POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

Elaborado por:	**Revisado por:**	**Aprobado por:**
Comité del Sistema Integrado de Gestión	Director de Ingeniería y Servicios	Gerente General
Fecha: 19/12/2025	**Fecha:** 19/12/2025	**Fecha:** 05/01/2026

TABLA DE CONTENIDO

1. OBJETIVO

El propósito de esta política es establecer las directrices específicas para gestionarla seguridad de información relativa a los activos de información de GRUPO ELECTRODATA y de sus partes interesadas, en relación a los requisitos del negocio, regulatorios y contractuales.

2. ALCANCE

Aplica a todo el personal de GRUPO ELECTRODATA, incluido practicantes, socios, contratistas, proveedores, consultores y cualquier otro personal externo autorizado para el tratamiento de activos de información de GRUPO ELECTRODATA y de sus clientes.

El personal autorizado para el tratamiento de activos de información del cliente debe adherirse adicionalmente a las políticas establecidas por el mismo, con el fin de mantener la confidencialidad, integridad y disponibilidad de los recursos asignados.

3. REFERENCIAS

- ISO 27001:2022 e ISO 27002:2022 Sistemas de Gestión de Seguridad de la Información – Requisitos A5.17; A8.1; A5.10; A8.24 y A7.8.

4. DEFINICIONES:

- **Activos de información:** Cualquier elemento que tiene valor para la organización. Esta definición incluye no sólo herramientas tangibles, como hardware y equipos de red, sino también los intangibles, como información, conocimientos, software, propiedad intelectual y reputación.
- **Dispositivos finales de usuario:** computadoras portátiles, teléfonos móviles, tablets u otro dispositivo electrónico que pueda conectarse a los sistemas de la organización
- **Confidencialidad:** Principio que requiere que la información sea accesible de forma única a las personas que se encuentran autorizadas.
- **Integridad:** Capacidad de mantener inalterada la información ante accidentes o intentos maliciosos
- **Disponibilidad:** Capacidad de mantener accesible y utilizable la información a pedido de personal autorizado.

5. ROLES ORGANIZACIONALES, RESPONSABILIDADES Y AUTORIDADES.

GRUPO ELECTRODATA ha definido y asignado las responsabilidades relativas a la seguridad de la información, definiendo en cada puesto de trabajo tanto las funciones

del personal que se encuentre en el mismo como las responsabilidades imputables, todo ello se realizará conforme al **GTH-M-01 Manual de Organización y Funciones.**

El Comité de SIG es responsable de revisar y proponer las directivas institucionales para su aprobación, la POLÍTICA de Seguridad de Información, las funciones generales en materia de seguridad de la Información y la estructuración, recomendación, seguimiento y mejora del Sistema de Gestión de Seguridad de la institución. Es responsabilidad de dicho Comité definir las estrategias de capacitación en materia de seguridad de la información al interior del GRUPO ELECTRODATA.

El Oficial de Seguridad de la Información será el responsable de coordinar las acciones del Comité, presentar las propuestas, mejoras, y de impulsar la implementación y cumplimiento del SGSI.

Los propietarios de activos de información son responsables de clasificar, mantener y actualizar la información, así como de documentar y mantener al día la clasificación efectuada. En términos generales, tienen la responsabilidad de preservar la integridad, confidencialidad y disponibilidad del activo de información durante su uso.

Los propietarios de los riesgos son responsables de ejecutar el plan de tratamiento de riesgos.

El Encargado de Servicios Generales será el encargado del acondicionamiento y aseguramiento de áreas físicas del GRUPO ELECTRODATA, previniendo con ello los accesos no autorizados, incendios, inundaciones y robos.

El Director de Ingeniería y Servicios debe cumplir con los requerimientos que en materia de seguridad de la información se establezcan para la operación, administración, comunicación y mantenimiento de los sistemas de información y los recursos de tecnología del GRUPO ELECTRODATA.

La Gerente de Administración y Finanzas asegura que los contratos, acuerdos y demás documentos suscritos por GRUPO ELECTRODATA con empleados y terceros contengan las disposiciones establecidas en la documentación del Sistema Integrado de Gestión.

La Gerencia General tiene la responsabilidad de supervisar y garantizar que la estrategia definida en GRUPO ELECTRODATA cumpla con la consecución de los objetivos organizativos. Asimismo, debe asignar todos los recursos necesarios para la implementación efectiva del Sistema de Gestión y llevar a cabo revisiones periódicas del Sistema Integrado de Gestión.

Los usuarios de la información y de los sistemas utilizados para su procesamiento tienen la responsabilidad de conocer y adherirse a la POLÍTICA de Seguridad de la Información actualmente en vigor.

6. DESCRIPCIÓN DE ACTIVIDADES

En este documento se establecen las políticas de seguridad que deben seguir los empleados en su puesto de trabajo. Esto abarca tanto las normas de acceso físico como las lógicas, que incluyen el acceso a las aplicaciones, intranet, correo electrónico, entre otras.

6.1. POLÍTICA DEL SISTEMA INTEGRADO DE GESTIÓN (SIG-D-01)

GRUPO ELECTRODATA S.A.C es una empresa comprometida con nuestros clientes buscando ser sus socios estratégicos de valor, implementando soluciones innovadoras y eficientes de tecnologías de la información y comunicaciones, manteniendo mecanismos de atención y comunicación dedicados. Asimismo, la revisión de nuestros objetivos contribuye a la mejora continua del Sistema Integrado de Gestión, buscando la excelencia en cada proyecto implementado.

Para cumplir con esto, **GRUPO ELECTRODATA S.A.C** se compromete a:

- Identificar, analizar y gestionar las necesidades e incidencias existentes en torno a la prestación de servicios, seguridad de la información y desarrollar los servicios necesarios para dar una adecuada respuesta a dichas necesidades, logrando la satisfacción de todos nuestros clientes.
- Identificar y cumplir con los requisitos legales aplicables a nuestra actividad, seguridad de la información, protección de datos y otros que la organización suscriba.
- Capacitar a nuestros colaboradores sobre temas relacionados a la calidad, servicio gestionado y seguridad de la información acorde a sus actividades mejorando su desempeño.
- Gestionar la continuidad del negocio, desarrollando planes con metodologías aplicables a la naturaleza del core business.
- Asegurar la confidencialidad, integridad y disponibilidad de los datos gestionados, principalmente aquella propiedad de nuestros clientes así como la protección de datos de carácter personal y la intimidad de las personas.
- Destinar los recursos y medios necesarios para desarrollar servicios con los niveles de calidad exigidos por los clientes. Prestando atención a la evolución tecnológica y a las nuevas tecnologías ponen a nuestra disposición, manteniendo un adecuado equilibrio entre costo y beneficio.

- Mejorar continuamente nuestros procesos, servicios y la eficacia del Sistema Integrado de Gestión, basado en las normas ISO 9001, ISO 27001 e ISO 20000, contando con el compromiso, participación, comunicación y aplicación de toda la empresa.

