TABLA DE CONTENIDO

1.INTRODUCCIÓN

Conforme a la Política General de la Seguridad de la información de la Compañía Customer Operation Success, considera a la información como un activo de vital importancia y el aseguramiento de la información cumpliendo con la legislación aplicable. Confidencialidad, disponibilidad e integridad de la información como prioridad para realizar con normalidad sus operaciones y actividades. Por lo tanto, establece los mecanismos para su protección, medios de soporte, comunicación y tratamiento de todo tipo de amenazas, las cuales pueden ser internas o externas, deliberadas o accidentales. Customer Operation Success, garantiza el apoyo al proceso de planificación, implementación, revisión y mejora del sistema de gestión de la seguridad de la información, asumiendo con ello, el compromiso de proteger los recursos de la información. Customer Operation Success, establece los mecanismos para respaldar la difusión y actualización, tanto de la presente política como de los demás componentes del sistema de gestión de seguridad de la información. En cumplimiento a los objetivos de seguridad de la información:

- Optimizar el nivel de eficacia de los controles de Customer Operation Success como parte del sistema de gestión de seguridad de la información.
- Garantizar el acceso a la información controlando los criterios de seguridad establecidos por la empresa, su normatividad aplicable y/o las partes interesadas.
- Mantener la integridad de la información de la empresa considerando los requisitos de seguridad aplicables, los resultados de la valoración y/o el tratamiento de los riesgos identificados.
- Asegurar que la información de Customer Operation Success esté disponible para los usuarios o procesos autorizados en el momento en que así lo requieran.
- Incrementar el nivel de uso de los clientes internos y/o externos de las herramientas informativas de Customer Operation Success .

La alta dirección en el presente documento define los lineamientos que se establecen para la gestión del sistema. Estas políticas serán revisadas cuando ocurran cambios en el contexto interno

o externo, después de realización de auditorías en caso de hallazgos o de lo contrario como mínimo una vez al año.

Dicha revisión y aprobación estará a cargo de la alta dirección, la cual puede formalizarse mediante el informe anual de revisión por la dirección del SGSI.

2.1. POLÍTICA DE ASIGNACIÓN Y RETIRO DE USUARIOS

2.2. Objetivo

Establecer las directrices para la asignación, modificación y retiro de usuarios de las campañas de la compañía, con el fin de dar un buen uso de las herramientas informáticas garantizando el control de la gestión de usuarios.

2.2 Alcance

Inicia desde la creación y asignación de los usuarios hasta el momento de la eliminación del usuario por el retiro del colaborador de la compañía.

2.3 Áreas responsables

- Selección
- Formación y Calidad
- Operación
- Administración de Accesos
- Jurídico
- Seguridad Física
- Infraestructura Tecnológica
- Seguridad de la Información

1.4

2.4.1 Ingreso

2.4.1.1 Aviso de ingreso

Se debe enviar una notificación de creación del nuevo usuario al área de Administración de accesos por parte del personal autorizado. Esta solicitud se realiza por medio de GLPI.

El área de Administración de usuarios debe velar porque se garanticen las siguientes directrices:

- ✓ Cada usuario debe utilizar un único ID o “Username”.
- ✓ Cada perfil tiene un nivel de acceso.
- ✓ Todos los usuarios deben estar dentro del sistema de autenticación del directorio activo que permita su control de acceso a los recursos compartidos de forma estricta.

La base de datos de usuarios y contraseñas del controlador de dominio es administrada y mantenida de forma confidencial y el área de Infraestructura Tecnológica de su administración.

2.4.1.2 Información de usuario contratación COS

Las cuentas de usuarios (Username o logon name) del directorio activo deben cumplir con el siguiente formato:

Nombre + “.” + Apellido

Ejemplo 1: Mauricio Pérez = Mauricio.Perez

Si existe un usuario con igual nombre y apellido, se debe incluir la primera letra del segundo nombre o la segunda letra del apellido en caso de no tener un segundo nombre.

Ejemplo: Mauricio Daniel Pérez = mauriciod.perez

Mauricio Perez Ortiz = mauricio.perezo

Cuando se cree un usuario en el Dominio se debe tener en cuenta:

1. Debe ubicarse en la OU (Unidad Organizacional) de acuerdo con su campaña.
2. Debe agregarse al grupo de seguridad de su área si existe tal grupo.
3. El nombre (First Name y Last Name) debe ser escrito con la primera letra en Mayúscula.

4. Se debe crear con una contraseña básica y debe señalar el campo “El usuario debe cambiar la contraseña en el siguiente inicio de sesión”.

Nota: Validar proceso específico de creación de usuarios (Claro y otras campañas) en el procedimiento de creación, modificación y eliminación de usuarios.

2.4.1.3 Información de usuario contratación externos

Las cuentas de usuarios (Username o logon name) del dominio deben cumplir con el siguiente formato:

Nombre + “.” + Apellido + .ext

Ejemplo 1: Mauricio Pérez = Mauricio.Perez.ext

Si existe un usuario con igual nombre y apellido, se debe incluir la primera letra del segundo nombre o la segunda letra del apellido en caso de no tener un segundo nombre.

Ejemplo: Mauricio Daniel Pérez = mauriciod.perez.ext

Mauricio Perez Ortiz = mauricio.perezo.ext

Cuando se cree un usuario en el controlador de dominio se debe tener en cuenta:

1. Debe ubicarse en la OU (Unidad Organizacional) de acuerdo con su campaña.
2. Debe agregarse al grupo de seguridad de su área si existe tal grupo.
3. El nombre (First Name y Last Name) debe ser escrito con la primera letra en Mayúscula.
4. Se debe crear con una contraseña básica y debe señalar el campo “El usuario debe cambiar la contraseña en el siguiente inicio de sesión”.

2.4.1.4 Administración de contraseñas

Las contraseñas establecidas para los usuarios deben cumplir:

- Histórico de contraseñas - 24 contraseñas recordadas
- Longitud mínima de contraseñas – 12 a 14 caracteres
- Complejidad de la contraseña – Debe contener números, letras mayúsculas y minúsculas.

- Umbral de bloqueo de cuentas – 3 intentos fallidos

Nota: Validar proceso específico de creación de usuarios (Claro y otras campañas) en el procedimiento de creación, modificación y eliminación de usuarios.

2.4.2. Modificación y/o cambio de perfil

En caso de cambio de un usuario de cargo o campaña se debe notificar por medio de un caso en GLPI al área de Administración de Accesos cumpliendo con el proceso establecido

Nota: Validar proceso específico de modificación de usuarios (Claro y otras campañas) en el procedimiento de creación, modificación y eliminación de usuarios.

2.4.3 Retiro

2.4.3.1 Aviso de retiro

En caso de retiro del personal de la compañía, el área de Jurídico debe notificar al área de Administración de Accesos mediante un caso GLPI en un tiempo máximo de 24 horas y enviar un correo electrónico con la carta de retiro. Esta notificación debe incluir los nombres completos del colaborador, identificación (PEP o No. de pasaporte para extranjeros), motivo de retiro, fecha de retiro y campaña.

El área de Administración de Accesos procede a dar de baja en el directorio activo a los usuarios retirados, según la base consolidada por el área de Jurídico.

