POLÍTICA
SEGURIDAD DE LA INFORMACIÓN

www.gesth.co

P-TI-01. Versión 2.1, Mayo 2023

Optimizamos tus procesos de reclutamiento y selección a través de un servicio especializado para atraer, evaluar y seleccionar el talento humano ideal que requiere tu equipo de trabajo.

TABLA DE CONTENIDO

1. OBJETIVO DE LA POLÍTICA

Establecer lineamientos relacionados con la seguridad de la información abordando temáticas específicas, como complemento a lo definido en la "**Política General de Seguridad de la Información**" con el fin de preservar la confidencialidad, integridad y disponibilidad de los activos de **GESTIÓN ESTRATÉGICA DEL TALENTO HUMANO S.A.S**

Dentro de las temáticas que se tocan en la política se encuentran por ejemplo la gestión de activos, seguridad física y ambiental, control de accesos, copias de seguridad, infraestructura en la nube y acceso a la información, lo cual estableció como principios necesarios e importantes los siguientes conceptos:

- **GESTIÓN ESTRATÉGICA DEL TALENTO HUMANO S.A.S** protegerá la información creada, procesada, transmitida o resguardada por sus procesos de negocio, con el fin de minimizar impactos financieros, operativos o legales debido a un uso incorrecto de esta.
- **GESTIÓN ESTRATÉGICA DEL TALENTO HUMANO S.A.S** protegerá su información de las amenazas originadas por parte del personal.
- **GESTIÓN ESTRATÉGICA DEL TALENTO HUMANO S.A.S** protegerá las instalaciones y su infraestructura tecnológica.
- **GESTIÓN ESTRATÉGICA DEL TALENTO HUMANO S.A.S** controlará y auditara la operación de sus procesos de negocio garantizando la seguridad de los recursos tecnológicos y las redes de datos.
- **GESTIÓN ESTRATÉGICA DEL TALENTO HUMANO S.A.S** implementará control de acceso a la información, sistemas y recursos de red.
- **GESTIÓN ESTRATÉGICA DEL TALENTO HUMANO S.A.S** garantizará la disponibilidad de sus procesos de negocio y la continuidad de su operación basada en el impacto que pueden generar estos eventos.
- **GESTIÓN ESTRATÉGICA DEL TALENTO HUMANO S.A.S** garantizará el cumplimiento de las obligaciones legales, regulatorias y contractuales establecidas.

2. INTRODUCCIÓN

La dirección de **GESTIÓN ESTRATÉGICA DEL TALENTO HUMANO S.A.S**, entendiendo que la seguridad de la información es un aspecto crucial para la organización. La protección de nuestros datos y sistemas de información es fundamental para mantener la confidencialidad, integridad y disponibilidad de los mismos.

Como parte de nuestros esfuerzos para garantizar la seguridad de la información, hemos elaborado esta política de seguridad de la información para establecer un marco de trabajo que nos permita proteger nuestros activos de información de manera efectiva. Esta política se aplica a todos los colaborador, contratistas, proveedores y terceros que tengan acceso a los sistemas y datos de nuestra organización. Es responsabilidad de todos cumplir con esta política y contribuir a la protección de nuestra información confidencial.

3. ALCANCE DE LA POLÍTICA

El presente manual de políticas aplica a funcionarios, contratistas, terceros, usuarios y visitantes de **GESTIÓN ESTRATÉGICA DEL TALENTO HUMANO S.A.S** por alguna razón tengan cualquier tipo de interacción con los activos de información. La política se aplica a todos los sistemas y recursos de información utilizados por la compañía, incluyendo hardware, software, redes, dispositivos móviles y cualquier otra tecnología que tenga acceso a los datos de la organización.

Esta política cubre todos los tipos de datos utilizados por la organización, incluyendo datos personales, datos financieros, datos de propiedad intelectual y cualquier otra información confidencial. La política se aplica en todas las ubicaciones físicas del **GESTIÓN ESTRATÉGICA DEL TALENTO HUMANO S.A.S**, incluyendo las oficinas, los centros de datos y cualquier otra ubicación de la organización.

