Contenido

1. OBJETIVO

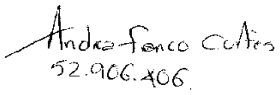
Establecer las directrices de la organización para garantizar los principios fundamentales de la información (disponibilidad, integridad y confidencialidad) para el buen uso y privacidad de los datos, alineados con la dirección estratégica organizacional, contemplando: políticas, procedimientos, controles, mejores prácticas, tomando como referente, requisitos legales, técnicos de la norma ISO/IEC 27001-2013, ISO/IEC 27002-2013 y MINTIC, INCIBE.

Como objetivo específico de la política se define:

- Identificar, establecer e implementar actividades de control para minimizar el riesgo de los procesos y áreas críticas, mediante una adecuada gestión de estos, garantizando la continuidad del negocio.

2. ALCANCE

El manual de Seguridad de la Información y Ciberseguridad aplica a toda la organización y a sus agentes relacionados. Es responsabilidad de cada parte cumplirla teniendo en cuenta los principios, controles y procedimientos.

Preparado por:	Revisado por:	Aprobado por:
Andrea Franco Cortés  Jefe de TIC Fecha: Marzo/2024	Erika Triana  Directora Administrativa y Financiera Fecha: Marzo/2024	Erika Triana  Directora Administrativa y Financiera Fecha: Marzo/2024
	Verifique que esta copia es la vigente, consultando el listado maestro de documentos o a través del código QR. El acceso al documento a través del código, le confirmará que está vigente. Si el enlace no está disponible indica que no es la versión vigente.	

3. DOCUMENTOS DE REFERENCIA

- ISO/IEC 27001-2013: Técnicas de seguridad. Sistema de gestión de la seguridad de la información
- ISO/IEC 27002-2013: Técnicas de seguridad. Código de practica para controles de seguridad de la información.
- MINTIC: Guía – Seguridad de la información MiPymes.
- INCIBE: Instituto Nacional de Ciberseguridad.
- Política de Seguridad de la Información y Ciberseguridad, DG-TI-02.
- Política general de tratamiento de datos, DG-DE-06.
- Alistamiento de equipos de cómputo, I-TI-01.
- Plan de gestión integral de residuos sólidos y peligrosos, DG-GI-33.
- Borrado seguro de la información, I-TI-03.
- Gestión del cambio, P-GI-06.
- Reglamento Interno de Trabajo de la organización.
- Código de ética y conducta, DG-GE-03.

4. POLÍTICAS DE SEGURIDAD ESPECÍFICAS

4.1 Evaluación y capacidad del riesgo de Seguridad de la Información

La organización deberá contar con un proceso para identificar, evaluar, documentar, gestionar y mitigar los riesgos de Seguridad de la Información; dicho proceso se hará por lo menos una vez al año o cuando ocurra algún evento especial, en donde se identificarán riesgos y se evaluará su probabilidad.

La Alta Dirección y el responsable TIC deberán alinearse con la gestión de riesgos de Seguridad de la Información, para identificar el nivel de tolerancia y la capacidad máxima de aceptación del riesgo, considerando el efecto de la naturaleza de sus operaciones y líneas de negocio.

4.2 Confidencialidad, integridad, disponibilidad y privacidad de la información

Todos los colaboradores de la organización deben garantizar y asegurar, la confidencialidad, integridad, disponibilidad y privacidad de la información, de tal manera que:

- Solo sea accedida por el personal autorizado.
- Este disponible en el momento que sea requerida.
- Sea accedida legítimamente y utilizada para lo que se autorizó, de acuerdo con la función del solicitante.
- La información no publicable a terceros, alojada en el sistema informático de la

organización (SharePoint, Intranet, OneDrive y demás herramientas) a excepción del contenido público de la página web debe ser tratada de manera que se garantice su confidencialidad.