Nota: Validar proceso específico de eliminación de usuarios (Claro y otras campañas) en el procedimiento de creación, modificación y eliminación de usuarios.

2.4.4. Restablecimiento de Contraseñas

En caso de bloqueo de los aplicativos internos y externos de la compañía se debe notificar por medio de un caso en GLPI al área de Administración de Accesos cumpliendo con el proceso establecido.

Nota: Validar proceso específico de eliminación de usuarios (Claro y otras campañas) en el procedimiento de creación, modificación y eliminación de usuarios.

3.POLÍTICAS DE COPIAS DE RESPALDO

3.1. OBJETIVO

Definir los lineamientos para generar copias de respaldo y asegurar que la información se pueda recuperar ante cualquier destrucción, perdida o incidente de seguridad de la información.

3.2 ALCANCE

Esta política aplica a todos los datos alojados en los activos y sistemas de información bajo resguardo establecido por el área propietaria.

3.3 RESPONSABLES

A) Propietario de activo de información: Define la clasificación y los derechos de acceso que tienen los demás usuarios.

B) Responsable de activo de información: Administra, implementa y monitorea los controles de seguridad que el propietario de los activos haya definido, con el fin de garantizar la confidencialidad, integridad y disponibilidad de la información.

3.4 DEFINICIONES

a) **Copia de respaldo:** Es una copia de los datos del sistema, la configuración o la aplicación que se almacena por separado del original.
b) **Restaurar copias de respaldo:** Es el proceso de copiar datos de respaldo desde el almacenamiento secundario y restaurarlos a su ubicación original o a una nueva ubicación. Se realiza una restauración para devolver datos perdidos, robados o dañados a su condición original o para mover datos a una nueva ubicación.
c) **Clasificación de la información:** Importancia y sensibilidad de los datos permitiendo considerar si las copias deben estar comprimidas, protegidas con contraseñas, o incluso cifradas.
d) **Naturaleza de la información:** Análisis de lo que se va a copiar de nuestros sistemas.
e) **Volumen de información:** Estimación de la cantidad de datos a copiar.
f) **Programación**: Forma de realizar el respaldo manual o automatizada.
g) **Periodicidad/frecuencia:** Diaria, semanal, mensual o anual y la frecuencia de las copias dependerá de los cambios producidos en la información y serán estimado de acuerdo con las modificaciones.
h) **Tipo de backup:** Cantidad de información a copiar (completo, incremental, diferencial).
i) **Localización/almacenamiento**: las copias pueden ser locales, remotas y externas.
j) **Soporte:** Elegir el objeto físico que almacena o contiene datos o documentos susceptibles de ser tratados en un sistema de información y sobre el cual se pueden grabar y recuperar datos.
k) **Estrategia:** Puede ser permanente o mediante la rotación de los soportes. mientras más sencillo sea el esquema estratégico, más fácil de mantener.
l) **Software:** Establecer la herramienta en función de las necesidades con características licenciadas para realizar las copias.
m) **Pre-tareas:** Acciones por realizar antes de realizar la copia de respaldo.
n) **Pos-tareas:** Acciones a realizar al finalizar la copia de respaldo.

o) **Causas de interrupción**: Los planes de backups se definen de acuerdo con las causas de posibles interrupciones partiendo de ellas se referencian los procedimientos a seguir en caso de que las mismas se presenten.

- **Daño en servidor:** Se presenta cuando el servidor asignado de la gestión y administración de datos tiene una falla ya sea de Hardware o Software.
- **Interrupción en el servicio de LAN o internet:** Se presenta alteración cuando el servidor al que se le está realizando backup pierde conexión.
- **Apagones de luz:** Se presenta cuando el suministro de energía se anula y la maquina se apaga, en este caso, no se realizará la copia de seguridad hasta que vuelva el suministro de energía.

3.53.5 LINEAMIENTOS

Esta política establece qué destino tendrá la información, así como la responsabilidad de los propietarios y responsables de los activos de información en conocer, adoptar y implementar la presente política. Se establece qué datos se deben copiar, dónde hacer cada copia, con qué frecuencia, las medidas de seguridad que deben aplicar para garantizar la confidencialidad, integridad y disponibilidad de las copias de seguridad. Se debe cumplir con los siguientes criterios:

3.5.1 Activos de información con copia de respaldo

a) Servidores físicos y virtuales (sistema operativo, configuraciones, logs de configuraciones del sistema y bases de datos)

b) Aplicaciones externas (paquetes, librerías y/o lenguajes de programación con los cuales han sido desarrollados o interactúan los aplicativos corporativos).

c) Aplicaciones propias (códigos fuentes, ejecutables, librerías de código y la base de datos).

d) Datos y estructura de datos (bases de datos, índices, tablas de validación, contraseñas, usuarios, roles, configuraciones y todo archivo necesario para el funcionamiento de los

sistemas de información de la compañía y la pronta recuperación de estos en caso de fallas, registros de auditoría y/o logs).

e) Archivos generados por los sistemas y usuarios en base a su gestión o utilización.

f) Archivos de configuración de los componentes de red.

g) Grabaciones de llamadas.

3.5.2 Tipos de respaldo

a) **Completo:** hacer una copia de todos los datos que una organización desea proteger en un solo de respaldo.

b) **Incremental**: copia los datos que se han modificado o creado desde que se realizó la actividad de respaldo anterior.

c) **Diferencial:** copia todos los archivos que han cambiado desde el último respaldo completo.

3.5.3 Frecuencia de respaldo

Cada propietario de activo de información debe generar un mínimo de tres (3) copias de respaldo al año y establecer el periodo en que se realizará cada copia. La custodia será responsabilidad del propietario y debe evidenciar al área de seguridad de la información y ciberseguridad el cumplimiento de este proceso.

3.5.4 Restauración copias de seguridad

Cada propietario de activo de información debe generar al menos una (1) vez al año una prueba de restauración, dejar registro de la ejecución de esta, verificar contra el tiempo de restauración requerido según la criticidad del activo y garantizar que la prueba es efectiva para uso de emergencia en caso necesario.

3.5.5 Cifrado de copias de seguridad

Las copias de seguridad deben estar cifradas mediante las técnicas criptográficas definidas por el administrador del activo de información para garantizar que la información confidencial esté protegida teniendo en cuenta la política de controles criptográficos.

3.5.6 Clasificación de la información

Realizar la clasificación de activos teniendo en cuenta los siguientes criterios:

a) **Publico:** Información que puede ser conocida y utilizada sin autorización por cualquier Persona, sea empleado de la Empresa o no.
b) **Privado:** es un tipo de información que la ley no permite divulgar ya que afecta la intimidad personal, la seguridad nacional, o simplemente es excluida por la ley.
c) **Confidencial**: Información que sólo puede ser conocida y utilizada por un grupo de empleados para realizar su trabajo y que cuya divulgación o uso no autorizados podría ocasionar pérdidas significativas para la empresa.

3.5.7 Periodo de retención

El borrado seguro de la información lógica y física debe cumplirse según los niveles y tiempos de retención definidos en el contrato con cada cliente, y debe realizarse de acuerdo con el procedimiento de entrega, borrado y destrucción de medios.