La política cumple con las leyes y regulaciones aplicables en cada jurisdicción donde opera la organización. Además, se aplicará a todos los procesos de negocio que involucren el procesamiento de datos de la organización.

Cualquier cambio en el alcance de esta política deberá ser aprobado por el Comité de Seguridad de la Información y comunicado a todos los colaboradores de la compañía.

4. DEFINICIONES

- **Activo de información:** cualquier tipo de información que es propiedad de la organización y que tiene un valor.
- **Amenaza:** cualquier evento o acción que podría dañar la seguridad de la información.

- **Autenticación:** el proceso de verificar la identidad de un usuario o dispositivo.
- **Autorización:** el proceso de otorgar permisos y acceso a un usuario o dispositivo.
- **Backup:** una copia de seguridad de la información importante para protegerla de la pérdida de datos.
- **Confidencialidad:** la propiedad de la información que se refiere a la protección contra el acceso no autorizado.
- **Criptografía:** el proceso de codificar información para protegerla de accesos no autorizados.
- **Gestión de accesos:** el proceso de controlar quién tiene acceso a la información.
- **Gestión de riesgos:** el proceso de identificar, evaluar y mitigar los riesgos para la seguridad de la información.
- **Incidente de seguridad:** cualquier evento que pueda poner en peligro la seguridad de la información.
- **Integridad:** la propiedad de la información que se refiere a su precisión y completitud.
- **Malware:** software malicioso diseñado para dañar o interferir con el funcionamiento normal de los sistemas de información.
- **Política de seguridad de la información:** un conjunto de reglas y pautas que definen cómo se protege la información de la organización.
- **Privacidad:** la protección de la información personal y confidencial.
- **Seguridad física:** la protección de los recursos físicos que contienen la información, como las instalaciones de la organización.
- **Seguridad lógica:** la protección de los recursos lógicos, como sistemas y redes, que contienen la información.
- **Sensibilidad:** el grado de protección que necesita la información basado en su valor y criticidad.
- **Usuario:** cualquier persona que tenga acceso a la información de la organización, ya sea un colaborador, contratista o proveedor externo.
- **Vulnerabilidad:** una debilidad en los sistemas de información que podría ser explotada para dañar la seguridad de la información.
- **Disponibilidad:** Propiedad de la información de ser accesible y utilizable a demanda por una parte interesada.

- **Sistema de Gestión de Seguridad de la Información:** Es el conjunto de manuales, procedimientos, controles y técnicas utilizadas para controlar y salvaguardar todos los activos que se manejan dentro de una entidad.

- **Controles:** Medida que permite reducir o mitigar un riesgo.

5. POLÍTICAS

GESTIÓN ESTRATÉGICA DEL TALENTO HUMANO S.A.S establece a continuación, los siguientes lineamientos de seguridad de la información, los cuales deberán ser cumplidos por todos los funcionarios, contratistas, terceros, usuarios y visitantes. Los lineamientos de seguridad están clasificados en diferentes temáticas, teniendo en cuenta el contexto interno y externo de la entidad:

POLÍTICAS DE SEGURIDAD DE LOS RECURSOS HUMANOS

- Durante el proceso de selección de personal de planta o contratistas, se realizará verificación de antecedentes disciplinarios de los candidatos sin importar el cargo o posición al cual se postulen.
- Todo el personal que labore en la entidad o preste servicios a la misma deberá firmar un acuerdo de confidencialidad y un documento de conocimiento y aceptación de las políticas definidas para el sistema de seguridad de la información y buen uso de los activos de información. Mediante el cual se compromete a realizar un adecuado uso de estos.
- Análisis de seguridad del entorno o puesto de trabajo, instalación de cámaras de seguridad, controles de acceso físico y medidas de seguridad en la red.

