trabajo Remoto también se estipula la devolución de equipos. Se cuenta con responsivas firmadas por los colaboradores (FO-SGSI-02 Carta responsiva de equipo), dónde se dan por enterados de la verificación de los equipos para revisar el cumplimiento de estas políticas.
Responsable	Infraestructura - Gerencias de Recursos Humanos - CISO

Control	5.12 Clasificación de la información
Requisito normativo	La información debe clasificarse de acuerdo con las necesidades de seguridad de la información de la organización en función de la confidencialidad, integridad, disponibilidad y los requisitos pertinentes de las partes interesadas.
Operación	El MN-SGSI-02 Manual de documentos contiene una política para la clasificación de información.
Responsable	Comité de Dirección - CISO

Control	5.13 Etiquetado de la información
Requisito normativo	Debería elaborarse y aplicarse un conjunto apropiado de procedimientos para el etiquetado de la información de conformidad con el sistema de clasificación de la información adoptado por la organización.
Operación	De acuerdo con el MN-SGSI-02 Manual de documentos, todos los procedimientos, manuales y formatos del SGSI cuentan con una sección donde se etiqueta la información. ● Información Pública ● Información Interna ● Información Confidencial
Responsable	Comité de Dirección - CISO

Control	5.14 Transferencia de información
Requisito normativo	Las reglas, procedimientos o acuerdos de transferencia de información deben existir para todos los tipos de instalaciones de transferencia dentro de la organización y entre la organización y otras partes.
Operación	Se cuenta con la PO-SGSI-08 Política de transferencia de información donde se establecen lineamientos sobre: ● Transferencia de información a proveedores o clientes. ● Transferencia de información digital o electrónica. ● Transferencia de información física. Se cuenta con el MN-SGSI-02 MANUAL DE DOCUMENTOS donde se clasifica la información. Se cuenta con el PR-SGSI-16 PROCESO DE PROVEEDORES DE TI INFRAESTRUCTURA donde se establece la existencia del Contrato de confidencialidad. Se cuenta con políticas y procesos donde se establece la existencia de la confidencialidad de la información de los clientes. ● PO-SGSI-01 Política de seguridad de la información para proyectos ● PO-SGSI-03 Política de Trabajo Remoto
Responsable	Comité de Dirección - CISO - Dirección de cumplimiento y auditoría

Control	5.15 Control de acceso
Requisito normativo	Las reglas para controlar el acceso físico y lógico a la información y otros activos asociados deben establecerse e implementarse en función de los requisitos comerciales y de seguridad de la información.
Operación	Se cuenta con una PO-SGSI-04 Política de control de acceso, en la cual se establecen lineamientos para derechos de acceso y gestión de contraseñas en: acceso a red, control

	de acceso de sistemas y aplicaciones generales, directorio activo, google suite, aplicativos y/o cuentas administrativas.
Responsable	Infraestructura - CISO -Desarrollo (plataforma)

Control	5.16 Gestión de identidades
Requisito normativo	Se debe gestionar el ciclo de vida completo de las identidades.
Operación	Para proporcionar el acceso a usuarios se cuenta con un PR-SGSI-19 Proceso de gestión de privilegios de accesos TI donde se indican actividades y lineamientos para: •Procedimiento para la Solicitud, Aprobación, Asignación, Monitoreo y Revocación de CUENTAS DE ADMINISTRADOR •Procedimiento para la Solicitud, Aprobación, Renovación, Asignación, Monitoreo y Revocación de Cuentas con Accesos Privilegiados •Resguardo de Cuentas de Administrador Se cuenta con un PR-SGSI-08 Proceso de Accesos al Aplicativo que índica los lineamientos a seguir para el ABC de usuarios en el aplicativo.
Responsable	Desarrollo - Infraestructura - CISO