3.6 ANEXOS

a) Procedimiento de clasificación, etiquetado y manejo de activos de información
b) Procedimiento de inventario de activos de información tecnológicos
c) Política de controles criptográficos.
d) Política de entrega borrado y destrucción de medios.
e) Procedimiento de Entrega, Borrado y destrucción de medios.

4.POLÍTICA DE CONTINUIDAD DE NEGOCIO

Desde la alta gerencia de COS estamos comprometidos con mantener la continuidad de la prestación de los servicios de telecomunicaciones y BPO* en Call, Contact center y Gestión de cobranzas y de los procesos críticos o de impacto contratados por nuestros clientes aliados, ante la ocurrencia de posibles incidentes de interrupción, protegiendo la vida de los colaboradores y partes interesadas, así como los recursos, la seguridad de la información, la imagen y la reputación, satisfaciendo el cumplimiento de los requisitos y asegurando la mejora continua del Sistema de Gestión de la Continuidad del Negocio (SGCN*).

4.1 Objetivos de continuidad del negocio

4.1.1 Objetivos estratégicos

- Cumplir los niveles de servicio aceptables pactados.
- Asegurar la capacidad de la continuidad del negocio, mediante los recursos necesarios para la prestación de los servicios.
- Proteger la confidencialidad, integridad y disponibilidad de la información durante la gestión la continuidad del negocio.
- Identificar y evaluar los riesgos para la continuidad del negocio, para reducir la probabilidad de ocurrencia e impacto de las consecuencias ante incidentes de interrupción.
- Cumplir los requisitos de continuidad del negocio vigentes aplicables.
- Mejorar continuamente la eficacia del Sistema de Gestión de la Continuidad del Negocio.

4.1.2 Objetivos generales de continuidad

- Preservar la vida.
- Mantener los niveles de servicios con calidad y seguridad de la información.

4.2 Vigencia

Esta política cuenta con la aprobación de la Gerencia General, es de obligatorio cumplimiento desde la fecha de emisión de este documento y será revisada de forma anual por el comité de continuidad, de ser necesario algún cambio se cambiará de versión y emisión con el visto bueno de los integrantes y gerencia general.

4.3 Alcance del SGCN

COS define la aplicabilidad de su Sistema de Gestión de Continuidad de Negocio (SGCN) para la prestación de los servicios BPO1 de call, contact center y telecomunicaciones en ventas, SAC, cobranzas, auditoría de servicios y backoffice, en la ciudad de Bogotá, los cuales se soportan mediante soluciones tecnológicas especializadas para optimizar y asegurar la consecución de los resultados. Esta Política se aplica a todos los colaboradores, altos directivos, miembros de la Junta Directiva de (en adelante denominados, Empleados), así como a todas las contrapartes, Stakeholder de interés y otros representantes (en adelante denominados, Socios de Negocio) que actúan en nombre de COS.

4.3.1 Comité de Continuidad del Negocio

Se crea el Comité de Continuidad de Negocio como ente rector en la materia con la participación de los siguientes cargos Gerente de tecnología e innovación, director de seguridad de la información, Gerente de Control interno, Gerente Administrativa, Gerente Financiera, Gerente de Talento y Gerente de Operaciones.

4.3.2 Exclusiones del alcance del SGCN

Se excluye del SGCN de COS el Desarrollo de software, mencionada en la página WEB corporativa, pero no realizadas directamente por COS. Respecto a los requisitos de la Norma ISO 22301:2019, NO APLICAN exclusiones. No se excluyen procesos de los sistemas de gestión de la organización (Ver Mapa de procesos).

4.4 Estructura del proceso de gestión de continuidad del negocio

COS ha establecido una estructura estratégica, táctica y operativa que tiene el propósito de lograr el aseguramiento de la recuperación de los procesos definidos como críticos y la adecuada atención de situaciones de crisis; así mismo, busca soportar el mantenimiento y la actualización de los diferentes componentes asociados al Plan de Continuidad de Negocio.

Esta estructura está conformada por el Grupo Gestión de Crisis, el Grupo de Gestión de riesgos y Continuidad del Negocio y el Grupo Operativo.

Tabla 1. Estructura de gobierno gestión de continuidad del negocio

Grupo Gestión de Crisis	Grupo Gestión de Continuidad	Grupo Operativo
Tomar decisiones en aspectos críticos, direccionar estrategias durante la contingencia y el retorno a la normalidad.	Mantenimiento de las etapas y actividades involucradas en la gestión de la continuidad de negocio de COS de manera permanente.	Ejecutar las diferentes actividades para restablecer los procesos críticos.

Ante una activación del Plan de Continuidad de Negocio, estos grupos son responsables de restablecer la operación de los procesos identificados como críticos, dentro de los plazos establecidos por el Análisis de Impacto al Negocio BIA.

4.4.1 Grupo gestión de crisis

Corresponderá al Grupo Gestión de Crisis tomar Toma de decisiones en el marco de la comunicación con los grupos de continuidad, operación y crisis relacionadas con aspectos críticos de carácter legal y/o normativo, de servicio, de operación, de imagen y/o financieros que sean necesarias durante las situaciones de crisis o contingencia; así como determinar la necesidad de realizar comunicaciones internas y/o externas. Ante una situación de crisis, este será convocado por el Gerente General de COS, o por el Líder PCN. Estará conformado por:

Ilustración 1. Estructura Grupo Gestión de Crisis COS.

4.4.2 Grupo gestión de continuidad

Este grupo se encargará de realizar las diferentes, etapas y actividades involucradas en la función de continuidad de negocio y será convocado por cualquiera de sus miembros. Está conformado por:

Ilustración 2. Grupo Gestión de Continuidad.

4.4.3 Grupo operativo

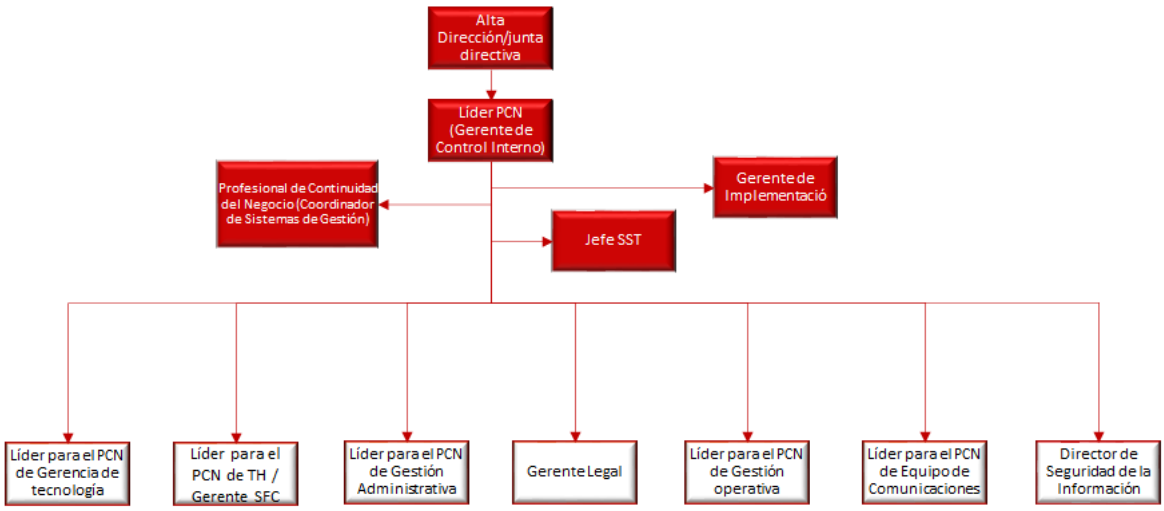
Este Grupo es el encargado de ejecutar las diferentes actividades para restablecer los procesos críticos. El Grupo Operativo, será convocado bajo la Instrucción del Grupo Gestión de Crisis; estará conformado por:

Ilustración 3. Grupo Operativo

4.5 Roles, responsabilidades y autoridades del pcn

Estructura de los roles y responsabilidades de los integrantes del grupo de gestión de continuidad en lo respectivo al Plan de Continuidad del Negocio.