6.2. SEGURIDAD EN LOS PUESTOS DE TRABAJO

6.2.1. Control de acceso físico.

- Dentro del horario laboral establecido, cada usuario tiene la capacidad de acceder temporal o permanentemente a las instalaciones, salas y ubicaciones, previa realización de un proceso de identificación y acreditación.
- Se restringe el acceso a las instalaciones de Grupo Electrodata SAC únicamente al personal autorizado, con el fin de evitar el acceso físico no autorizado a la información y de otros activos asociados.
- Las directrices de acceso físico se declaran en la ficha de procesos de **ÁREAS SEGURAS (SSG-FP-01).**
- Los colaboradores de Grupo Electrodata SAC, deben cumplir la **Política de uso de fotocheck (GTH-D-06)** el cual se debe portar en un lugar visible, al ingresar, permanecer y desplazarse en las instalaciones de la empresa, clientes y proveedores.
- En situaciones excepcionales que demanden la presencia de un empleado fuera del horario regular de oficina, se requiere coordinación previa con la jefatura directa correspondiente. Toda solicitud para acceder en horarios no habituales debe ser consultada y aprobada previamente por la jefatura directiva pertinente.
- El personal que visite o sea destacado a las instalaciones del cliente deberá cumplir con lo establecido en sus políticas de acceso.

6.2.2. Ubicación y protección de equipos:

- Los equipos deben estar ubicados en zonas que se reduzca el acceso físico no autorizado, asegurando la confidencialidad de la información.
- Todas las impresoras deben ser protegidas y estar custodiadas durante su uso para evitar accesos no autorizados a la información que puedan generar. Por consiguiente, cada usuario con acceso a una impresora debe verificar que no queden documentos impresos que contengan información confidencial o secreta en las bandejas de salida. En el caso de impresoras compartidas, cada usuario debe retirar los documentos conforme vayan siendo impresos.

6.2.3. Ficheros temporales.

- Se consideran como ficheros temporales aquellos creados para atender una finalidad específica y de duración limitada. Estos pueden generarse extrayendo datos de ficheros preexistentes o como documentos adicionales o preparatorios. Es imperativo que los ficheros temporales sean eliminados una vez que hayan perdido su utilidad para los propósitos que motivaron su creación. La responsabilidad de borrar dichos ficheros recae en el usuario que los generó.

6.2.4. Normas de acceso y uso de Internet.

- Cada usuario **debe utilizar Internet exclusivamente para fines laborale**s, de acuerdo con las instrucciones impartidas por Grupo Electrodata.
- El usuario no debe modificar las configuraciones de los navegadores de los equipos, ni la activación de servidores o puertos sin autorización de la Gerencia de servicios gestionados o el área de NOC/SOC.
- Queda estrictamente prohibido acceder a imágenes o contenidos ilegales o contrarios a la moral y buenas costumbres. Además, se prohíbe el acceso, descarga o almacenamiento en cualquier medio de páginas que contengan este tipo de contenidos, así como de formatos de imágenes, sonido o vídeo que puedan ser perjudiciales.
- Se encuentra terminantemente prohibida la descarga de archivos susceptibles de contener virus o códigos maliciosos, así como la utilización de programas piratas o ilegales.
- No se permite el acceso a listas, servicios o foros de chat o sitios similares.
- No está permitido participar en actividades de propagación de cartas encadenadas, esquemas piramidales o similares.
- No está permitido difundir contenidos ilegales o contrarios a la moral y buenas costumbres.
- Se prohíbe efectuar ataques dirigidos para obstruir sistemas informáticos, o cualquier actividad que tenga por objeto la paralización del servicio por saturación de líneas, de la capacidad del servidor, o cualquiera similar.

6.3. POLÍTICA DE USO DE LA INFORMACIÓN

- **Propiedad intelectual e industrial.** Queda estrictamente prohibido el uso, reproducción, cesión, transformación o comunicación pública de cualquier tipo de obra protegida por los derechos de propiedad intelectual o industrial, así como la instalación de programas informáticos sin la correspondiente licencia.

En el marco de la propiedad intelectual e industrial, nos referimos a las invenciones, avances, proyectos, estrategias comerciales y signos distintivos pertenecientes al GRUPO ELECTRODATA.

- **Uso de la información.** En el desempeño de sus funciones, los usuarios pueden tener acceso a información dentro del ámbito de aplicación de Grupo Electrodata. Por consiguiente, están obligados a mantener la confidencialidad exigida por la empresa para el manejo de dicha información. Deben utilizarse exclusivamente en el marco de sus responsabilidades laborales y de acuerdo con las funciones inherentes a su cargo.

  Como usuario del Sistema Integrado de Gestión (SIG), y según las funciones asociadas a su cargo, cada usuario cuenta únicamente con acceso a los datos, carpetas, documentos y recursos necesarios para llevar a cabo sus responsabilidades laborales. Además, cada usuario será responsable de la custodia de la información y los datos almacenados en su estación de trabajo.

- **Soportes de información**. Está terminantemente prohibida la copia, extracción o distribución de información incluida en el SIG en cualquier tipo de soporte, salvo autorización expresa del Responsable del área o comité del SIG, dependiendo del documento.
- **Seguridad de documentos.** No está permitido extraer fuera de las sedes de Grupo Electrodata cualquier información para la que el usuario no esté autorizado expresamente por jefe de área o dirección.
- **Destrucción de los documentos al ser desechados.** Bajo autorización previa, en situaciones que requieran la destrucción de documentos por parte del personal, este proceso debe llevarse a cabo conforme a la ficha de proceso **SIG-FP-06 Gestión de Activos**. Se priorizará, cuando sea factible, la trituración de la documentación de papel previa eliminación.
- **Administración de base de datos.** Para proteger la integridad y confidencialidad de la información de las bases de datos, se considerará lo siguiente:
  - Cifrar los datos sensibles almacenados y en tránsito.
  - Limitar el acceso a las bases de datos únicamente a usuarios autorizados.
  - Implementar autenticación fuerte y políticas de auditoría a los logs de acceso a las bases de datos.
  - Realizar revisiones trimestrales de permisos y accesos de usuarios.

6.4. POLÍTICA DE PUESTO DE TRABAJO DESPEJADO Y PANTALLAS LIMPIAS

Para las computadoras desatendidas y pantallas limpias:

- Todos los usuarios son responsables de bloquear la sesión de su estación de trabajo en el momento en que se retiren de su puesto, la cual se podrá desbloquear solo con la contraseña del usuario.
- Sin perjuicio de lo anterior, y transcurridos 5 minutos de inactividad, el protector de pantalla del computador se debe activar en forma automática exigiendo, que la persona ingrese su usuario y clave para desbloquear el equipo.

Para los puestos de trabajo despejados:

- Mantener la estación de trabajo libre de documentos, despejada y limpia.
- Mantener la documentación guardada y clasificada según su importancia.
- Mantener la información restringida o confidencial bajo llave.
- No dejar papeles con las claves de acceso pegadas en la pantalla o en lugares de fácil acceso por terceras personas.