POLÍTICAS DE GESTIÓN DE ACTIVOS

- Toda información sea física o digital generada, almacenada o transformada por los funcionarios, contratistas o proveedores de la entidad, utilizando los recursos dispuestos por la entidad para tal fin o en desempeño de sus labores o servicio contratado, son activos de información propiedad de **GESTIÓN ESTRATÉGICA DEL TALENTO HUMANO S.A.S.**
- Los activos dispuestos por el **GESTIÓN ESTRATÉGICA DEL TALENTO HUMANO S.A.S**. para el apoyo de las labores desempeñadas por los funcionarios, contratistas o proveedores, únicamente se permitirá su utilización para ejecución de tareas establecidas en el ámbito laboral de **GESTIÓN ESTRATÉGICA DEL TALENTO HUMANO S.A.S.**

- **GESTIÓN ESTRATÉGICA DEL TALENTO HUMANO S.A.S** identificara, clasificara y gestionara su inventario de activos conforme a los manuales y procedimientos de Gestión de Activos formalizados.

POLÍTICAS DE CONTROL DE ACCESO LÓGICO

- Para la protección de los activos de información, se establecerán procedimientos y políticas para el control de acceso a la red, sistemas de información e infraestructura física (Instalaciones). Con el fin de mitigar los riesgos asociados al acceso no autorizado a la información.
- Todos los usuarios deberán asumir la responsabilidad sobre la información física o digital que accedan y procesan dando un uso adecuado con el fin de salvaguardar la confidencialidad, integridad y disponibilidad de la información.
- Gestión de procedimientos para la monitorización de los accesos, registro de eventos y auditorias periódica con el fin de detectar y prevenir posibles ataques o intentos de acceso no autorizados.

POLÍTICAS DE CRIPTOGRAFÍA

- **GESTIÓN ESTRATÉGICA DEL TALENTO HUMANO S.A.S** implementará herramientas de cifrado en todos los portátiles de compañía, unidades de disco duro, áreas contables y financieras, con el fin de proteger la confidencialidad e integridad de la información. Así mismo, el Grupo/Oficina de Tecnológica de Información y las Comunicaciones determinara los equipos a los cuales se les deberán instalar controles criptográficos adicionales cuando así se requiera.
- Se hace uso de herramientas informáticas criptográficas que nos permiten cifrar los datos, gestionar las claves criptográficas, generación de claves seguras, distribución segura de claves, almacenamiento seguro de claves y la eliminación segura de claves cuando ya no sean necesarias.

POLÍTICAS DE SEGURIDAD FÍSICA Y DEL ENTORNO

- **GESTIÓN ESTRATÉGICA DEL TALENTO HUMANO S.A.S** adoptará medidas para el control de acceso físico a las instalaciones y áreas seguras con el fin de mitigar los riesgos asociados a la afectación de la confidencialidad, disponibilidad e integridad de la información.
- **GESTIÓN ESTRATÉGICA DEL TALENTO HUMANO S.A.S** definirá áreas seguras y los controles de acceso físico correspondientes para la protección de la información que allí se resguarda.
- Todas las personas que ingresen a las instalaciones de **GESTIÓN ESTRATÉGICA DEL TALENTO HUMANO S.A.S** deben cumplir con los lineamientos establecidos para el control de acceso físico sin excepción.

POLÍTICAS DE SEGURIDAD DE LAS COMUNICACIONES

- El Grupo de Tecnológica de la Información y las Comunicaciones, establecerá los controles para acceso lógico y protección de las redes del **GESTIÓN ESTRATÉGICA DEL TALENTO HUMANO S.A.S**, con el fin de asegurar y cumplir con los acuerdos de niveles de servicios que sean establecidos para los servicios de red y que deberán ser acordados con la alta dirección.
- El **GESTIÓN ESTRATÉGICA DEL TALENTO HUMANO S.A.S** definirá procedimientos y lineamientos para la transferencia segura de información interna o externamente, de tal forma que se garantice la integridad y confidencialidad de la información.