Ilustración 4. Roles y responsabilidades PCN



4.6 Responsabilidades del comité

Teniendo en cuenta su rol dentro de la organización sus responsabilidades dentro del sistema de continuidad de negocio serán las siguientes:

- Velar por la aplicación de la presente política de continuidad de negocio, así como formular, y gestionar las modificaciones en la misma, y someterlas a aprobación por parte de gerencia general.
- Validar los procesos críticos empresariales que se deban considerar en el Plan de Continuidad de Negocio, así como la estimación del tiempo máximo que puede soportar la compañía con la interrupción del servicio, producto del incidente que se presente.
- Asegurar que se formulen, evalúen, y mantengan actualizados los Planes de Continuidad de Negocio, por parte de los responsables de los procesos críticos, y que se divulguen a todos los empleados, contratistas y proveedores de servicios. Se entiende como plan de continuidad de negocio, un plan documentado y probado con el fin de responder ante una emergencia de manera adecuada, logrando así el mínimo impacto en la operación del negocio.
- Asegurar que se mantenga actualizado el análisis de vulnerabilidad y amenazas, así como la evaluación periódica de los riesgos y sus probabilidades de materialización con el fin de actualizar los planes de continuidad de negocio.
- Garantizar que se documenten y mantengan actualizados y disponibles los procedimientos para hacer frente a un incidente, desde que éste se presenta, hasta la restauración o vuelta a la normalidad, tanto en lo que se refiere al accionar interno como externo a la compañía.
- Asegurar que las funciones y responsabilidades detalladas en los planes de continuidad de negocio, se asignen al personal idóneo para la atención de los incidentes. El mismo criterio se aplicará al plan de sucesión en caso de incidentes.
- Velar porque se cumpla con los planes de capacitación al personal, tanto titular como sucesor en los roles que debe desempeñar en caso de incidentes.

- Asegurar que, como parte de los planes de continuidad, se elaboren y actualicen los planes de comunicación interna y externa, para aplicar cuando se presente un incidente.
- Asegurar que se mantenga actualizada la evaluación de proveedores de insumos para los procesos críticos.
- Asegurar que los planes de continuidad incluyan en forma detallada los roles ante la presencia de un incidente y que se realicen las pruebas de validación y efectividad de estos planes, así como de control del tiempo requerido para la restauración de las operaciones.
- Asegurar que, ante cambios significativos en los procesos empresariales, se actualice el plan de continuidad de negocio.
- Sugerir los planes coherentes y que sean apoyados a la realidad de la compañía.
- Asistir a las reuniones que sean proyectadas para la validación de la eficacia del sistema de gestión de continuidad de negocio.
- Comunicar a sus equipos de trabajo la importancia del plan de comunidad y las estrategias propuestas teniendo en cuenta el análisis de impacto de negocio (BIA)
- Diligenciar los registros necesarios para la validación de trazabilidad del plan de continuidad o estrategias previstas.
- Cumplir con las estrategias pactadas, si de llegar a generarse cambios estos deben tener el visto bueno del comité.
- Participar activamente en el comité de riesgos y continuidad de negocio.

5.POLÍTICA DE CONTROL DE ACCESOS FÍSICOS Y LOGICOS

5.1 OBJETIVO

Establecer los lineamientos que aseguren los accesos físicos y lógicos basados en la premisa o principio de que todo acceso está prohibido, a menos que se permita de manera formal y bajo los

privilegios para el ingreso a las instalaciones, sistemas de información, servicios de infraestructura tecnológica, aplicaciones externas, y demás activos de información de COS, con el propósito que estén disponibles única y exclusivamente para los propietarios, responsables y usuarios de la información que tengan autorizado el acceso para el ejercicio de sus funciones

5.2 ALCANCE

Esta política aplica a todas las áreas, procesos, sistemas, instalaciones y activos de información de la organización que requieran protección frente a accesos no autorizados. Cubre a todos los usuarios internos, contratistas, proveedores, consultores y cualquier tercero que acceda a los recursos de información de la empresa, ya sea de forma local o remota

5.3 RESPONSABLES

El cumplimiento de esta política es responsabilidad de todo el personal que haga parte de la organización.

.

5.4 DEFINICIONES

- Acceso Físico: ingreso o presencia dentro de una zona física controlada donde se encuentran activos de información, tales como oficinas, salas de servidores o archivos confidenciales.
- Acceso Lógico: ingreso a sistemas informáticos o plataformas digitales mediante autenticación electrónica (usuario/contraseña, tokens, biometría, etc.).
- Autenticación: proceso mediante el cual se verifica la identidad de un usuario, dispositivo o sistema antes de conceder acceso.
- Autorización: permiso o privilegio otorgado a un usuario o sistema para realizar ciertas acciones sobre recursos específicos.
- Principio de Mínimos Privilegios: principio que establece que cada usuario debe tener solo los permisos necesarios para cumplir con sus responsabilidades.

- Incidente de Seguridad: cualquier evento que comprometa la seguridad de la información, como accesos no autorizados, violaciones de políticas, pérdida de control de credenciales, etc.

- VPN (Virtual Private Network): red privada virtual que permite establecer una conexión segura y cifrada entre un dispositivo y la red interna de la organización a través de internet. Su uso protege la confidencialidad e integridad de los datos transmitidos y es esencial para accesos remotos controlados.

- CCTV (Closed-Circuit Television): sistema de videovigilancia compuesto por cámaras conectadas a un circuito cerrado que permite la supervisión y grabación de espacios físicos. Es utilizado como un control de acceso físico y medida de seguridad para prevenir o detectar accesos no autorizados y otros incidentes.

- DHCP (Dynamic Host Configuration Protocol): protocolo de red que asigna automáticamente direcciones IP y otros parámetros de configuración a dispositivos dentro de una red. Facilita la administración de direcciones IP y contribuye al control y monitoreo del acceso lógico a los recursos de red.

5.5 LINEAMIENTOS

5.5.1 RESPONSABILIDADES DE LOS USUARIOS

Los usuarios asignados para el acceso a las herramientas tecnológicas y/o sistemas de información son de uso exclusivo e intransferible y son responsabilidad de cada usuario.