6.5. POLÍTICA DE ACCESO A INTERNET

- Aunque a todos los colaboradores con sistemas de información asignados se les otorga acceso a Internet desde sus estaciones de trabajo, Grupo Electrodata se reserva el derecho de retirar o restringir dicho acceso según sea necesario.
- El acceso a Internet será monitoreado por el Arquitecto de Red para asegurar el uso apropiado y el cumplimiento de las Políticas de Seguridad.
- La empresa ha implementado un control de navegación en Internet que limita el acceso a categorías inapropiadas para las actividades laborales regulares. Este control incluye la gestión del consumo de ancho de banda, el bloqueo de sitios con contenido pornográfico y la prohibición de acceder a contenidos relacionados con racismo, violencia, ocio, entretenimiento, entre otros.
- El acceso a Internet provisto a los usuarios es exclusivamente para las actividades relacionadas con las necesidades del puesto y función que desempeña.
- Todos los accesos a Internet tienen que ser realizados a través de los canales de acceso provistos por la empresa. En caso de necesitar una conexión especial a Internet, ésta tiene que ser notificada y aprobada por el Arquitecto de Red.
- Los colaboradores que cuentan con acceso a Internet están obligados a informar cualquier incidente de seguridad informática a la Mesa de Servicio

tan pronto como lo identifiquen.

- Se prohíbe el uso de aplicaciones, programas y/o herramientas que saturen los canales de comunicación o Internet, tales como gestores de descarga de archivos multimedia (audio y/o videos), P2P, Torrent, carga o descarga de juegos, entre otros.
- Se requiere que los invitados que ingresen a la empresa se conecten a la Red Guest para acceder a Internet.
- Los colaboradores con acceso a Internet en la empresa aceptan:
  - Sujetarse al monitoreo de las actividades realizadas en Internet.
  - Acatar la prohibición de acceso a páginas no autorizadas.
  - No transmitir archivos reservados o confidenciales sin autorización.
  - No descargar software sin la autorización de la Mesa de Servicio.
  - Utilizar Internet exclusivamente para el desempeño de sus funciones y no con fines personales.

6.6. POLÍTICA DE USO CORREO ELECTRÓNICO

- El usuario debe emplear el correo electrónico proporcionado por Grupo Electrodata exclusivamente para realizar las funciones asignadas, prohibiendo su uso con fines privados.
- El usuario es responsable de todas las actividades realizadas en sus cuentas de correo y respectivos buzones.
- No debe permitir la utilización del mismo a personas no autorizadas ni enviar mensajes a personas que no deseen recibirlo.
- No está permitido participar en actividades de propagación de correos en cadena, esquemas piramidales o similares.
- No está permitido difundir contenidos ilegales o contrarios a la moral y buenas costumbres.
- Se prohíbe efectuar ataques para obstruir sistemas informáticos dirigidos a un usuario o al propio sistema de correos, o cualquier actividad que tenga por objeto la paralización del servicio por saturación de líneas, de la capacidad del servidor, o cualquiera similar.
- Ningún mensaje de correo electrónico es considerado como privado, por lo que Grupo Electrodata podrá ordenar la revisión, sin previo aviso, de los mensajes de correo electrónico corporativo, con el fin de comprobar el cumplimiento de las normas establecidas y prevenir actividades que puedan afectarla.

- Cualquier fichero que introduzca un usuario en la red corporativa o en su terminal a través de mensajes de correo electrónico que provenga de redes

externas debe cumplir con los requisitos establecidos en estas normas y, en especial, las referidas a propiedad intelectual e industrial y a control de virus.

- Se establece como requisito que todas las cuentas de correo electrónico de la empresa tengan implementadas una doble autenticación, un proceso de seguridad que requiere la verificación de dos métodos distintos para acceder a la cuenta. Esto refuerza la protección de las cuentas y contribuye a prevenir accesos no autorizados.
- Mesa de Servicio asignará una cuenta de correo electrónico. El formato de su dirección de correo electrónico será **1ERASIGLADELNOMBREAPELLIDO@electrodata.com.pe**.
- Existe un formato para que puedas poner en el pie del correo tus datos de contacto y profesionales. El texto sería el siguiente:

6.7. POLÍTICA DE CONTROL DE ACCESOS, IDENTIFICACIÓN Y AUTENTIFICACIÓN DE USUARIOS

Todos los trabajadores de Grupo Electrodata deben cumplir con lo estipulado en cada uno de los siguientes aspectos:

6.7.1. Control de acceso a datos.

En el ejercicio de sus funciones y al entrar en contacto con información sensible de Grupo Electrodata y la de sus clientes, el usuario de los sistemas de información debe respetar rigurosamente su confidencialidad, utilizándose exclusivamente en el ámbito de sus responsabilidades laborales y de acuerdo con las tareas asignadas a su cargo. Además, como usuario de los sistemas informáticos, tendrá acceso exclusivo a los datos y recursos necesarios para llevar a cabo sus funciones, siendo responsable de la custodia de la información y de los datos de acceso a su ordenador.

- Está prohibido intentar ingresar a la infraestructura tecnológica con la cuenta de usuario de otro colaborador.

- Toda la información contenida en los sistemas informáticos es de GRUPO ELECTRODATA.

6.7.2. Sistema de control de acceso.

- A cada usuario se le asignará un nombre de usuario y una contraseña para acceder a los archivos informáticos, responsabilizándose de su custodia. En caso de detectar o sospechar el uso indebido de sus claves por personas no autorizadas, se requiere que notifique la incidencia de inmediato a Mesa de Servicio y al Comité del Sistema Integrado de Gestión (SIG) para su atención y cambio inmediato de las claves afectadas.

  Con estos datos podrá acceder a:
  - ❖ Cuenta de correo electrónico
  - ❖ Sistema documental

- Usted será el responsable de la custodia y buen uso de los datos de acceso.
- Las contraseñas de acceso se sustituirán periódicamente, siendo el área de Mesa de Servicio el encargado de la modificación de las directivas de grupo establecidas en el Directorio Activo.
- La sustitución de contraseñas se efectuará automáticamente y el usuario será el único conocedor de la misma.
- El nivel de acceso a un sistema de información se otorgará de acuerdo con:
  - ○ La clasificación de la información.
  - ○ Funciones del usuario.
  - ○ Perfiles de acceso estandarizados.
  - ○ Pedido, autorización y administración de acceso.
- El supervisor, jefatura inmediata, o la persona que se designe será el responsable de monitorizar los accesos y roles de su equipo de trabajo, verificando periódicamente que sean los que les corresponde de acuerdo con las funciones que desempeñan.

6.7.3. Monitorización.

- En aras de la seguridad, el sistema, los servicios y la red que lo respaldan pueden utilizar programas de monitorización con el fin de detectar usos y accesos no autorizados. Al emplear estos sistemas, el usuario otorga su consentimiento para la utilización de dichos medios de monitorización.