Control	5.17 Información de autenticación
Requisito normativo	La asignación y gestión de la información de autenticación debe controlarse mediante un proceso de gestión, incluido el asesoramiento al personal sobre el manejo adecuado de la información de autenticación.
Operación	Para proporcionar el acceso a usuarios se cuenta con un **PR-SGSI-08** Proceso de accesos a aplicativo, PR-SGSI-19 Proceso de gestión de privilegios de accesos TI y PR-SGSI-17 Proceso de altas bajas y cambios TI infraestructura donde se indican actividades y lineamientos para: ● Proporcionar la información secreta de autenticación. ● La configuración de políticas técnicas de acceso a los sistemas Se cuenta con una política PO-SGSI-09 Política de Desarrollo, Actualización, Mantenimiento y Administración de los Aplicativos con apartado: ● Del Control de Acceso Lógico: que indica que las contraseñas de acceso al aplicativo se resguardarán “cifradas" utilizando algoritmo SHA256. Se cuenta con una PO-SGSI-04 Política de control de acceso, en la cual se establecen lineamientos respecto a la responsabilidad de cada usuario para responsabilizarse del resguardo de sus credenciales (usuarios y contraseña) de identidad electrónica y por lo tanto son personales e intransferibles.
Responsable	Desarrollo - Infraestructura - CISO

Control	5.18 Derechos de acceso
Requisito normativo	Los derechos de acceso a la información y otros activos asociados deben aprovisionarse, revisarse, modificarse y eliminarse de acuerdo con la política y las reglas específicas del tema de la organización sobre el control de acceso.
Operación	Para proporcionar el acceso a usuarios se cuenta con un PR-SGSI-19 Proceso de gestión de privilegios de accesos TI donde se incluyen los siguientes procedimientos: •Procedimiento para la Solicitud, Aprobación, Asignación, Monitoreo y Revocación de CUENTAS DE ADMINISTRADOR

	•Procedimiento para la Solicitud, Aprobación, Renovación, Asignación, Monitoreo y Revocación de Cuentas con Accesos Privilegiados •Resguardo de Cuentas de Administrador Para la provisión, modificación y cancelación de los accesos se debe solicitar el requerimiento al área correspondiente a través de correo electrónico tanto al Director de Infraestructura y CISO. Se cuenta con un PR-SGSI-08 Proceso de Accesos al Aplicativo que índica los lineamientos a seguir para el ABC de usuarios en el aplicativo Para la gestión acceso a usuarios se cuenta con un PR-SGSI-17 Proceso de altas bajas y cambios TI infraestructura, donde se indican actividades y lineamientos a seguir donde: •El área de Recursos Humanos o Director de Proyecto o Gerente de Proyecto debe notificar por medio de ticket a JIRA el aviso de baja inmediata o la fecha y hora programada de baja, copiando en el correo al Gerente de Continuidad y CISO.
Responsable	Desarrollo - Infraestructura - CISO

Control	5.19 Seguridad de la información en las relaciones con los proveedores
Requisito normativo	Se deben definir e implementar procesos y procedimientos para gestionar los riesgos de seguridad de la información asociados con el uso de los productos o servicios del proveedor.
Operación	Se cuenta con un PR-SGSI-16 Proceso de gestión de proveedores de TI infraestructura, donde en el apartado de políticas se especifican los lineamientos a seguir con los proveedores.
Responsable	Direcciones Jurídica - Infraestructura - CISO

Control	5.20 Abordar la seguridad de la información dentro de los acuerdos con proveedores
Requisito normativo	Los requisitos relevantes de seguridad de la información deben establecerse y acordarse con cada proveedor en función del tipo de relación con el proveedor.
Operación	Se firman contratos de prestación de servicios y se establecen acuerdos de confidencialidad con los proveedores. La organización cuenta con un PR-SGSI-16 Proceso de gestión de proveedores de TI infraestructura.
Responsable	Direcciones Jurídica - Infraestructura - CISO