- Joyco y sus consorcios protegerán la privacidad y confidencialidad del tratamiento y protección de datos personales de sus clientes, colaboradores y demás agentes relacionados, que recopile en sus bases de datos de información, conforme a la ley 1581 de 2012 y de acuerdo con lo establecido en la *Política general de tratamiento de datos, DG-DE-06*. Esta política es apoyada por los acuerdos de confidencialidad de la información que se firma con los proveedores e internamente con colaboradores de la organización.
- No se permite el envío de información que sea considerada confidencial o reservada a terceros, ni entre usuarios de la misma organización de diferentes procesos; en caso de ser requerido, se deberá solicitar por medio de mesa de ayuda junto con la autorización del jefe directo para así llevar a cabo la gestión.

4.3 Almacenamiento de la información corporativa

Joyco, ha dispuesto la plataforma Office 365 como sitio en común de trabajo, donde almacenar el resultado de trabajos individuales y colaborativo para compartir información entre los diferentes usuarios de la organización. La información será distinguida entre información general que puede ser utilizada por todos los usuarios, se prestará una atención especial cuando esta sea confidencial, critica o si está sujeta a algún requisito legal.

- Es responsabilidad de los directores, jefes y coordinadores de proyectos y procesos; informar la distinción o clasificación de la información.
- Es responsabilidad de los colaboradores almacenar la información en las herramientas corporativas en la nube (SharePoint y Teams para trabajo en equipo y One Drive para trabajo individual) y otras herramientas contratadas por la organización y dispuestas para tal fin.
- En los casos de sincronización de las herramientas como One Drive y SharePoint en los equipos corporativos, **es responsabilidad del usuario el monitoreo continuo del correcto funcionamiento del agente para garantizar que efectivamente la información esta sincronizada en la nube.**
- No está permitido la **visualización y sincronización de las herramientas corporativas** (Office 365 y otras que la organización disponga para el trabajo) en los computadores personales de los usuarios.
- No es permitido alojar o cargar información en plataformas, herramientas de terceros o que no se han contratadas por la organización para tal fin.
- Los dispositivos de almacenamiento extraíble (memorias USB, discos duros, tarjetas de memoria, CD); debido a la susceptibilidad al robo, manipulación, extravío e infección por virus no están permitidos en la organización. De requerir una excepción con una justa causa, se debe diligenciar el *Declaración*

de indemnidad, F-TI-11.

- Es responsabilidad de los jefes y directores de procesos o proyectos, verificar al retiro de un colaborador o contratista de la organización, que el trabajo realizado se encuentre almacenado en la nube. Para ello el usuario que se retira debe diligenciar el *Reporte de devolución de equipo de cómputo y dispositivos de tecnología*, *F-TI-12,* el cual debe contar **con el visto bueno de su jefe inmediato.**

4.4 Preservación de la información digital

Se establecen los siguientes lineamientos, con el objetivo de asegurar el acceso a la información histórica, garantizando las características básicas de la información:

- Cada proyecto y/o proceso que inicie debe contar y asumir un presupuesto para:

  - almacenamiento de la información vigente (Share Point);
  - licenciamiento para respaldo de la información vigente;
  - licenciamiento para aprovisionar información histórica para su preservación a largo plazo.

- Cada proyecto y/o proceso debe mantener organizada y depurada la información con el fin de evitar duplicidad y optimizar el almacenamiento requerido.
- Al finalizar un proyecto (público o privado) aún sin ser liquidado, se mantendrá activo en la plataforma office 365, durante tres meses, a partir de ese tiempo se migrará al repositorio histórico, con el fin de optimizar los recursos de almacenamiento. Una vez se encuentre la información en repositorio histórico y si se requiere acceso para consulta se debe solicitar por mesa de ayuda.