- Las siguientes actividades se encuentran expresamente prohibidas:
  - ❖ Compartir o facilitar el identificador de usuario y la clave de acceso facilitados por Grupo Electrodata a otra persona física, incluido el personal de la propia empresa. En caso de incumplimiento de esta prohibición, el usuario será el único responsable de los actos realizados por la persona física que utilice de forma no autorizada el identificador del usuario.
  - ❖ Falsear los registros del sistema.
  - ❖ Intentar descifrar las claves, sistemas o algoritmos de cifrado o cualquier otro elemento de seguridad.

6.7.4. Responsabilidades del usuario en relación a la información de autenticación:

- Asegurar la confidencialidad de las contraseñas. La información secreta de autenticación personal NO DEBE ser compartida con nadie.
- Las credenciales de acceso no deben almacenarse
- En caso de verse comprometida la información de autenticación, esta se debe cambiar inmediatamente tras recibir notificación de compromiso.
- No se deben utilizar las mismas contraseñas en distintos servicios y/o sistemas de información.
- Los usuarios deben cambiar sus contraseñas en el primer inicio de sesión o cuando sea necesario.
- Las cuentas o identidades compartidas están permitidas siempre y cuando se cuente con aprobación de la jefatura o gerencia inmediata, quienes serán los responsables de controlar y cambiar las contraseñas periódicamente o cuando sea necesario, es decir, después de un incidente de seguridad, cese o cambio de puesto.

6.7.5. Gestión de usuarios privilegiados

Para controlar de manera adecuada las funciones de los usuarios con acceso privilegiado o de administración se considerará:

- Utilizar cuentas separadas para tareas regulares y tareas de administración de sistema.
- Monitorear las actividades realizadas por los usuarios con acceso privilegiado o de administración por medio de los logs de administración.
- Realizar revisiones trimestrales de permisos y accesos de usuario.

6.8. POLÍTICA DE USO ACEPTABLE DE LA INFORMACIÓN Y ACTIVOS ASOCIADOS

6.8.1. USO ACEPTABLE

Es un deber de los empleados conocer, respetar y cumplir las políticas para el uso aceptable y procedimientos para manejo de la información y otros activos establecidos por Grupo Electrodata.

- Se deberán proteger físicamente los dispositivos de usuario final contra el robo, sobre todo en automóviles, habitaciones de hotel, centros de formación y reuniones, cafeterías, etc. No se deberá dejar solo, o sin vigilar, un equipo que contenga información importante, sensible o crítica.
- El personal de GRUPO ELECTRODATA es responsable de preservar y tratar adecuadamente los recursos informáticos asignados. En el caso de que el usuario decida NO utilizar los equipos asignados y opte por emplear sus propios dispositivos, se le solicita que se comunique con Mesa de Servicio para verificar si cumple con los requisitos mínimos de seguridad para el tratamiento de la información que gestionará según la naturaleza de sus funciones, posterior a la verificación y aprobación se procede con la devolución inmediata de los equipos asignados.
- Los equipos y sistemas de información de GRUPO ELECTRODATA y/o los del cliente deben ser utilizados **exclusivamente** con fines laborales.
- No se permite el uso de los activos de información para fines personales, ilegales o no autorizados, incluyendo la distribución de información confidencial sin el debido permiso.
- El tratamiento de los recursos asignados por GRUPO ELECTRODATA y los de sus clientes se realizarán acorde a la Ley de protección de datos y las políticas establecidas en el presente documento, y/o por el propietario de la información. Informar a la brevedad al responsable del sistema de cualquier supuesto incidente debilidad, o violación de seguridad, de tal manera de ejecutar las actividades para la investigación y eliminación de éstos.
- Una vez finalizados los procedimientos de identificación y autorización de usuario, es esencial que los ordenadores y terminales no se dejen desatendidos.
- Es un deber de los empleados utilizar el servicio de correo electrónico y redes sociales corporativas de manera adecuada y responsable.
- Mantener en secreto y cambiar periódicamente las contraseñas de los usuarios de Grupo Electrodata.

- Depurar periódicamente el contenido de las carpetas del correo electrónico. Esto para ayudar a evitar la retención prolongada de mensajes, mitigando posibles congestiones o bloqueos en el sistema.
- Únicamente se instalarán en los equipos informáticos aquellos software y aplicaciones que hayan sido previamente aprobados por su jefatura y/o el cliente, y para los cuales se cuente con las licencias correspondientes.
- Todos los colaboradores que utilicen los sistemas de procesamiento de la información o los recursos de la empresa, deberán actuar basados en las normas establecidas en la política de seguridad de la información.
- Ante robo, pérdida, uso indebido, deterioro o destrucción de activos, información o documentos de la empresa, los colaboradores deben informar de inmediato al Grupo Electrodata. Además, deben presentar la denuncia correspondiente a la autoridad policial local.
- En caso de presentar fallas o incidentes con el equipo asignado, este debe ser reportado a Mesa de Servicio para su respectivo diagnóstico. Mesa de Servicio asignará un equipo de préstamo hasta la devolución o reposición del equipo, el cuidado del equipo en préstamo es responsabilidad del colaborador. La custodia y transferencia de la información del usuario en el equipo prestado son responsabilidad del colaborador, quien deberá cargar una copia de seguridad en su cuenta de Google Drive. En caso la copia de seguridad sea muy pesada y de no contar con espacio disponible, el colaborador deberá contactar a Mesa de Servicio para el soporte correspondiente.

6.8.2. USO INACEPTABLE

Está estrictamente prohibido:

- Utilizar los recursos de la empresa para ejecutar juegos de cualquier índole.
- Ejecutar actividades de minado de criptomonedas en los equipos de la empresa y/o los de sus clientes.
- Compartir información confidencial de la empresa o clientes con terceros sin la debida autorización.
- Acceder, modificar o eliminar información/o configuraciones sin los permisos correspondientes.
- Instalar software no autorizado en los sistemas de la empresa que puedan poner en riesgo la seguridad de la información.
- Utilizar los activos de información de manera que puedan perjudicar la reputación de la empresa o sus clientes.
- Eludir los controles de seguridad establecidos.

Estas actividades darán lugar a la apertura de un expediente disciplinario para la investigación y determinación de sanciones disciplinarias, **según lo establecido en los capítulos *XIX. Medidas disciplinarias y XX.Procedimiento disciplinario del Reglamento interno de Trabajo (GTH-D-01)***, incluyendo la terminación del contrato o empleo, según su gravedad. Por ende GRUPO ELECTRODATA se reserva el derecho de monitorear el uso de sus activos de información para garantizar el cumplimiento de esta política.

6.9. POLÍTICA DE USO DE DISPOSITIVOS DE USUARIO FINAL

El objetivo de esta política es establecer los lineamientos para el uso adecuado y seguro de los dispositivos finales de los usuarios que se utilicen para acceder a los sistemas, datos y recursos de GRUPO ELECTRODATA y/o de sus clientes.