Las siguientes faltas son motivo de cancelación de contrato, ya que van en contra de la confidencialidad y el buen manejo de la información:

1) No está autorizado prestar credenciales de usuario a otra persona ni trabajar con otros usuarios diferentes a los asignados.

2) El ingreso a cuentas personales, de familiares, amigos u otras personas en las herramientas de consulta, que no estén reportadas en la data asignada por nuestro cliente.

3) Realizar o recibir llamadas personales desde o hacia el canal destinado para la gestión operativa de casos.

4) Envió o recepción de correos electrónicos desde o hacia cuentas personales o de dominio diferente al de COS y a las autorizadas por la empresa.

Todos los funcionarios de COS o terceros que tengan un usuario para el acceso a la información y plataforma tecnolgíca deberán conocer y cumplir con el uso de esta ppolítica específica, donde se dictan pautas sobre derechos y deberes con respecto al uso adecuado de los usuarios y contraseñas.

5.5.2 ACCESO FÍSICO

COS establece las siguientes políticas de acceso a las instalaciones de la Organización:

1.Todos los funcionarios de la compañía deben registrarse al ingreso al inicio y fin de turno mediante el control biométrico, sólo los funcionarios de alta dirección tienen excepción a esta política, adicionalmente, todo el personal debe portar el carné en un lugar visible en todo momento dentro de las instalaciones de la organización.

2.Todo personal que no pertenezca a la organización debe registrarse con fecha y hora de entrada y salida en la recepción, esperar en el lobby para ser atendido por un funcionario de la compañía, y siempre debe estar acompañado por un funcionario de la organización, durante su permanencia en las instalaciones y deben portar el carné de visitante de COS en un lugar visible para facilitar su identificación.

3.Se permitirá el ingreso de visitantes a la organización únicamente para fines específicos, autorizados y se deberá emitir instrucciones sobre los requisitos de seguridad de la empresa y sobre los procedimientos de emergencia.

4.No está permitido el acceso de equipos de cómputo, tecnológicos y/o de almacenamiento externos tales como teléfonos celulares, equipos portátiles, tablets, agendas digitales y demás equipos electrónicos, en las áreas críticas, lo cual incluye áreas operativas o donde

se maneja información sensible o crítica, salvo aprobación y mediante caso cargado en la plataforma GLPI, en cuyo caso debe ser requerido por el gerente del área o campaña que lo atenderá justificando la necesidad.

5.Está prohibido la toma de fotografías y grabaciones al interior de las instalaciones o áreas seguras. En caso debe ser necesario, debe ser solicitado por el gerente del área o campaña que lo atenderá justificando la necesidad.

6.En caso de que se tenga habilitado tablero para toma de apuntes, se deben realizar borrados cuando esta información ya no se requiera dejando limpio y organizado. No está permitido la anotación de información confidencial, ni privilegiada.

7.El porte del carné sólo está permitido en las instalaciones de la compañía, todos los colaboradores al terminar el turno y/o salir de las instalaciones de COS no deben portar el carné en un lugar visible, ya que podrían afectar la seguridad de la compañía.

8.Las áreas restringidas deben contar con mecanismos de autenticación de personal por medio de lectura de huella dactilar y/o tarjeta de proximidad y las puertas deben permanecer en todo momento cerradas.

9.Para el personal que se encuentra en etapa de formación y capacitación inicial el acceso físico a áreas restringidas o no autorizadas debe ser otorgado por el área de talento humano y con la validación del área de seguridad física, ya que en esta fase no cuentan con el registro de las huellas para el control de acceso biométrico; esto quiere decir que, deben estar acompañados permanentemente y requieren el uso visible del carné corporativo o del que lo identifique en proceso de formación.

10.Los mecanismos físicos de identificación y autenticación, como lo son carnés y/o acceso con huellas otorgados al personal que ingresa a las instalaciones de COS, deben ser retirados, en el momento en que sea desvinculado de la organización.

11.Se debe asegurar la visualización y enfoque de puntos de acceso a zonas seguras por medio de cámaras de circuito cerrado de televisión (CCTV) de COS a las áreas seguras y/o críticas.

12.Las grabaciones del CCTV deben ser almacenadas mínimo 2 meses, siempre y cuando no se incumplan acuerdos contractuales específicos con algún cliente externo. No obstante, en caso de requerir las grabaciones como parte de evidencias de eventos o incidentes de seguridad de la información deben ser almacenadas hasta que se cierre el caso o durante el tiempo que se determine.

13.Cuando un cliente externo solicita cámaras del CCTV, se debe realizar por medio formal, a través del gerente de cuenta. COS cuenta con tres (3) días hábiles para presentar las grabaciones requeridas. No está autorizado entregar por ningún medio las grabaciones a los solicitantes externos, sin embargo, esto será posible sólo en aquellos casos en los que se requiera por el cliente bajo la solicitud del jefe de operación, gerente de operación y/o gerente de cuenta.

14.El ingreso al centro de monitoreo del CCTV es restringido únicamente para personal autorizado por el(a) jefe de seguridad física o la alta dirección de COS.

15.El(a) jefe de seguridad física es el responsable delegado por alta dirección con acceso y autorización para administrar la base de datos de videovigilancia. Como propietario del activo de información es el responsable de aplicar los controles de seguridad de la información para la gestión y administración del activo.

16.Es responsabilidad de la alta dirección de COS establecer de forma clara las áreas seguras dentro de la organización donde se accede, procesa, almacena o comunica información privilegiada y/o confidencial, o áreas en donde su acceso indebido pone en riesgo la seguridad de la información de las partes interesadas de COS, por lo anterior únicamente el personal debidamente autorizado podrá acceder a dichas áreas. Algunas de estas áreas seguras en la organización son:

17.Áreas Operativas, acceso permitido únicamente a los funcionarios del proyecto operativo.

- ✓ Centro de impresión y fotocopiado.
- ✓ Centro de monitoreo de CCTV.
- ✓ Oficina de gerencia de tecnología y diseño.
- ✓ Oficinas para atención presencial de titulares.
- ✓ Áreas de gestión documental.
- ✓ Salas de juntas
- ✓ Oficina de la alta dirección.
- ✓ Centros de procesamiento de datos principal y alterno.
- ✓ Centros de cableado y telecomunicaciones.
- ✓ Cuartos eléctricos, cuarto de planta eléctrica y cuarto de UPS y/o baterías.

18.Todo personal autorizado que ingrese a uno de los centros de procesamiento de datos debe registrarse en la bitácora destinada para tal fin.

19.Las áreas como la recepción, el lobby y las cafeterías son consideradas de uso interno, y pueden ser usadas por todos los funcionarios de la organización incluso visitante autorizado.

20.Para los casos en los que los colaboradores internos por razones personales requieran ingresar este tipo de equipos mencionados en el literal a las instalaciones de la compañía, deben ser registrados y dejados en la recepción de la sede.

21.Los representantes de los clientes externos o terceros autorizados que requieran ingresar equipos de cómputo tecnológicos y/o de almacenamiento, deben registrarlos al ingreso y salida de las instalaciones de COS.