POLÍTICAS DE ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS

- El Grupo/Oficina de Tecnológica y Comunicaciones, velara que los sistemas de información que sean implementados en la entidad cumplan con los requerimientos de seguridad y buenas prácticas.
- Todos los procesos de la entidad que realicen desarrollos deberán cumplir con los procedimiento y metodologías de desarrollo establecidos y formalizados para poder liberar sus aplicaciones.
- Todos los procesos de la entidad deberán informar al área de tecnología sobre sus proyectos de adquisición de sistemas de información, con el fin de brindar las observaciones correspondientes y revisar los aspectos técnicos necesario para su desarrollo e implementación.

POLÍTICAS DE RELACIONES CON LOS PROVEEDORES

- **GESTIÓN ESTRATÉGICA DEL TALENTO HUMANO S.A.S** establecerá políticas y requisitos de seguridad de la información para mitigar los riesgos asociados a cada proceso de contratación.
- Antes de Iniciar la ejecución de contratos con terceras partes, deberán suscribirse los respectivos acuerdos de confidencialidad que incluyan las cláusulas de confidencialidad y los aspectos de seguridad de la información necesario durante y después del contrato.

POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN EN LA CONTINUIDAD DE NEGOCIO

- **GESTIÓN ESTRATÉGICA DEL TALENTO HUMANO S.A.S** establecerá un plan de continuidad tecnológica donde se debe incluir la continuidad de la seguridad de la información y restauración oportuna de los servicios en un escenario de contingencia.
- El Grupo/Oficina de TIC generará dicho plan de continuidad tecnológica con base a Planes de Recuperación de Desastres (DRP) y Análisis de Impacto al Negocio (BIA).

ESCRITORIO LIMPIO:

- No deberán dejarse documentos críticos en el "Escritorio" tanto físico como el Escritorio virtual (se denomina "Escritorio" al espacio digital en los equipos de cómputo).
- Cada vez que los funcionarios se retiren del lugar de trabajo deben bloquear los equipos de cómputo.
- Emplear las cajoneras o archivos para el almacenamiento de la información sensible o crítica.

USO ADECUADO DE INTERNET

El internet es un recurso valioso para el desempeño de las labores de todos los funcionarios y, por lo tanto, se definen los siguientes lineamientos para su uso adecuado.

- Estará limitado el acceso a portales de: Juegos, pornografía, drogas, terrorismo, segregación racial, hacking, malware, software gratuito o ilegal y/o cualquier otra página que vaya en contra de las leyes vigentes.
- Estará limitado el acceso a redes sociales en general.
- Se restringirá el acceso a portales de nube e intercambio de información masiva (exceptuando a la nube corporativa o institucional).
- El grupo/oficina de TIC podrá verificar los logs o registros de navegación cuando así se solicite o se requiera para las investigaciones o requerimientos que puedan generarse.

USO ADECUADO DE CORREO ELECTRÓNICO:

- Los buzones de correo asignados a los funcionarios, contratistas o terceros pertenecen a **GESTIÓN ESTRATÉGICA DEL TALENTO HUMANO S.A.S**, por lo tanto, su contenido también es propiedad de la Entidad.
- El correo electrónico solo deberá emplearse para uso institucional y el desempeño de las funciones correspondientes a cada cargo.
- La oficina/grupo de tecnología podrá verificar el contenido de los buzones de los correos electronicos en los casos que se requiera acudir a información para continuar con la prestación del servicio o para investigaciones específicas.

USO DE USUARIOS Y CONTRASEÑAS:

- Cada funcionario o contratista cuyas funciones requieran de acceso a sistemas de información o correo electrónico, deberá asignársele un usuario y contraseña.