Para asegurar que la información no esté comprometida, será obligatorio adoptar las siguientes medidas de seguridad:

- Cerrar las sesiones activas de los sistemas de información críticos cuando ya no sean necesarios, tales como: SIDIGE, ITMS, BITRIX, VPN, Inconcert u otra plataforma del cliente, que sea considerada bajo este nivel de clasificación.
- Proteger los dispositivos finales de los usuarios contra el uso no autorizado mediante contraseñas robustas, según la definición de criterios de complejidad de credenciales establecidas en **MDS-FP-05 CONTROL DE ACCESO** o lo establecido en las políticas de autenticación del cliente.
- Utilizar dispositivos con especial cuidado en lugares públicos, oficinas abiertas, lugares de reunión y otras áreas no protegidas. Evita acceder a información confidencial en lugares donde personal no autorizado pueda leer desde atrás.
- Cuando la información sea altamente confidencial, se usarán técnicas de encriptación para evitar el acceso no autorizado o la divulgación de la información almacenada.
- Instalar y mantener al día antivirus y/u otros procedimientos contra software malicioso actualizado y configurado para realizar análisis automáticos regulares.
- Aplicar parches de seguridad de manera regular para el sistema operativo y aplicaciones críticas, preferiblemente de manera automática.
- Configurar políticas de uso para dispositivos externos como USB, permitiendo su uso solo a usuarios autorizados.
- La instalación de software estará restringida solo a usuarios administradores autorizados para evitar la instalación de software no aprobado en dispositivos de usuario final.

- Asegurar que la información sensible se cargue en Google Drive para asegurar una copia de seguridad recuperable en caso de pérdida o robo del dispositivo.
- Es fundamental brindar especial atención a la protección de los dispositivos de usuario final conectados a las redes de la empresa o de los clientes. Los accesos remotos a la información de la empresa solo deben realizarse a través de mecanismos de seguridad de control de accesos autorizados, y después de conseguir una identificación y autenticación exitosas.
- El usuario NO DEBE modificar las configuraciones de seguridad de los dispositivos de usuario final establecidas en la ficha de procesos de **SEGURIDAD DE LOS EQUIPOS (SSG-FP-02)**
- Se prohíbe la modificación y alteración de las partes del sistema operativo restringidas por el fabricante , vulnerando los mecanismos de protección.

Los trabajadores encargados de los dispositivos remotos son los máximos responsables de su seguridad y como tales deberán asumir las sanciones impuestas ante un posible incidente de seguridad.

6.10. POLÍTICA DE TELETRABAJO

- El periodo de trabajo remoto debe ser autorizado por la Gerencia General o cada Gerencia de unidad, indicando modalidad, turnos, horarios y tiempo.
- Es posible el acceso a SIDIGE, File Server y servicios operativos usando el VPN. Los usuarios, pedirán acceso por Service Desk mediante correo y el administrador de red dará los permisos necesarios.
- El uso de la VPN es para fines de trabajo exclusivos de Electrodata, no está permitido el uso de los recursos e información fuera del ámbito laboral y de negocio.
- El tiempo de trabajo remoto será supervisado por cada jefatura/gerencia quienes serán los responsables del rendimiento de los equipos de trabajo de la empresa.
- Se ha autorizado para las reuniones de trabajo el uso de los recursos de Zoom y Google Meet, pudiendo ser grabadas o monitoreadas, según sea el caso.
- Los horarios de trabajo remoto serán acordados por cada supervisor, jefatura o gerencia según sea el caso y la flexibilidad o compensación será de mutuo acuerdo entre el empleador y el trabajador.
- No está permitido la extracción o uso no adecuado de la información de la empresa durante el trabajo remoto, siendo responsabilidad de cada usuario la protección y confidencialidad de la información.
- El reporte de incidentes o vulnerabilidades durante el trabajo remoto será comunicado a Service Desk mediante correo o teléfono para su atención

oportuna. Es responsabilidad de cada usuario la inmediata alerta y comunicación.

- Durante el periodo de trabajo remoto, el usuario es responsable de mantener y cuidar los activos TI asignados acorde a la POLÍTICA de Uso Aceptable de Activos.
- Cualquier dispositivo que no sea propiedad de Electrodata y que pueda conectarse a su red debe recibir la aprobación previa del Director de Ingeniería y Servicios.
- Los usuarios dentro del periodo de trabajo remoto no están excluidos de las auditorías internas, externas o monitoreos por seguridad.
- El incumplimiento de los requerimientos exigidos por esta POLÍTICA y los casos de pérdida de información serán evaluados y podrán tener como consecuencia acciones disciplinarias según el GTH-D-01 Reglamento Interno de Trabajo.
- Con el objetivo de verificar el cumplimiento de estas POLÍTICAS, GRUPO ELECTRODATA podrá llevar a cabo auditorías a los trabajadores. Estas auditorías incluirán la revisión de toda la información y documentación almacenada en medios físicos y digitales de GRUPO ELECTRODATA, abarcando archivos, carpetas, correo electrónico, equipo informático asignado, registros de navegación, y cualquier otro componente necesario en el marco de la Auditoría.

6.11. ACTIVOS DE INFORMACIÓN PROPORCIONADA A TERCEROS

- El acceso de terceros a la información de la empresa solo será permitido con la autorización previa del Director de Ingeniería y Servicios o del Gerente de Minería.
- Cuando se trata de proporcionar información que involucra aspectos tecnológicos, es indispensable obtener la aprobación anticipada de Mesa de Servicios. Ellos se encargan de validar los riesgos asociados con la seguridad de la información solicitada, garantizando así un proceso seguro y eficiente.
- Las solicitudes de terceros de información registral, informes financieros, documentos de POLÍTICA internas, actas, manuales, estudios económicos, procedimientos, y, en general, todo tipo de información, se encuentran amparados por los lineamientos de la POLÍTICA de Seguridad de la Información y bajo previa autorización de cada Jefatura o responsable para la comunicación al tercero.
- La información concerniente a las medidas de seguridad, sistemas de procesamiento de datos y redes es de carácter confidencial. Su divulgación a

usuarios no autorizados está prohibida, a menos que se cuente con la expresa autorización del Director de Ingeniería y Servicios.