Control	5.21 Gestión de la seguridad de la información en la cadena de suministro de las TIC
Requisito normativo	Deben definirse e implementar procesos y procedimientos para gestionar los riesgos de seguridad de la información asociados con la cadena de suministro de productos y servicios de TIC.
Operación	Se cuenta con un PR-SGSI-16 Proceso de gestión de proveedores de TI infraestructura y con un LT-SGSI-11 Inventario de proveedores críticos TI infraestructura donde se indican los datos de contacto del proveedor.
Responsable	Gerente de infraestructura - CISO

Control	5.22 Supervisión, revisión y gestión del cambio de los servicios de los proveedores
Requisito normativo	La organización debe monitorear, revisar, evaluar y gestionar regularmente el cambio en las prácticas de seguridad de la información del proveedor y la prestación de servicios.
Operación	Se cuenta con el formato DX-26 Checklist Proveedores Externos TI Cibergestión y siguiendo lo establecido en el PR-SGSI-16 Proceso de gestión de proveedores de TI infraestructura. Los cambios en la provisión de servicios por parte de proveedores, incluyendo el mantenimiento y la mejora de las políticas de seguridad de la información existentes, procedimientos y controles, deben ser administrados, tomando en cuenta el PR-SGSI-12 Proceso de gestión de cambios de infraestructura.
Responsable	Dirección Jurídica - Gerente de Infraestructura - CISO

Control	5.23 Seguridad de la información para el uso de servicios en la nube
Requisito normativo	La organización debe monitorear, revisar, evaluar y gestionar regularmente el cambio en las prácticas de seguridad de la información del proveedor y la prestación de servicios.
Operación	Se cuenta con el PR-SGSI-30 Proceso de gestión de cambios infraestructura,y se tiene formato DX-26 Checklist Proveedores Externos TI Cibergestión y siguiendo lo establecido en el PR-SGSI-16 Proceso de gestión de proveedores de TI infraestructura. Ademas se tiene el PR-SGSI-27 Proceso de Seguridad de la Información para el uso de Servicios en la Nube
Responsable	Dirección de Infraestructura - CISO

Control	5.24 Planificación y preparación de la gestión de incidentes de seguridad de la información
Requisito normativo	La organización debe planificar y prepararse para la gestión de incidentes de seguridad de la información mediante la definición, el establecimiento y la comunicación de procesos, roles y responsabilidades de gestión de incidentes de seguridad de la información.
Operación	Se cuenta con el PR-SGSI-23 Proceso de gestión de incidentes, el cual establece las actividades para la gestión de incidentes de seguridad de la información, cada actividad cuenta con uno o varios responsables y se hace referencia al uso delL. Se cuenta con un DXI-08 RISI Reporte de Incidentes de Seguridad de la Información Se cuenta con un DX-33 Proceso de Recolección de Información y Cadena de Custodia en Incidentes
Responsable	CISO

Control	5.25 Evaluación y decisión sobre eventos de seguridad de la información
Requisito normativo	La organización debe evaluar los eventos de seguridad de la información y decidir si deben clasificarse como incidentes de seguridad de la información.
Operación	Se cuenta con el PR-SGSI-23 Proceso de gestión de incidentes, el cual establece las actividades para la gestión de incidentes de seguridad de la información, cada actividad cuenta con uno o varios responsables y se hace referencia al uso del DX-06 REP_VUL.
Responsable	CISO

Control	5.26 Respuesta a incidentes de seguridad de la información
Requisito normativo	Los incidentes de seguridad de la información deben responderse de acuerdo con los procedimientos documentados.
Operación	Se cuenta con el PR-SGSI-23 Proceso de gestión de incidentes, el cual establece las actividades para la gestión de incidentes de seguridad de la información, cada actividad cuenta con uno o varios responsables y se hace referencia al uso del DX-06 REP_VUL.
Responsable	CISO