4.5 Controlar y mitigar

Joyco y sus consorcios, cuentan con controles generales de accesos, privilegios y actualizaciones en los siguientes aspectos mínimos:

4.5.1 Control de acceso físico: (oficinas e instalaciones físicas)

- Para el acceso de la oficina Elemento, se deberá enviar un correo electrónico al jefe de Infraestructura con los datos de las personas a autorizar el ingreso (nombre completo, número de identificación, proyecto y cargo). Para el caso de un usuario frecuente, se deberá gestionar la asignación de tarjeta de acceso y registro en el dispositivo biométrico para tal fin.
- Para usuarios frecuentes en oficina Elemento, el jefe de Infraestructura

registra el usuario en la herramienta de control de acceso (biométrico u otro) para así asignar o denegar el acceso a la oficina.
- Los responsables del proceso de TIC serán los encargados de agendar y organizar al personal de mantenimiento preventivo y correctivo de los equipos de cómputo y dispositivos activos.
- El personal del proceso TIC es el único autorizado para mover, cambiar o extraer equipos del centro de cómputo de la oficina Elemento u otras oficinas de la organización.
- No está permitido el ingreso y consumo de alimentos o bebidas en el centro de cómputo de la oficina Elemento u otras oficinas donde aplique.
- Por ningún motivo se almacenarán equipos o elementos que no tengan una función de telecomunicaciones o administración de servicios en el centro de cómputo en la oficina Elemento u otras oficinas donde aplique.

4.5.2 Control de acceso Lógico

Joyco y sus consorcios, garantizarán la seguridad en el intercambio de información, por medio de los únicos medios autorizados para enviar y recibir mensajes los cuales corresponden al correo corporativo y mensajería instantánea (Teams), se prohíbe el uso de correos personales, plataformas gratuitas para envió de información corporativa y creación de correos alternos, utilizando el nombre de la compañía o del contrato para el cual se encuentra laborando.

El responsable del proceso de TIC será encargado de asignar los recursos informáticos corporativos y brindar la capacitación para el correcto uso de estos, establecer mecanismos de autenticación, revisión de permisos, revocación de permisos y eliminación de cuentas.

Es responsabilidad de los jefes y directores de procesos o proyectos:

- Solicitar los recursos tecnológicos requeridos al ingreso de un colaborador, especificando a que sitios debe tener accesos y su nivel de permiso (lectura o edición) por medio de la *Requisición, F-CC-03,* con una antelación mínima de diez días hábiles.
- Reportar por mesa de ayuda, cuando un usuario cambie de proyecto o proceso dentro de la organización, para realizar el cambio respectivo de los accesos a los diferentes sitios y centros de costos.
- Reportar inmediatamente al proceso de TIC, por medio de mesa de ayuda, la fecha de retiro de un colaborador, con el fin de denegar los accesos correspondientes.

Es deber de los usuarios:

- Mantener el puesto de trabajo siempre limpio y ordenado, se prohíbe el consumo de bebidas y alimentos en este.
- Utilizar las cuentas de usuario y recursos de cómputo, para ingreso a los sistemas informáticos y exclusivamente para actividades corporativas y laborales, ya que estas son propiedad de Joyco y sus consorcios.
- No compartir las cuentas de acceso a los sistemas y recursos de las tecnologías de información, ya que son para uso exclusivo de único usuario e intransferibles.
- No suministrar el número ID de la herramienta de acceso remoto (Anydesk) a personal diferente del proceso TIC.
- Las solicitudes de soporte técnico se deben registrar en el canal dispuesto para ello: https://joyco.net.co/
- Notificar al proceso de TIC sospecha de incidente, infección por virus u otro software malicioso, en caso de robo, daño o perdida del equipo o dispositivo.