- Las credenciales son personales e intransferibles.
- Deben utilizarse esquemas de seguridad para la creación de contraseñas (uso de Mayúsculas, Minúsculas, Caracteres, Números).

POLÍTICAS DE ROLES Y RESPONSABILIDADES

- Los colaboradores de la organización deben tomar medidas adecuadas para proteger la información confidencial. Esto incluye mantener la información en lugares seguros y limitar el acceso a ella solo a las personas que la necesitan.
- Los colaboradores deben seguir los estándares de seguridad establecidos por la organización para proteger la información confidencial.
- Los colaboradores deben informar cualquier violación de seguridad o incidente de seguridad que puedan encontrar. Esto puede incluir la divulgación no autorizada de información confidencial o cualquier intento de acceso no autorizado.
- Los colaboradores deben estar al tanto de la importancia de la seguridad de la información y ser entrenados para reconocer y prevenir posibles amenazas de seguridad.
- Las responsabilidades frente a la seguridad de la información serán definidas, compartidas, publicadas y aceptadas por cada uno de los colaborador, proveedores, socios de negocio o terceros.
- Se designa como oficial de seguridad de la información de la compañía **GESTIÓN ESTRATÉGICA DEL TALENTO HUMANO S.A.S** al Líder de Sistemas de la compañía.

POLÍTICA DE DISPOSITIVOS MÓVILES

- **GESTIÓN ESTRATÉGICA DEL TALENTO HUMANO S.A.S** implementara para todos los dispositivos de computación móvil como son teléfonos, portátiles y tabletas. Fuertes contraseñas de acceso, encriptación de datos, actualizaciones de seguridad, requerir permisos a ciertas aplicaciones para acceder a diferentes funciones o información del dispositivo, copias de seguridad periódicas, bloqueo remoto y eliminación de la información esto nos ayuda a prevenir la pérdida de información en caso de que el dispositivo se pierda o sea dañado.

POLÍTICA DE TELETRABAJO

- **GESTIÓN ESTRATÉGICA DEL TALENTO HUMANO S.A.S** para todos los colaboradores que estén en teletrabajo se implementaran los siguientes controles de seguridad: Uso de VPN prevenimos la interceptación de datos y aseguramos la privacidad de la información transmitida. Autenticación de dos factores (2FA) para acceder a un sistema o aplicación. Encriptación de datos, Actualizaciones de seguridad, Uso de Antivirus ayuda a proteger los dispositivos utilizados para el teletrabajo contra ataques cibernéticos y malware. Capacitaciones de seguridad para comprender la importancia de mantener la seguridad de los datos y la información de la empresa.

POLÍTICA DE USO ACEPTABLE DE LOS ACTIVOS

Se considera uso aceptable de los recursos tecnológicos para apoyar las labores propias de los colaborador de acuerdo con la misión y visión del **GESTIÓN ESTRATÉGICA DEL TALENTO HUMANO S.A.S.**

- Deben ser usados racionalmente evitando el uso ineficiente de los mismos.
- Los datos e información creada, relacionada con las operaciones propias de la compañía deberán ser almacenadas de manera estricta en dispositivos y sistemas de información pertenecientes al **GESTIÓN ESTRATÉGICA DEL TALENTO HUMANO S.A.S.**
- Todos los datos e información sin importar su clasificación, relacionados con la operación de la compañía, son de propiedad exclusiva del **GESTIÓN ESTRATÉGICA DEL TALENTO HUMANO S.A.S** y deberá solicitarse permiso por medio formal cuando se requiera manipular esta información.
- El uso de todos los recursos tecnológicos de la compañía tiene el único propósito, apoyar los procesos asignados a cada colaborador del **GESTIÓN ESTRATÉGICA DEL TALENTO HUMANO S.A.S.**

Se considera uso no aceptable de recursos tecnológicos:

- El uso de los activos tecnológicos con fines personales, lúdicos o de lucro para el usuario.
- La publicación de contenido que resulte incómodo para los otros colaborador o que atente contra los valores y la ética de la compañía.
- El uso y transmisión de información violando derechos de propiedad intelectual.
- El inicio de sesión en activos personales o ajenos a la compañía sin autorización previa.