6.12. POLÍTICA DEL CENTRO DE DATOS

- Los Centros de Datos están clasificados como áreas de acceso restringido. Solo se podrá ingresar si cuenta con la autorización del Gerente de Calidad y Proyectos.
- Es responsabilidad del Director de Ingeniería y Servicios, asegurar que todos los recursos de computación y comunicaciones, cuenten con planes de mantenimiento preventivo y/o correctivo debidamente contratados.
- Es responsabilidad del Director de Ingeniería y Servicios, que los Centros de Datos cuenten con registro y monitoreo de control de acceso físico, que puedan ser auditados. En este caso la bitácora de acceso y control de la llave manual para el ingreso serán los mecanismos de accesos físicos.
- Dentro del Centro de Datos, queda estrictamente prohibido llevar a cabo actividades como fumar, comer, beber, jugar, descansar, entre otras.
- Los racks deben estar cerrados y el acceso al Centro de Datos controlado por Mesa de Servicio.
- Cualquier acceso al Centro de Datos será monitoreado por una cámara CCTV durante el periodo de la actividad.
- El personal que ingrese al data center deberá completar el formulario de "Control de orden y limpieza Data Center" (https://forms.gle/abXXnXtkJmDKEwKe9) para registrar el estado en el que lo encuentra y deja el centro de datos. Esto a fin de controlar el acceso y el orden y limpieza del mismo.
- El Data Center debe mantenerse limpio y ordenado en todo momento. Todo el personal que ingrese a realizar trabajos en el mismo deberá remover sus desechos y cajas vacías antes de salir de las instalaciones.
- Al iniciar y/o finalizar cualquier tarea en el Data Center, es imperativo que el personal verifique la correcta instalación y orden de todos los cables en sus respectivos gabinetes. Además, deben asegurarse de que todas las puertas estén cerradas de manera adecuada.
- Dentro del Centro de Datos está prohibido dejar cajas de cartón o equipos apilados.
- Las condiciones ambientales (temperatura, humedad) serán controladas y monitorizadas.
- Se debe gestionar una solicitud de Cambio cada vez que se realice una modificación al Centro de Datos.

6.13. POLÍTICA DE GESTIÓN DEL DIRECTORIO ACTIVO

El Directorio Activo será administrado por Mesa de Servicio y autorizado por el Director de ingeniería y servicios, la configuración estándar es dada por el Gerente de ingeniería
Todas las políticas relacionadas a la administración del Directorio Activo serán aprobadas por el Director de ingeniería y servicios aplicada acordes a la necesidad de la empresa en la administración centralizada.

Las políticas incluyen:

- Configurar políticas de contraseñas seguras y forzar el cambios de contraseñas periódicamente.
- Deshabilitar cuentas de usuarios inactivos automáticamente tras un periodo de tiempo definido
- Implementar la replicación segura y controlada de controladores de dominio.
    - Monitorear y auditar los cambios críticos del directorio activo (AD).

Estas políticas son aplicadas para determinar:

- Software Setting: Publicar o asignar aplicación a equipos dentro de un dominio o usuarios.
- Security Setting: Cambios de la seguridad del sistema operativo.
- Plantillas Administrativas: Aplicación de las configuraciones que son guardadas en el registro del equipo, incluyen aquellas que controlan el funcionamiento y configuración de los componentes utilizados por las políticas.

6.14. GESTIÓN DE INCIDENCIAS

Debe reportar cualquier debilidad, fallo y/o amenaza observada o sospechada, respecto a la seguridad de los sistemas, datos, programas o servicios de Grupo Electrodata, y aquellas incidencias producidas en la realización de sus tareas enviando un correo electrónico a servicedesk@electrodata.com.pe.

La gestión de incidentes de seguridad de la información será atendida según lo establecido en la ficha de procesos de **Gestión de incidentes y requerimientos (MDS-FP-01).**

6.15. POLÍTICA DE CIFRADO Y CRIPTOGRAFÍA

- El área de Desarrollo debe garantizar la privacidad de la información que se respalda en medios de almacenamiento secundarios, sobre los aplicativos y software de la empresa (ITMS, SIDIGE, y otras BD). Por lo tanto, se recomienda cifrar dicha información para mayor seguridad.
- En el desarrollo de aplicativos o software se debe considerar estándares para la aplicación de controles criptográficos.
- Los desarrolladores deben cifrar la información reservada o restringida y certificar la confiabilidad de los sistemas de almacenamiento de dicha información.
- Es responsabilidad de los desarrolladores garantizar que los controles criptográficos de los sistemas construidos cumplan con los requisitos técnicos de los clientes, especialmente en lo que respecta al cifrado o encriptamiento, en caso de que sea aplicable.
- La información que por sus características de integridad o confidencialidad deba ser protegidas, debe estar en formatos que protejan su modificación o confidencialidad (contraseñas o cifrado).
- El equipo de Tecnologías de información se encarga de realizar el cifrado del backup de la información del FileServer con una contraseña, la cual tiene visibilidad los responsable de mesa de servicio y TI.
- El equipo de desarrollo utiliza un software de protección de claves criptográficas en la nube para el backup del sistema ITMS, al cual tiene acceso el Gerente de Minería y el equipo de desarrollo.

6.16. POLÍTICA DE DESARROLLO SEGURO

Las POLÍTICAS mencionadas aplican a las aplicaciones de desarrollo propio de la empresa (ITMS) y los servicios de desarrollo con los clientes:

- La empresa se compromete a garantizar que tanto el desarrollo interno como externo de los sistemas de información cumplan con los requisitos de seguridad establecidos, así como con las buenas prácticas para el desarrollo seguro de aplicativos. Además, se seguirán metodologías para la realización de pruebas de aceptación y seguridad en el software desarrollado. Se velará también por asegurar que todo software, ya sea desarrollado internamente o adquirido externamente, cuente con el nivel de soporte necesario.
- El área de Desarrollo, en conjunto con los propietarios de los aplicativos, debe realizar las pruebas necesarias para asegurar que los sistemas de información

desarrollados cumplen con los requerimientos de seguridad establecidos antes del paso a producción.

- El área de Desarrollo, en conjunto con los propietarios de los aplicativos, debe realizar las pruebas por entrega de funcionalidades nuevas, por ajustes de funcionalidad o por cambios sobre la plataforma tecnológica en la cual funcionan los aplicativos.
- El área de Desarrollo, en conjunto con los propietarios de los aplicativos, debe aprobar las migraciones entre los ambientes de desarrollo, pruebas y producción de sistemas de información nuevos y de cambios o nuevas funcionalidades.
- El área de Desarrollo, debe implantar los controles necesarios para asegurar que las migraciones entre los ambientes de desarrollo, pruebas y producción han sido aprobadas, de acuerdo con el procedimiento de control de cambios en caso apliquen.
- El área de Desarrollo, debe contar con sistemas de control de versiones para administrar los cambios de los sistemas de información.
- El área de Desarrollo, debe asegurarse que los sistemas de información adquiridos o desarrollados por terceros, cuenten con un acuerdo de licenciamiento el cual debe especificar las condiciones de uso del software y los derechos de propiedad intelectual.
- El área de Desarrollo, debe generar metodologías para la realización de pruebas al software desarrollado, que contengan pautas para la selección de escenarios, niveles, tipos, datos de pruebas y sugerencias de documentación.
- El área de Desarrollo, debe asegurar que la plataforma tecnológica, las herramientas de desarrollo y los componentes de cada sistema de información estén actualizados con todos los parches generados para las versiones en uso y que estén ejecutando la última versión aprobada del sistema.
- El área de Desarrollo, debe incluir dentro del procedimiento y los controles de gestión de cambios, los cambios en el software aplicativo y los sistemas de información.
- Los desarrolladores de los sistemas de información deben considerar las buenas prácticas y lineamientos de desarrollo seguro durante el ciclo de vida de los mismos, pasando desde el diseño hasta la puesta en marcha.
- Los desarrolladores deben proporcionar un nivel adecuado de soporte para solucionar los problemas que se presenten en el aplicativo; dicho soporte debe contemplar tiempos de respuesta aceptables.
- Los desarrolladores deben construir los aplicativos de tal manera que efectúen las validaciones de datos de entrada y la generación de los datos de salida de

manera confiable, utilizando rutinas de validación centralizadas y estandarizadas.