4.5.3 Uso del correo electrónico

- Usar una contraseña robusta.
- Utilizar doble factor de autenticación.
- Nunca usar el correo corporativo con fines personales.
- Revisar los correos antes de abrirlos (autenticidad): identificar remitentes, analizar los adjuntos (si sospecha: no se descargan ni se abren), inspeccionar enlaces antes de acceder a ellos.
- Se prohíbe él envió de mensajes no deseados o considerados como SPAM.
- Se prohíbe él envió de correos masivos sin autorización oficial.
- Se prohíbe él envió o intercambio de mensajes con contenido que atente contra la integridad de las personas o instituciones, tales como: contenido ofensivo, obscenos, pornográfico, terrorista, discriminación sobre la raza, genero, nacionalidad, edad, orientación sexual, religión, cualquier contenido que represente un riesgo para la seguridad de la información de la organización o la legislación colombiana.
- Crear, enviar, alterar, borrar mensajes suplantando identidad de un usuario.
- Abrir, usar o revisar indebidamente la cuenta de correo de otro usuario, sin contar con la autorización del titular. Cuando aplique temas de investigación o revisiones debe contar con aprobación de su superior.

4.5.4 Contraseñas

El tratamiento diario de la información de la organización requiere el acceso a distintos servicios, dispositivos y aplicaciones para los cuales utilizamos, usuario y contraseña, por la seguridad de los servicios y sistemas, se debe garantizar que las credenciales de autenticación se generan, actualizan y revocan de forma óptima y segura.

La contraseña para ingresar a Office 365, debe cumplir con:

- Una longitud mínima de 8 caracteres.
- Su configuración debe constar de la combinación de letras mayúsculas, minúsculas, números y caracteres especiales.
- Debe tener una duración de sesenta (60) días.
- Debe tener implementado el MFA (Autenticación Multi Factor).
- No se debe incluir el nombre de usuario o datos asociados al correo asignado.
- No se deben utilizar contraseñas por defectos de los aplicativos.
- No compartir contraseñas con nadie.
- No utilizar la misma contraseña para servicios diferentes.
- Cambiar contraseñas periódicamente.
- No permitir recordar en los navegadores y aplicaciones.

4.5.5 Control de uso de Software

- Joyco y sus consorcios, cumple con los derechos de uso de software instalados en los computadores corporativos.
- No se permite software con versiones educativas o para desarrollar trabajos educativos en el entorno laboral.
- El software licenciado o adquirido por la organización, no debe proporcionarse a personas u organizaciones externas o usarse con fines de lucro.
- Cualquier solicitud para instalación de software en equipos de cómputo, debe ser solicitada en la mesa de ayuda; el responsable del caso deberá estudiar dicha solicitud y verificar si cuenta con aprobación o rechazo.
- En ninguna circunstancia el usuario está autorizado para instalar software en el equipo corporativo asignado.
- Ningún funcionario de la organización tiene la autoridad para aprobar la instalación de software **no licenciado** en los equipos de la organización.
- El proceso TIC realizará verificaciones periódicas (programadas y no programadas) para validar que el software instalado en cada uno de los equipos de los usuarios está autorizado y cumple en licenciamiento.

4.5.6 Actualizaciones de Software

Todo software es susceptible de requerir actualizaciones, esto incluye el firmware en los sistemas operativos de los dispositivos electrónicos, aplicaciones informáticas.

Los fabricantes de software lanzan actualizaciones que mejoran, añaden nuevas funcionalidades y corrigen vulnerabilidades. Los sistemas no actualizados son aprovechados por delincuentes para explotarlos. Debemos ser conscientes sobre esta necesidad y mantener permanentemente actualizado y parchado todo el software de la organización. En los casos donde se requiere que sea manual se debe realizar de la **fuente directa del fabricante o página oficial. En casos de subcontratos a terceros, exigiremos que el software este actualizado.**

4.5.7 Control de Navegación (Antimalware)

La navegación en el ciberespacio abre las puertas a lo desconocido y con ello aparecen virus y todo tipo de malware, las vías de contagio son numerosas, a continuación, se relacionan los controles para proteger los activos de información:

Se deniega el acceso web a plataformas que no correspondan al contexto corporativo como redes sociales, TV en línea, radio en línea, descarga de música, páginas con contenido violento, drogas y sexual.