- El uso excesivo de los recursos para fines no relacionados con las labores asignadas causando lentitud en los objetivos de la compañía.
- El uso de software malicioso para generar degradación de los activos de información de la compañía.
- El uso de software licenciado no autorizado en los equipos de la compañía.
- El uso de tecnologías de almacenamiento externo, sin la debida autorización de los colaborador a cargo del SGSI de la compañía.
- El proporcionar usuarios, contraseñas o cualquier otro tipo de credenciales de accesos a personal no autorizado por la compañía.
- Cualquier acción vandálica que cause degradación en los activos de información de la compañía.
- La reubicación de activos, así como conexión o desconexión de estos sin autorización de la Dirección de TI.
- La modificación de los equipos de escritorio, portátiles y/o dispositivos móviles a nivel sistema operativo, sin autorización de la Dirección de TI.
- La manipulación de las bases de datos internas o pertenecientes a los clientes sin autorización de la Dirección de TI.

POLÍTICA DE DEVOLUCIÓN DE ACTIVOS

- Todos los colaboradores y usuarios de partes externas deberán devolver todos los activos de la organización que se encuentren a su cargo, al terminar su empleo, contrato o acuerdo. La Dirección IT revisara el estado y condiciones en el que fueron entregados estos implementos de tecnología y se procederá a seguir el procedimiento de cancelación de cuentas, el acceso remoto y las credenciales de acceso del colaborador o contratista. En caso de no cumplimiento de las políticas de devolución de activos se aplicaran medidas disciplinarias, incluyendo las sanciones correspondientes según la gravedad de la infracción.

POLÍTICA DE MANTENIMIENTO DE EQUIPOS

- **GESTIÓN ESTRATÉGICA DEL TALENTO HUMANO S.A.S** todos los activos fijos de la compañía cuentan con un programa de mantenimiento preventivo que incluye inspecciones y reparaciones regulares para asegurar que los equipos estén en buen estado de

funcionamiento. Se implementa procedimiento para la limpieza de equipos, para prevenir la acumulación de polvo y suciedad, lo que puede reducir la vida útil del equipo.

- Gestión de actualizaciones y parches de software, para garantizar que el software utilizado por la empresa esté actualizado y protegido contra las últimas vulnerabilidades de seguridad.

POLÍTICA DE RETIRO DE ACTIVOS

- Los equipos informáticos de la compañía no deben ser retirados de las instalaciones sin autorización previa de la compañía. Los colaboradores de la compañía deben solicitar autorización para retirar equipos que incluyan la verificación de la necesidad de retirar el equipo, siguiendo el procedimiento de documentación y el seguimiento de los equipos retirados.

POLÍTICA DE CONTROLES CONTRA CÓDIGOS MALICIOSOS

- Se implementara controles de detección, de prevención y de recuperación, combinados con la toma de conciencia apropiada de los usuarios, para proteger contra códigos maliciosos.

POLÍTICA DE RESPALDO DE INFORMACIÓN

- Toda la información será respaldada a través de copias de seguridad, realizadas periódicamente, estas copias serán sujetas de pruebas de restauración para garantizar que el proceso de respaldo se realice correctamente. Incluyen archivos críticos como bases de datos, correos electrónicos, archivos del paquete office y otros datos importantes para el negocio.

POLÍTICA DE GESTIÓN DE MEDIOS REMOVIBLES

- Se permite el uso de dispositivos extraíbles a los funcionarios cuyos roles y responsabilidades requieran hacer uso de estos recursos y previa autorización de la Dirección de TI, así mismo el funcionario se compromete a salvaguardar lógica y físicamente el dispositivo. Se establecerá procedimientos para endurecer el uso de estos dispositivos con el fin de disminuir el riesgo de fuga de información por acceso no autorizado o perdida de estos.