22.Se cuenta con un sistema de seguridad física en las instalaciones de COS. Algunos de sus componentes son:

- ✓ Circuito de televisión cerrada (cámaras) - CCTV
- ✓ Controles de acceso y biometría
- ✓ Torniquetes
- ✓ Celaduría privada
- ✓ Identificación con carné

23.Las instrucciones de ingreso a las instalaciones visitantes y empleados describen el proceso y controles de manera detallada.

24.El uso del celular en la operación no está autorizado en las áreas seguras. Este numeral está detallado en la política de dispositivos móviles.

5.3 ACCESO LÓGICO

COS establece las siguientes políticas de acceso a la información:

1.El control de acceso a todos los sistemas o aplicativos de la compañía debe efectuarse por medio de autenticación con nombres de usuario y contraseñas únicas para cada funcionario (Log-in). Las cuentas de usuario y contraseñas son de uso personal, intransferible y privilegiado. Adicional, no está permitido el acceso a la información sensible por parte de usuarios con identidades desconocidas o de forma anónima.

2.En cada inicio de sesión de los equipos de cómputo de la compañía se debe exhibir la siguiente advertencia de acceso:

- Se trata de un sistema informático privado propiedad de Customer Operation Success.

- Se prohíbe el acceso o uso no autorizado y sólo se permiten los usuarios autorizados.

- El uso de este sistema constituye consentimiento para la supervisión en todo momento y el usuario no debe tener ninguna expectativa de privacidad.

- El acceso no autorizado o las violaciones de las normas de seguridad son ilegales y, por lo tanto, si el monitoreo revela cualquiera de ellos, se tomarán medidas disciplinarias

apropiadas contra los empleados que violen las normas de seguridad o que hagan uso no autorizado de este sistema.

- Si revela información, interna de Customer Operation Success o de sus clientes sin previa autorización, podría estar, incurriendo en una violación de la Normativa de la compañía, que podría, incluso, suponer la posible comisión de un delito o falta. Recuerde que su clave de acceso es personal e intransferible. La divulgación de la clave puede afectar la seguridad de nuestra red. En caso de sospecha de divulgación de su clave, proceda a cambiarla de inmediato.

3.El acceso a la información sensible relativa al objeto social o Core del negocio, bien sea de insumo o producto de la gestión, solo puede estar disponible al personal operativo de la campaña correspondiente, requiriéndolo a través de la plataforma integral de procesos.

4.La información y su tratamiento debe tener designado un propietario, el cual designa un responsable de administrar y controlar el acceso y autoriza de manera formal cualquier solicitud de acceso a esta información. Este numeral está contemplado en el procedimiento de clasificación, etiquetado y manejo de activos de información.

5.El acceso a las aplicaciones de cliente o archivos en red debe ser separado. Únicamente está autorizado el acceso a los usuarios pertenecientes al proyecto o área encargada.

6.El gerente de tecnología y diseño tiene la responsabilidad de custodiar la información almacenada en los centros de datos, servidores, aplicaciones, y demás sistemas de información de la organización.

7.El acceso a los usuarios se encuentra asociado en la matriz de roles y privilegios, por ello todos los usuarios registrados, son asignados a grupos y unidades organizativas con permisos predeterminados y están separados por campaña.

8.La autorización de acceso a los sistemas de información es aprobada asegurando que el usuario conoce las políticas de seguridad de la información y ha firmado el acuerdo de confidencialidad.

9.Los dispositivos externos de autenticación (tarjetas inteligentes, token etc.) deben ser custodiados con carácter personal e intransferible al igual que los usuarios y contraseñas.

10.Cualquier tipo de conexión desde sitios externos a COS debe realizarse a través de canales cifrados. Este numeral está contemplado en la política y procedimiento de transferencia de información.

11.No se debe guardar el nombre de usuarios y/o contraseñas en los exploradores de internet o aplicaciones que están a disposición de los colaboradores.

12.Las conexiones no seguras a los servicios de red pueden afectar a COS, por lo tanto, se controlará el acceso a los servicios de red tanto internos como externos. Esto es necesario para garantizar que los usuarios que tengan acceso a las redes y a sus servicios no comprometan la seguridad de estos. Las reglas de acceso a la red a través de los puertos estarán basadas en las premisas “Todo está restringido, a menos que este expresamente permitido” y “Sólo se permite el acceso a los recursos necesarios para su labor”.

13.Se desarrollarán procedimientos para la activación y desactivación de **derechos de acceso a las redes**, los cuales comprenderán:

- ✓ Controlar el acceso a los servicios de red tanto internos como externos.
- ✓ Identificar las redes y servicios de red a los cuales se permite el acceso.
- ✓ Realizar normas y procedimientos de autorización de acceso entre redes.
- ✓ Establecer controles y procedimientos de administración para proteger el acceso y servicios de red.

14.Los servicios de **conexiones externas** están aprobados bajo el modelo de conexión VPN con las siguientes características:

- ✓ Se tiene parametrizado el modelo de conexión dedicada S2S y SSL.
- ✓ Autenticación de doble factor basada en tokens por medio de cuentas de correo electrónico personal.

15.Para el acceso a la información por medio de una conexión inalámbrica se tiene establecido los siguientes parámetros:

- ✓ Uso de equipos portátiles (laptop) de la compañía registrados, se conectan por autenticación de usuario de red activo.
- ✓ Uso de equipos portátiles (laptop) de clientes y/o proveedores, se conectan por autenticación de red (SSID) con contraseña y protocolo de cifrado WPA2 Enterprise.

16.El acceso se brindará para los equipos conectados a la red, mediante controladores de dominio y asignación manual de IP o por DHCP.

17.Las conexiones hacia los activos (switch, AP) se controlan y monitorean a través del proceso de hardening donde se validan la aplicación de políticas de acceso en los puertos activos y no activos.

18.Los puertos que permitan realizar mantenimiento y soporte remoto a los equipos de red servidores y equipos de usuario final, estarán restringidos a los administradores de red o servidores.

19.Los usuarios finales deberán permitir tomar el control remoto de sus equipos al área de soporte. El usuario no debe tener archivos de información sensible a la vista o desatender el equipo mientras que se tenga el control por un tercero.

20.La gerencia de tecnología y diseño proveerá a través de sus ISPs (Proveedor de Servicio de Internet) el servicio de internet corporativo será administrado y controlado y será el único servicio de internet autorizado.

21.Las **contraseñas** en el momento de ser digitadas en el ingreso a aplicativos o sesiones de ingreso, cuentan con enmascaramiento total con la finalidad de que estas no se puedan visualizar. Adicionalmente, se implementará como buenas prácticas:

- ✓ Pregunta de acceso al CRM (En aquellas campañas que así lo requieran).
- ✓ Cambio regular de contraseñas.
- ✓ El ingreso al sistema de telefonía requerirá autenticación doble. Una de usuario personal y otra de estación autorizada y asignada a la campaña o servicio.

22.El **acceso a programas** especiales será controlado y estará sujeto a la matriz de roles y privilegios definida por la organización.

23.Las **creaciones de usuarios y contraseñas** (en combinación denominadas credenciales) deben ser únicas por cada colaborador, configurándose en el directorio activo. Por medio de esta única credencial se otorgan los correspondientes accesos básicos y necesarios a los sistemas de información de COS.