Como excepción, algunas redes sociales serán permitidas para los procesos de comunicaciones y mercadeo, talento y gestión comercial, en el caso que otro proceso requiera de estas, deberá justificar su uso de acuerdo con sus funciones.

- No es permitido la visualización o descarga de información con contenidos que no forman parte de las actividades propias asignadas al usuario.
- Es responsabilidad de cada usuario la información que circule en las plataformas corporativas, por lo cual debe velar por el cumplimiento de los controles y buenas prácticas para la seguridad de la información; sin embargo, el proceso TIC implementa estrategias para salvaguardar la información divulgada.
- Toda solicitud de acceso a información o servicios no incluidos en la configuración inicial de usuario deberá ser solicitada por escrito en mesa de ayuda, justificar el motivo, tipo de permiso (visitante -lector, Integrante - permisos para editar) junto con la aprobación del jefe de área o director de proyecto.
- Los responsables del proceso TIC tendrán la facultad de interrumpir las actividades de los demás usuarios cuando se presenten situaciones que así lo ameriten, ya sea por casos de contingencia, auditoria, monitoreo y/o restablecimiento de servicios.

- Los usuarios deberán solicitar apoyo al proceso de TIC, registrando en mesa de ayuda, cualquier duda, inconveniente o cambio en el manejo de los recursos de cómputo de la organización.

4.5.8 Protección puesto de trabajo

La gestión de la información se realiza desde el puesto de trabajo (oficina o teletrabajo) tanto desde dispositivos tecnológicos como la forma tradicional (papel, teléfono, entre otros). De allí la importancia de concientizar y exigir el cumplimiento de normas de seguridad en el puesto de trabajo para garantizar la seguridad de la información:

- Bloqueo de sesión: bloquear la sesión al ausentarte del puesto de trabajo.
- Sistema operativo actualizado.
- Antivirus actualizado y activo.
- Bloqueo de puertos USB.
- Se prohíbe la alteración de la configuración del equipo e instalación de aplicaciones no autorizadas.
- Mesas limpias y despejadas: la mesa de trabajo debe permanecer limpia y despejada, sin documentación confidencial, ni dispositivos al alcance de otras personas.
- No abandonar documentación sensible en impresoras o escáner: recoger inmediatamente los documentos enviados a imprimir y guardar en el sitio adecuado la información escaneada y eliminas del sitio público.
- Destrucción de información confidencial de forma segura, teniendo en cuenta el método apropiado para el soporte de almacenamiento. Utilizar maquina destructora de papel para eliminar información confidencial.
- No compartir información de la organización a usuarios no autorizados o terceros no identificados: peligros de la ingeniería social y la información que no se debe revelar.
- No publicar ni compartir claves, tampoco anotar en documentos, libretas ni en cualquier otro tipo de soporte (WhatsApp).

4.5.9 Uso de redes wifi y redes externas

Las redes wifi-abiertas en su mayoría no cuentan con capas de seguridad que ofrece encriptación de los datos, esto puede permitir que los ciberdelincuentes intercepten los datos trasmitidos a través de la red por tal razón, no se debe conectar computadores corporativos ni ingresar a las herramientas o plataformas corporativas con conexión a redes wifi-públicas como (café internet, bibliotecas, centros comerciales, aeropuertos). Por el contrario, conectar el equipo a redes conocidas y privadas. Cuando no hay redes confiables la última opción es conectar a la red de datos móvil, configurarla previamente con una clave robusta.