- Los desarrolladores deben asegurar que los sistemas de información construidos validen la información suministrada por los usuarios antes de procesarla, teniendo en cuenta aspectos como: Rangos válidos, Longitud, Listas de caracteres aceptados, caracteres considerados peligrosos, caracteres de alteración de rutas.
- Los desarrolladores deben suministrar opciones de desconexión o cierre de sesión de los aplicativos (logout) que permitan terminar completamente con la sesión o conexión asociada, las cuales deben encontrarse disponibles en todas las páginas protegidas por autenticación.
- Los desarrolladores deben asegurar que los aplicativos proporcionen la mínima información de la sesión establecida, almacenada en cookies y complementos.
- Los desarrolladores deben asegurarse de que la información confidencial, como detalles del sistema, identificadores de sesión o datos de cuentas de usuarios, no se revele en respuestas de error. Además, es fundamental que implementen mensajes de error genéricos.
- Los desarrolladores deben remover todas las funcionalidades y archivos que no sean necesarios para los aplicativos, previo a la puesta en producción.
- Los desarrolladores deben prevenir la revelación de la estructura de directorios de los sistemas de información construidos.
- Los desarrolladores deben remover información innecesaria en los encabezados de respuesta que se refieran a los sistemas operativos y versiones del software utilizado.
- Los desarrolladores deben evitar incluir las cadenas de conexión a las bases de datos en el código de los aplicativos. Dichas cadenas de conexión deben estar en archivos de configuración independientes, los cuales se recomienda que estén cifrados.
- Los desarrolladores deben desarrollar los controles necesarios para la transferencia de archivos, como:
    - Exigir autenticación.
    - Almacenar los archivos transferidos en repositorios destinados para este fin o en bases de datos.
    - Eliminar privilegios de ejecución a los archivos transferidos.
    - Asegurar que dichos archivos sólo tengan privilegios de lectura.
- Los desarrolladores deben proteger el código fuente de las aplicaciones construidas, de tal forma de que no pueda ser descargado ni modificado por los usuarios.

- Los desarrolladores deben asegurar que no se permite que los aplicativos desarrollados ejecuten comandos directamente en el sistema operativo.

6.17. ACEPTACIÓN DE FUNCIONES Y RESPONSABILIDADES

Todo el personal afectado por el alcance (interno, externos) debe de conocer, aceptar y cumplir tanto la POLÍTICA de seguridad del sistema de gestión de seguridad de la información como lo indicado en este procedimiento. En este sentido, se proporcionará una copia de esta guía para su firma, junto con los compromisos adicionales de confidencialidad y no competencia que puedan ser necesarios en cada situación particular.

Como personal de Grupo Electrodata tiene las siguientes obligaciones:

- Cumplir estrictamente las obligaciones detalladas sobre seguridad de la información en este documento, así como de las instrucciones proporcionadas a través de la herramienta de gestión documental de Grupo Electrodata.
- Respetar la confidencialidad de información manejada por Grupo Electrodata, evitando su envío o difusión al exterior o a personas no autorizadas, por cualquier medio o soporte.
- Guardar la máxima reserva y no divulgar, directa o indirectamente, por sí o por personas o entidades interpuestas, los datos, documentos, metodologías, claves, contraseñas, programas y demás información a la que tengan acceso durante su relación laboral con Grupo Electrodata.
- Utilizar o poseer únicamente los materiales o información de Grupo Electrodata que sean precisos para el ejercicio de sus funciones, y dentro del ámbito de su relación laboral.
- Al concluir la relación laboral, es obligatorio devolver a Grupo Electrodata cualquier tipo de datos o información a los que se haya tenido acceso, ya sea por cualquier medio o soporte, durante el desempeño de las funciones laborales.
- Utilizar el correo electrónico conforme a las normas de Grupo Electrodata.
- Cumplir las normas de Grupo Electrodata para el acceso a Internet.
- No comunicar o divulgar los identificadores de usuario y las claves de acceso. En caso de incidentes relacionados, se debe informar oportunamente sobre cualquier eventualidad.
- No acceder a recursos, programas, datos o informaciones a las que no esté expresamente autorizado, por ser precisas para el ejercicio de sus funciones.

- No realizar copias de información en cualquier tipo de soporte sin la autorización previa del responsable, ni utilizarlas para fines ajenos a los de su trabajo.
- No dañar, alterar, destruir o inutilizar los datos, programas o documentos de Grupo Electrodata.
- Abstenerse de intentar descifrar las claves, sistemas o algoritmos de cifrado o cualquier otro elemento de seguridad que intervenga en los procesos telemáticos de Grupo Electrodata.
- Informar de inmediato cualquier incidente de Seguridad de Información, incluyendo Vulnerabilidades, Ciber Incidentes o pérdida de información en formato digital, a Mesa de Servicio y al comité del SIG. La notificación debe hacerse el mismo día del conocimiento del hecho, comunicándose a Mesa de Servicio (servicedesk@electrodata.com.pe) y a su superior inmediato.
- Utilizar adecuadamente la red corporativa, los recursos y sistemas de Grupo Electrodata, sin introducir programas no autorizados, programas ilegales, virus, macros o cualquier otro dispositivo que puedan causar alteraciones en los mismos.
- Abstenerse de crear carpetas en recursos de Grupo Electrodata con datos personales sin la previa autorización del jefe del área.
- Impedir la acumulación de información sobre datos personales, de forma que se evite la posibilidad de realizar valoraciones sobre la personalidad de los titulares de los datos.
- Cualquier otra obligación que resulte de la POLÍTICA de seguridad de Grupo Electrodata, plasmada en el Documento de Seguridad, las Instrucciones de Seguridad, sus fichas de procesos de actuación y la normativa vigente.

6.18. CONDUCTA EN EL ENTORNO DE TRABAJO

Como personal de GRUPO ELECTRODATA tiene las siguientes obligaciones:

- Cumplir con sus obligaciones de forma profesional, responsable y celosa, procurando la excelencia de desempeño.
- Facilitar a sus superiores información veraz y explicar con total transparencia sus decisiones y comportamientos profesionales.
- Proteger el patrimonio de Grupo Electrodata utilizándolo sólo en la ejecución de los procesos de negocio y asegurando su uso eficiente.
- Informar de cualquier comportamiento que esté en conflicto con este manual de buenas prácticas y código de conducta. Se garantiza la confidencialidad y

protección jurídica de quien informa, de acuerdo con la reglamentación propia, y un trato justo a sobre quién se informa.