Control	5.27 Aprender de los incidentes de seguridad de la información
Requisito normativo	El conocimiento obtenido de los incidentes de seguridad de la información debe utilizarse para fortalecer y mejorar los controles de seguridad de la información.
Operación	Se cuenta con el PR-SGSI-23 Proceso de gestión de incidentes, el cual establece las actividades para la gestión de incidentes de seguridad de la información, cada actividad cuenta con uno o varios responsables y se hace referencia al uso del DX-06 REP_VUL.
Responsable	CISO

Control	5.28 Obtención de pruebas
Requisito normativo	La organización debe establecer e implementar procedimientos para la identificación, recopilación, adquisición y preservación de evidencia relacionada con eventos de seguridad de la información.
Operación	Se cuenta con el PR-SGSI-23 Proceso de gestión de incidentes, el cual establece las actividades para la gestión de incidentes de seguridad de la información, cada actividad cuenta con uno o varios responsables y se hace referencia al uso del DX-06 REP_VUL.
Responsable	CISO

Control	5.29 Seguridad de la información durante la interrupción
Requisito normativo	La organización debe planificar cómo mantener la seguridad de la información en un nivel apropiado durante la interrupción.
Operación	Se cuenta con el FO-SGSI-07 ANÁLISIS DE IMPACTO AL NEGOCIO (BIA), PL-SGSI-15 Plan de Recuperación de Desastres DRP y PL-SGSI-16 Plan de continuidad del negocio BCP donde se incluyen requisitos de seguridad de la información al implementar cualquier acción de contingencia. La organización debe verificar los controles de la continuidad de la seguridad de la información establecidos y aplicados a intervalos regulares con el fin de asegurarse de que son válidos y eficaces en situaciones adversas.
Responsable	Infraestructura

Control	5.30 Preparación de las TIC para la continuidad de las actividades
Requisito normativo	La preparación para las TIC debe planificarse, aplicarse, mantenerse y probarse sobre la base de los objetivos de continuidad de las actividades y los requisitos de continuidad de las TIC.
Operación	Se cuenta con el BCP y DRP
Responsable	Infraestructura

Control	5.31 Requisitos legales, estatutarios, reglamentarios y contractuales
Requisito normativo	Los requisitos legales, estatutarios, reglamentarios y contractuales relevantes para la seguridad de la información y el enfoque de la organización para cumplir con estos requisitos deben identificarse, documentarse y mantenerse actualizados.
Operación	Se cuenta con el apoyo de un departamento jurídico encargado de revisar: ● Requisito a cumplir. ● Ley o regulación asociada. ● Descripción de la ley o regulación. ● Áreas y responsables involucrados. ● Comentarios de la última revisión de la ley o regulación vigente. También se cuenta con un Marco Normativo Aplicable disponible en el DN-SGSI-01 Contexto de la organización y partes interesadas. La organización se ajusta a la regulación vigente aplicable a sus clientes con respecto a la contratación con terceros de servicios para la realización de procesos operativos estipulada en las Disposiciones de Carácter General aplicables a las Instituciones de Crédito. La organización cuenta con la PO-SGSI-05 Política sobre el uso de controles criptográficos, donde se describe los siguientes apartados: ● Uso de controles criptográficos, que indica las características de configuración que se deberán implementar. ● Gestión de claves criptográficas internas, que indica el tratamiento que se les dará a las claves.
Responsable	Jurídico - Cumplimiento y auditoría - CISO

Control	5.32 Derechos de propiedad intelectual
Requisito normativo	La organización debería aplicar procedimientos adecuados para proteger los derechos de propiedad intelectual.
Operación	El software desarrollado por OPERADORA CIBERGESTION S.A. DE C.V. (PRESTO) es registrado ante el Registro Público de Derecho de Autor con número de obra <<03-2014-021414082600-01>>, en la rama de programa de computación, así como en el Instituto Mexicano de la Propiedad Industrial (IMPI) con el número de registro IMPI <<1521470>>. Toda la información del diseño y desarrollo se registra como “Confidencial”. En el contrato individual de trabajo del personal se incluyen cláusulas relacionadas a la propiedad intelectual y de los desarrollos de sistemas.
Responsable	Jurídico