24.En caso de requerir correo electrónico corporativo, se debe cumplir con el procedimiento correspondiente para asignar el buzón de correo. Las credenciales del correo electrónico corporativo deben ser las mismas que las habilitadas para el controlador de dominio.

25.Cuando algún colaborador se desvincule de COS, se deben deshabilitar las credenciales que tenía a cargo para el acceso a los sistemas de información internos. Adicionalmente, si el colaborador tenía autorizados accesos adicionales y servicios de TI estos deben ser eliminados máximo 8 días calendario después de la solicitud de la desvinculación.

26. Las contraseñas que sean utilizadas como medio de autenticación de las credenciales de acceso de sistemas de información y repositorios de red interna, deben cumplir con los siguientes parámetros:

- ✓ La longitud mínima de las contraseñas es de 12 a 14 caracteres.
- ✓ La contraseña debe incluir números, letras mayúsculas y minúsculas.

- ✓ La recordación debe ser de 24 contraseñas.
- ✓ Debe ser cambiada mínimo cada 30 días.
- ✓ No puede repetirse la contraseña por lo menos durante los últimos 24 cambios.

27. Todo el personal que deba tener acceso a los sistemas de información internos de COS debe cumplir con:

- ✓ Conservar los datos de acceso en secreto.
- ✓ Contraseñas de fácil recordación y difíciles de adivinar, por ejemplo; no utilizar palabras, números de teléfono, fechas de nacimiento, nombres o estar relacionada con la cuenta de usuario.
- ✓ Usar diferentes contraseñas para los servicios y sistemas (en caso de que aplique).
- ✓ Reportar cualquier evento o sospecha de irregularidades relacionado con sus contraseñas como pueden ser pérdida, robo, acceso no correspondiente al colaborador, al área de seguridad de la información, por los medios o canales autorizados divulgados.

28.Los sistemas de administración de contraseñas de COS, deben estar configurados para:

- ✓ No se permite el uso de usuarios genéricos en ningún caso.
- ✓ Cada colaborador debe tener una cuenta de acceso personal, asegurando la trazabilidad y no repudio.
- ✓ Permitir que los usuarios cambien sus contraseñas luego de cumplido el plazo mínimo de conservación de estas o cuando consideren realizarlo.
- ✓ Los usuarios deben cambiar las contraseñas provisionales, asignadas por el administrador del sistema de información, inmediatamente después del primer ingreso exitoso.
- ✓ El bloqueo por inactividad es de 4 días.

Las cuentas se bloquean al tercer intento fallido de ingreso.

No se permite mostrar las contraseñas en texto claro cuando son ingresadas.

29. Para cada tipo de recurso o servicio específico como:

- ✓ Cuentas de correo o dominios específicos.
- ✓ Software operacional o que apoye la prestación de los servicios acceso a enlaces de aplicativos del cliente externo.
- ✓ Acceso a enlaces de consulta.

30.La información de autenticación predeterminada predefinida o proporcionada por los proveedores se cambia inmediatamente después de la instalación de sistemas o software.

31.El proveedor o contratista solo podrá acceder a los recursos estrictamente necesarios para cumplir con el servicio contratado, aplicando el principio de mínimo privilegio y necesidad de saber.

32.Se deben requerir los accesos y privilegios mediante caso en la plataforma integral GLPI teniendo en cuenta la matriz de roles y privilegios.

33.El acceso a la administración de los sistemas operativos y aplicaciones de los equipos de cómputo es restringido para todos los usuarios finales, este acceso sólo es autorizado para el personal del área de tecnología con fines exclusivamente de configuraciones de soporte, quienes deben garantizar el correcto y seguro funcionamiento de los sistemas de procesamiento de la información.

34.Todos los usuarios que son de custodia del área de tecnología, como lo son administradores de servidores, administradores de red, desarrolladores, administradores de bases de datos y demás cuentas administradoras de los sistemas, deben ser cuentas únicas y personales de cada colaborador del área de tecnología, asegurando la trazabilidad de las actividades.

35.El uso de las cuentas administradoras de los sistemas y activos de TI de COS, deben ser usadas para fines autorizados por la gerencia de tecnología y diseño, para garantizar el correcto y seguro funcionamiento sobre los activos de información.

36.La gerencia y/o jefes de IT determinaran el periodo de tiempo necesario para hacer uso de las cuentas administradoras o accesos privilegiados en los sistemas y activos de IT. En todo caso, no deben otorgarse derechos de acceso privilegiado de forma permanente si no es de requerimiento de acuerdo con las funciones del colaborador.

37.Para los casos de cambios de proyecto o área se debe garantizar la revocación de los accesos a los sistemas de información y repositorios de red, así mismo si el colaborador tenía autorizado servicios TI adicionales, referente al cargo anterior.

38.Para desempeñar el nuevo cargo o cambio de área, los nuevos accesos deben ser asignados y aprobados por el jefe directo en cumplimiento de la revocación de usuarios y asignación de los derechos estrictamente necesarios para su nueva ocupación, dejando evidencia en la hoja de ruta y en la plataforma integral de procesos.

39.En COS se permite exclusivamente para la operación del negocio aplicaciones acordes al Core del negocio y que el cliente externo requiere para el intercambio o tratamiento de la información objeto del contrato del servicio. Para el acceso a estas aplicaciones se deben seguir las directrices acordadas con cada uno de los clientes externos, así mismo en caso de desvinculación del personal que tenga acceso a estas aplicaciones, debe ser reportado al cliente dentro de los 8 días calendario siguientes a la novedad reportada por el medio autorizado, para realizar su correspondiente eliminación de accesos.

40.Cada propietario de activo debe depurar las conexiones de aplicaciones y páginas externas de proyectos desvinculados de COS, una vez se haya acordado la fecha de entrega y/o depuración de la información con el cliente externo. No obstante, por motivos de facturación o temas pendientes con el cliente desvinculado es posible requerir los permisos por un periodo adicional el cual,

41.Debe ser notificado y autorizado por la dirección de seguridad de la información.

42.Los derechos de acceso de los usuarios deben ser revisados según el cronograma.

43. Estas revisiones deben incluir, aunque no están limitados a las siguientes velicaciones:

- ✓ Roles y perfiles asignados al usuario.
- ✓ Permisos de lectura y estructura asignados a los roles y perfiles.
- ✓ Funcionarios asociados a los roles.
- ✓ Registros de acceso.
- ✓ Accesos privilegiados.

44. Estas revisiones deben ser objeto de velicación y análisis por parte de los responsables del activo de la información y deben estar programados de manera periódica según el cronograma de revisión de derechos de accesos.

6. POLÍTICA DE PANTALLA Y USUARIO DESPEJADO

6.1. OBJETIVO

Establecer medidas que aseguren la confidencialidad, integridad y disponibilidad de los activos de información de la organización, mediante la implementación de directrices de seguridad apropiadas en los puestos de trabajo de los colaboradores.

6.2 ALCANCE

Esta política aplica a nivel general de la empresa y de cumplimiento obligatorio de los colaboradores de la compañía que hace uso de los equipos de cómputo y se le haya otorgado permiso de acceso a la documentación, sistemas de información, bases de datos, o servicios de tecnologías de la información de la empresa, finaliza en el momento de terminar sus labores diarias.