- Respetar e incentivar los valores de Grupo Electrodata promoviendo la cooperación, la responsabilidad individual y aceptando la diversidad.
- Procurar desarrollar y actualizar de forma continua sus conocimientos y competencias y sacar el mejor provecho de las acciones de formación promovidas por Grupo Electrodata.

6.19. SEGURIDAD DE LA INFORMACIÓN DE BANCO DE DATOS PERSONALES

- Limitar el acceso a la base de datos y a las aplicaciones que la utilizan únicamente personal autorizado, permitiendo solo el acceso a la información necesaria para el desempeño de sus funciones
- Cifrar y proteger los datos personales sensibles, como información financiera, de salud u otros datos críticos, tanto en reposo (cuando están almacenados) como en tránsito, mediante el uso de protocolos seguros como TLS/SS
- Realizar backups diarios y probar los procedimientos de restauración de forma trimestral para asegurar una recuperación rápida y efectiva ante pérdidas o ataques.
- Notificar a la Oficial de Datos Personales (ODP) cualquier Incidente de Seguridad (destrucción, pérdida, alteración o exposición no autorizada de datos) dentro de las 48 horas siguientes a su detección.
- Es obligatorio elaborar y mantener actualizado un documento que detalle las medidas de seguridad implementadas, los roles y responsabilidades, los riesgos identificados y los procedimientos establecidos para la protección de la información persona

7. CONSECUENCIAS DEL INCUMPLIMIENTO

El personal, tanto interno como externo, que no siga las directrices establecidas en las políticas, normas, procedimientos u otros documentos del presente Sistema de Gestión que sean aplicables a su puesto de trabajo, podría comprometer la seguridad de la información y los sistemas involucrados en su tratamiento diario.

Por ello, en caso de incumplimiento grave de cualquiera aspecto contenido en los citados documentos, el trabajador podrá ser objeto de la apertura de un expediente disciplinario en los términos y condiciones establecidos por Grupo Electrodata de acuerdo a los capítulos **XIX.Medidas disciplinarias y XX.Procedimiento disciplinario del GTH-D-01 Reglamento Interno de Trabajo.**

8. CONTROL DE CAMBIOS

Revisión	Fecha	Cambio o Modificación	Sección
12	05/01/2026	● Se incluye el apartado de seguridad de la información de banco de datos personales.	6.19
11	18/10/2024	● Se actualiza objetivo ● Se incluye en el alcance lo siguiente: ○ La presente política aplica para el personal que realice el tratamiento de activos de información de GRUPO ELECTRODATA y de sus clientes. ○ El personal autorizado para el tratamiento de activos de información del cliente debe adherirse adicionalmente a las políticas establecidas por el mismo, con el fin de mantener la confidencialidad, integridad y disponibilidad de los recursos asignados. ● Se actualizan referencias según ISO 27001:2022 ● Se incluyen definiciones: Activos de información y Dispositivos de usuario final. ● Se incluye política de Administración de bases de datos ● Se actualiza la política de seguridad en los puestos de trabajo, donde se incluye la Política de uso de fotochecks. ● Se reemplaza autorización de SIG por área NOC SOC: *El usuario no debe modificar las configuraciones de los navegadores de los equipos, ni la activación de servidores o puertos sin autorización de la Gerencia de servicios gestionados o el área de NOC/SOC.* ● Se actualizan Políticas de control de acceso, identificación y autenticación de usuario, incluyendo adicionalmente responsabilidades del usuario en relación a la información de autenticación. ● Se actualiza Políticas de uso aceptable de la información y activos asociados., segmentando uso aceptable e inaceptable ● Se incluyen los capítulos de XIX.Medidas disciplinarias y XX.Procedimiento disciplinario del GTH-D-01 Reglamento Interno de Trabajo	Objetivo Alcance Referencias Definiciones 6.3 6.4 6.2.4 6.7 6.8 7
10	13/02/2024	● Se cambia el nombre del puesto del Gerente de Operaciones por el de Director de Ingeniería y Servicios. ● Se elimina la máquina de fax. ● Se añade la definición de Propiedad Intelectual e Industrial. ● Se elimina el uso del módem portátil. ● Se añade la obligatoriedad de la doble verificación.	Todo el documento 5.2 5.3 5.5 5.6

		• Se incorpora a las plataformas de redes sociales corporativas para asegurar su buen uso. • Se incluye el procedimiento a seguir en caso de robo o pérdida de activos, información o documentación de la empresa. • Se establece la prohibición de llevar a cabo cualquier actividad de minado de criptomonedas en los activos de la empresa. • Se añade los servicios operativos para que sean accesibles mediante VPN. • Se incluye la evaluación de cada caso de incumplimiento, haciendo referencia al GTH-D-01 Reglamento Interno de Trabajo . • Se incorpora el proceso de auditoría para garantizar el cumplimiento de las POLÍTICAS. • Se modifican los sistemas por registro y monitoreo de control de acceso físico. • Se actualiza el cargo de Gerente de Operaciones a Gerente de Calidad y Proyectos. • Se explica mejor el procedimiento de comunicar cualquier incidencia de Seguridad de Información. • Se modifica ficheros por carpetas. • Se añade el código del Reglamento Interno de Trabajo.	5.8 5.8 5.8 5.10 5.10 5.10 5.12 5.13 5.17 5.17 5.19
09	01/02/2023	Se actualiza la firma del correo corporativo. Se actualiza el cargo de Gerencia de ECC a Gerencia de Minería	5.11 ; 5.15
08	20/06/2022	Se actualiza la POLÍTICA de centro de datos	5.12
07	07/03/2022	Se incluyen roles y responsabilidades	4
06	06/05/2021	Se realiza en las secciones: • “En caso el usuario manifieste que NO hará uso de los equipos asignados y hará uso de sus equipos personales, éste deberá contactar a Mesa de servicio para su devolución inmediata.” • Se agrega los siguientes lineamientos para los callos de equipos prestados y la información del mismo.	4.8
05	13/01/2021	Adición: • Política de teletrabajo (Trabajo remoto)	4.10
04	29/05/2020	Se incluyen lineamientos de la forma en qué se gestionan las claves del mecanismo de cifrado y la recuperación de las llaves de encriptación.	4.14
03	15/10/2019	Adición: • Política de Cifrado y Criptografía • Política de Desarrollo Seguro.	4.14 4.15
02	22/01/2019	Se cambia el nombre del documento, de “Guía del Usuario” a “Política de Seguridad de la Información”. Se agregan:	4.5 4.8

		• Política de acceso a internet. • Política de uso aceptable de equipos. • Política de activos de la información proporcionada a terceros. • POLÍTICA del centro de datos. • Política de Directorio Activo.	4.10 4.11 4.12
01	07/08/2018	Revisión y Aprobación del Documento	--
00	17/02/2017	Creación del documento	--