4.5.10 Teletrabajo seguro

El teletrabajo permite llevar a cabo la actividad laboral desde una ubicación distinta a la oficina, habitualmente se realiza desde el domicilio del colaborador. La seguridad durante el teletrabajo está vinculada a tecnología utilizada para el acceso a las herramientas corporativas de la organización, se debe garantizar la seguridad de toda la información y los recursos gestionados cuando se teletrabaja, a continuación, se incluyen una serie de controles para teletrabajo seguro:

- No se permite el uso de computadores personales para teletrabajar, ya que los colaboradores cuentan con un equipo corporativo configurado con parámetros de seguridad que la organización considera necesarios y tiene el software puntual para realizar el trabajo de forma segura.
- Se realizarán verificaciones para asegurar el cumplimiento del uso del equipo asignado en teletrabajo.
- La configuración de la red Wifi domiciliaria debe también contar con clave robusta.
- La herramienta permitida para teleconferencia y entorno colaborativo es Teams.
- Bloquear siempre la sesión del equipo cuando no este frente a él.
- Mantener condiciones de orden y aseo.

4.5.11 Protección de Equipos

Los usuarios deberán cuidar, respetar y hacer un uso adecuado de los recursos informáticos de acuerdo con lo mencionado en este documento:

- El cableado estructurado debe ser protegido contra intercepción, interferencias y posibles daños.
- Los usuarios no están autorizados para mover, readecuar, suprimir o modificar las conexiones eléctricas y de datos.
- Los equipos de cómputo de escritorio deben ser protegidos contra fallas de suministro eléctrico con un sistema de energía ininterrumpido (UPS) o estabilizador.
- Los mantenimientos preventivos periódicos de los equipos de cómputo se deben ejecutar según se acuerde con el proveedor del servicio de alquiler del equipo y es deber del usuario asistir a la fecha programada para la ejecución de este.
- Los usuarios no están autorizados para realizar limpieza profunda física y lógica o mantenimiento al equipo asignado.
- No exponer los equipos a altas temperaturas.
- No descuidar el portátil en el transporte público.
- No dejarlo visible en el vehículo o fácilmente accesible.

- Si el lugar de trabajo no garantiza su custodia, anclarlo con guaya o guardarlo en un cajón con seguridad.
- Con el fin de evaluar las condiciones técnicas y de funcionalidad de los equipos, anualmente se verificará el estado de obsolescencia; acorde a los resultados obtenidos se tomarán acciones para repotenciar o remplazar los dispositivos, teniendo como base los requerimientos mínimos establecidos para la organización definidos en la ficha técnica, de acuerdo con el *Alistamiento de equipos de cómputo, I-TI-01.*
- Es obligatorio el uso del computador corporativo para actividades laborales, no se permite el uso de equipos personales para ejecutar su trabajo en la organización.
- Los dispositivos asignados deben ser utilizados exclusivamente para actividades laborales.
- Joyco y sus consorcios garantizará la adecuada disposición final de los RAEE, de los equipos alquilados se hace exigiendo el cumplimiento de la legislación vigente al proveedor de los equipos; para los dispositivos electrónicos propios se hace de acuerdo con lo establecido en el *Plan de gestión integral de residuos sólidos y peligrosos, DG-GI-33.*

4.5.12 Borrado Seguro

- Cuando se devuelva un equipo al proveedor o se liberen dispositivos de almacenamiento, es responsabilidad del usuario garantizar que la información se encuentre alojada en la plataforma Office 365. A su vez el equipo TIC, realizará el borrado seguro según lo descrito en el *Borrado seguro de la información, I-TI-03.*
- Cuando se presente daño físico del dispositivo de almacenamiento, se deberán realizar acciones sobre este que imposibilite la recuperación de información.
- Se deberá utilizar el proceso de triturado para destruir la información de soportes no electrónicos (papel y soportes magnéticos).
- Se deberá eliminar información para la reutilización de medios electrónicos.
- Cuando finalice un servicio con un tercero que incluya alojamiento de información se deberá respaldar y eliminar previamente la información alojada y solicitar al proveedor la evidencia del borrado o eliminación por completo de su infraestructura tecnológica.