NOTIFICACIÓN DE INCIDENTES:

Toda violación de estas políticas se deberá notificar al encargado de la seguridad de la información, inmediatamente, a través de la cuenta tecnologia@grupops.com.co Se deberán notificar situaciones tales como:

- Personas ajenas de la organización en centros de cómputo sin la debida autorización.
- Correos con virus.
- Reinicio de los equipos de cómputo o enrutadores.
- Mala utilización de recursos.
- Uso ilegal del software.
- Mal uso de información corporativa.
- Alteración de información, etc.

6. SENSIBILIZACIÓN Y COMUNICACIÓN EN SEGURIDAD DE LA INFORMACIÓN

SENSIBILIZACIÓN Y COMUNICACIÓN

GESTIÓN ESTRATÉGICA DEL TALENTO HUMANO S.A.S, definirá un "**Plan de Comunicación en Seguridad de la Información"** a través de su oficina de comunicación interna y externa y el Grupo/Oficina TIC, donde se planificará ANUALMENTE la manera en que se comunicarán recomendaciones o tips de seguridad de la información por diferentes medios a todos sus funcionarios y contratistas, con el fin de socializar las políticas institucionales en seguridad de la información o las buenas prácticas en seguridad que se desean socializar para aumentar las capacidades de todas las áreas y procesos de la entidad. La creación de los contenidos se hará con apoyo de la oficina TIC y/o el Oficial de Seguridad de la información.

CAPACITACIONES EN SEGURIDAD

GESTIÓN ESTRATÉGICA DEL TALENTO HUMANO S.A.S, a través de sus áreas/procesos de Talento Humano y Contratos, incluirá dentro de sus capacitaciones e inducciones las temáticas de seguridad de la información, con el objetivo de que cualquier funcionario y/o contratista que se vincule a la entidad tenga pleno conocimiento de las políticas de seguridad de seguridad de la información, el grupo TIC y/o el Oficial de Seguridad de la Información apoyará en dichas inducciones.

7. APROBACIÓN Y REVISIÓN DE LAS POLÍTICAS

Las políticas aquí definidas se harán efectivas a partir de su aprobación por la Alta Dirección y serán revisadas por lo menos anualmente, cuando existan incidentes de seguridad de la información o cuando se produzcan cambios estructurales considerables, esto con el fin de asegurar su vigencia y aplicabilidad dentro del **GESTIÓN ESTRATÉGICA DEL TALENTO HUMANO S.A.S.**

8. SANCIONES

La falta de conocimiento de los presentes lineamientos no libera al personal de **GESTIÓN ESTRATÉGICA DEL TALENTO HUMANO S.A.S** de las responsabilidades establecidas en ellos por el mal uso que hagan de los recursos de TIC o por el incumplimiento de los lineamientos aquí descritos.

a. Se aplicarán sanciones de acuerdo con el Código Único Disciplinario.

b. Pueden aplicarse sanciones de tipo penal según sea el caso y la gravedad de este, si así lo consideran los entes investigativos y judiciales correspondientes.

c. El Grupo TIC será el encargado de recopilar y entregar a la Oficina de Gestión Humana las evidencias de incumplimiento de los lineamientos, informes de impactos y consecuencias y cualquier otro insumo requerido para formalmente manejar la investigación inicialmente a nivel interno, así mismo, el grupo TIC será el encargado de registrar y gestionar el Incidente de seguridad derivado con el incumplimiento de las políticas.

ELABORÓ	REVISÓ	APROBÓ
Oscar Daniel Lozano Diaz Analista de Desarrollo y Tecnología – Implementador ISO 27001 Fecha: 01-06-2023	Angela Gonzalez Directora de Proyectos Fecha: 01-06-2023	Sergio Mercado Gerente General Fecha: 01-06-2023