Control	5.33 Protección de registros
Requisito normativo	Los registros deben protegerse contra pérdida, destrucción, falsificación, acceso no autorizado y divulgación no autorizada.
Operación	Se establecen mecanismos de seguridad a los registros los cuales se indican en el PR-SGSI-02 Proceso de registros y en la LT-SGSI-02 Lista maestra de registros. Se cuenta con la disponibilidad que nos entrega la suite de Office 365 para la recuperación de información. Además, se cuenta con una póliza contra riesgos cibernéticos contratada por Operadora Cibergestión y que ampara contra este tipo de riesgos.
Responsable	Jurídico - Cumplimiento y auditoría - CISO - Responsable de cada proceso

Control	5.34 Privacidad y protección de la PII
Requisito normativo	La organización debe identificar y cumplir con los requisitos relacionados con la preservación de la privacidad y la protección de la PII de acuerdo con las leyes y regulaciones aplicables y los requisitos contractuales.
Operación	La organización implementa mecanismos para cumplir con la Ley Federal de Protección de Datos Personales en Posesión de los Particulares a través de su aviso de privacidad. Se cuenta con el documento D**X 34 Política y Procedimiento Sobre la Ley de Proteccion de Datos Personales en Posesion de Los Particulares y su Reglamento**
Responsable	Cumplimiento y auditoría- Jurídico -CISO

Control	5.35 Revisión independiente de la seguridad de la información
Requisito normativo	El enfoque de la organización para gestionar la seguridad de la información y su implementación, incluidas las personas, los procesos y las tecnologías, debe revisarse de forma independiente a intervalos planificados o cuando se produzcan cambios significativos..
Operación	Operadora Cibergestión S.A. de C.V. se somete a auditorias de seguridad anuales por los siguientes proveedores o clientes: ● NYCE En cada auditoría se entrega un informe de resultados por parte del cliente o proveedor.
Responsable	Comité de Dirección - Cumplimiento y auditoría - CISO

Control	5.36 Cumplimiento de políticas, reglas y estándares para la seguridad de la información
Requisito normativo	El cumplimiento de la política de seguridad de la información de la organización, las políticas, reglas y estándares específicos del tema deben revisarse regularmente.
Operación	Se cuenta con el FO-SGSI-13 Informe de revisión por la dirección, donde se registran los resultados de las auditorías que validan el cumplimiento del procesamiento de información de acuerdo con las políticas, normas o cualquier otro requisito de seguridad apropiado. La organización cuenta con un PR-SGSI-15 Proceso de Gestión de Vulnerabilidades donde estipula lo siguiente: ● La Infraestructura deberá ser analizada al menos una vez al año como procedimiento interno de la Dirección de TI. ● Solo cuando se actualicen y/o modifiquen los componentes centrales de la infraestructura deberá programar un nuevo análisis. ● El análisis de Vulnerabilidades de infraestructura será ejecutado por un tercero, cumpliendo con la metodología y entrega previamente acordada con la Dirección de TI de Infraestructura. ● Los Aplicativos deberán ser analizados al menos una vez al año como procedimiento interno de la Dirección de TI por el CISO. ● Solo cuando se actualicen y/o modifiquen los componentes centrales de la arquitectura del aplicativo deberán de ser analizados por un tercero. Así también de manera continua es revisada la operación por nuestros clientes
Responsable	Comité de Dirección - Cumplimiento y auditoría - CISO

Control	5.37 Procedimientos operativos documentados
Requisito normativo	Los procedimientos operativos de las instalaciones de procesamiento de información deben documentarse y ponerse a disposición del personal que los necesite. Los procedimientos operativos de las instalaciones de procesamiento de información deben documentarse y ponerse a disposición del personal que los necesite.
Operación	Los documentos del SGSI, ya sean operativos o externos, necesarios para proteger, tratar o procesar la información son referenciados en la LT-SGSI-01 Lista maestra de documentos.
Responsable	CISO