4.6 Sistema de Seguridad de la Información en situaciones de contingencia

El responsable de Seguridad de la información de la organización deberá diseñar, implementar y probar un plan de continuidad del negocio que permita recuperar en un tiempo razonable la operatividad de la organización.

5. COPIAS DE SEGURIDAD

Los medios o sistemas de almacenamiento contienen uno de los activos más preciado, que es la información, este puede verse involucrado en situaciones como robo, virus, borrado accidental, entre otros. Joyco, definirá un procedimiento que permita determinar los activos que, de acuerdo con su criticidad, las cuales requieren copias de seguridad para garantizar la continuidad del negocio.

5.1 Concienciación y Formación.

El creciente uso de las nuevas tecnologías hace indispensable la concienciación sobre los riesgos, es necesario que los colaboradores conozcan y apliquen buenas prácticas en el uso de dispositivos (Computador de escritorio, portátiles, dispositivo móvil, memorias USB, discos duros, entre otras herramientas) y sistemas (página web, servicios en la nueve, redes sociales, correo electrónico, plataformas corporativas, entre otras) para lo cual Joyco y sus consorcios, proporcionará formación en ciberseguridad adecuada para prevenir incidentes:

- Todos los colaboradores deben mejorar continuamente sus conocimientos en materia de Seguridad de la Información y Ciberseguridad a su vez son responsables de adquirir estas competencias asistiendo a las actividades, capacitaciones a las cuales se le invite o programe.

5.2 Gestión de Incidentes

Un incidente de Seguridad de la Información es cualquier evento que daña o representa una amenaza para toda o una parte de la infraestructura tecnológica y de la información, pueden ser: sustracción de información, intrusión a sistemas de información, uso no autorizado de datos, denegación de servicios, violación a las políticas de uso de servicios, entre otros. Con el objetivo de proteger las características fundamentales de la información y prevenir la perdida de servicios y cumplir con requisitos legales se establece que:

- Cualquier colaborador, contratista, tercero puede reportar incidentes de seguridad de la información que afecten a la organización.
- Cada responsable de proceso o proyecto debe identificar incidentes de seguridad de la información y reportarlo.
- Cualquier dispositivo de uso personal (celulares, tablets) o computador corporativo que este implicado en incidentes de seguridad puede ser sometido a cadena de custodia para fines de investigación o evidencia ante fines administrativos o legales, previa coordinación con el usuario.

5.3 Supervisar la Gestión de Seguridad de la Información.

La Alta Dirección debe aprobar y revisar periódicamente la Gestión de Seguridad de la Información mediante, el seguimiento del Plan de Seguridad Informática para asegurarse de que las políticas, procesos y sistemas se aplican eficazmente.

5.4 Gestionar el cambio

Una vez evaluado el riesgo y se requiera la planificación de actividades que permitan subsanar una brecha o mejora, se debe seguir el procedimiento de *Gestión del cambio, P-GI-06.*

5.5 Realizar Seguimiento

El responsable del proceso TIC debe monitorear regularmente la evolución de los controles implementados con el fin de verificar su eficacia.

6. INVESTIGACIÓN Y SANCIONES

La *Política de Seguridad de la Información y Ciberseguridad, DG-TI-02,* es de aplicación obligatoria para todo el personal de la empresa Joyco, sus consorcios y sus agentes relacionados, el incumplimiento de esta y demás actividades que se deriven de ella traerá consigo las consecuencias disciplinarias y legales que apliquen de acuerdo con el *Reglamento Interno de Trabajo de la organización* y con el *Código de ética y conducta, DG-GE-03,* y legislación colombiana.

7. REGISTROS REFERENCIADOS

- *Declaración de indemnidad, F-TI-11.*
- *Reporte de devolución de equipo de cómputo y dispositivos de tecnología*, *F-TI-12.*
- *Requisición, F-CC-03.*

8. CONTROL DE CAMBIOS

Versión	Fecha	Cambios realizados
01	Marzo/2024	Versión inicial