6.3 RESPONCABLES

El cumplimiento de esta política es responsabilidad de todos los colaboradores que hacen parte de la organización

6.4 DEFINICIONES

a. **Pantalla limpia:** se refiere a la instalación de programa para que los equipos dejen de brindar actualizaciones, ya sea de seguridad, performance, comodidad etc. Buenas prácticas de uso del equipo cuando no esté en uso.
b. **Escritorio Limpio**: es la protección de los papeles y dispositivos removibles de almacenamiento de información, almacenados y manipulados en estaciones de trabajo (escritorio, oficina, etc.) de accesos no autorizados, perdida y/o daño de la información durante y fuera de las horas laborales.
c. **Usuario desatendido:** es la protección de las computadoras, notebook, u otros dispositivos, mediante el bloqueo de pantalla o desconexión cuando no se está en uso prolongadamente o por tiempos cortos.
d. **Activos de información:** Un activo de información es cualquier dato, documento u otro recurso basado en información que es propiedad de una organización, que la administra o mantiene. Esto incluye información física y digital, como documentos, imágenes, videos, archivos de audio, bases de datos y sitios web.

6.5 Desarrollo..

ÍTEM	ACTIVIDAD	RESPONSABLES
1	**Escritorio Limpio y seguro:** Retirar de los escritorios o áreas visibles toda información utilizada, independientemente del medio en que se encuentre. Queda prohibido tener documentos, esferos, papelería o elementos no autorizados en las áreas de operación.	Colaboradores Cos

	Nota: Los lideres de cada proceso serán los responsables directos de realizar controles que permitan mantener dentro de sus operaciones libres de elementos no autorizados.	
2	Realizar la destrucción o eliminación de la información confidencial siguiendo el procedimiento de entrega borrado y destrucción de medios.	Personal autorizado
3	Borrar la información sensible o crítica en los tableros, pizarras o en otros tipos de pantallas cuando ya no se necesiten.	Personal autorizado
4	Restringir el uso de fotocopiadoras y otra tecnología de reproducción a personal o usuarios no autorizados.	Personal autorizado
5	Todo documento que contenga información confidencial deberá ser retirado de manera inmediata de las impresoras, utilizando para ello un código como mecanismo de verificación generado por el área de tecnología.	Personal autorizado Tecnología e innovación
6	Velar que las salas de reuniones permanezcan cerradas y será exclusivo para reuniones de trabajo.	Seguridad física
7	Todo equipo de cómputo o dispositivo de información utilizado en las salas de reuniones, salas de operación u oficinas debe permanecer apagado al finalizar su uso. Asimismo, se deben	Colaboradores Cos, Seguridad física Personal autorizado

	retirar y guardar bajo llave en un gabinete o en otro tipo de mueble de seguridad los documentos utilizados para prevenir la exposición o pérdida de información. **Nota:** Realizar barrido final antes de retirarse de las salas con el fin de evitar dejar documentos caídos en el piso o detrás de muebles o cajones.	
8	Queda prohibido tener líquidos, sin tapa en sus puestos de trabajo (especialmente en operación), que pudieran dañar documentos originales y/o equipo de trabajo y la información almacenada en ellos, ingerir comida en los puestos de trabajo, es una falta grave dentro de la operación y en las oficinas. Tanto de personal interno de la compañía como externo (clientes, proveedores), para ello se cuenta con las áreas de comedores para todo el personal.	Colaboradores Cos Seguridad física y Servicios generales
9	**Pantalla limpia:** El escritorio de la computadora no debe poseer archivos o carpetas con accesos directos que faciliten la ubicación de información, excepto los programas autorizados por la gerencia de tecnología e innovación para su instalación.	Colaboradores Cos
10	Proteger la información, desactivar ventanas emergentes, cerrar pestañas, archivos que contengan información confidencial durante	Colaboradores Cos

	reuniones en línea, pantallas compartidas o en áreas públicas.	
11	El único fondo de pantalla autorizado para los usuarios que utilizan equipos propiedad de COS es el autorizado por el proceso de gestión tecnología y diseño.	Colaboradores Cos
12	Queda prohibido decorar las pantallas de los equipos con stickers, sellos y papeles.	Colaboradores Cos
13	**Usuario desatendido:** Todos los usuarios deben terminar las sesiones activas cuando finalicen sus labores.	Colaboradores Cos
14	El usuario debe bloquear su equipo al retirarse de su área de trabajo por cualquier motivo y solo será desbloqueado por medio del usuario y contraseña de red.	Colaboradores Cos
15	El sistema debe bloquear automáticamente el equipo luego de tres minutos de usuario inactivo y solo será desbloqueado por medio del usuario y contraseña de red.	Colaboradores Cos
16	Cuando el usuario abandone su escritorio para asistir a alguna reunión, capacitación entre otros, debe verificar que no exista información sensible o documentos sobre el escritorio, sin importar el tiempo de ausencia.	Colaboradores Cos

17	Se prohíbe el ingreso de USB y demás medios de almacenamiento extraíbles; todos los equipos deben tener activo el bloqueo de puertos USB.	Colaboradores Cos Personal autorizado
18	El usuario deberá apagar su equipo de cómputo al finalizar su jornada de trabajo, con excepciones de algunos equipos que deben permanecer encendido en caso se deban ejecutar procesos durante horas no hábiles, o bien por accesos que deban realizarse en forma remota con motivo de garantizar la continuidad de las operaciones en la empresa. (Se encuentran marcados como equipo de consulta). Los equipos con la autorización de no ser apagados deben ser informados al gerente de tecnología e innovación.	Colaboradores Cos

7.POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN PARA PROVEEDORES Y CONTRATISTAS

7.1 Objetivo:

El principal objetivo de este documento es establecer el marco normativo en relación con la seguridad de la información para los proveedores y contratistas de COS S.A.S, que en el desarrollo de sus funciones pueda tener acceso a la información, sistemas de información o recursos de la compañía en general, con el fin de proteger la confidencialidad, integridad y disponibilidad de la información y sistemas manejados por la empresa.

Para ello, las empresas proveedoras y contratistas a las que se les remitan estas políticas de seguridad se responsabilizan de informar a las personas que destinen en COS S.A.S, así como de obtener su compromiso por escrito de que se comprometen a respetar dichas políticas.

7.2. ALCANCE

Esta política aplica a todos los proveedores y contratistas externos que tengan acceso, manejo o procesamiento de los activos de información de COS S.A.S, ya sea directa o indirectamente, en modalidad presencial o remota

7.3 RESPONSABLES

- Proveedores y contratistas
- Gerencia financiera
- Gerencia Legal
- Gerencia de tecnología
- Seguridad de la información

7.4 DEFINICIONES

- **Activo de información:** cualquier dato, documento, sistema, servicio, infraestructura o recurso relacionado con la información que tenga valor para la organización.
- **Proveedor:** entidad externa contratada para suministrar bienes o servicios a la organización.
- **Contratista:** Persona natural o jurídica que presta servicios a la organización bajo un contrato específico, sin formar parte de su plantilla.
- **Información confidencial:** información cuyo acceso está restringido a personas autorizadas y cuya divulgación no autorizada puede afectar los intereses de la organización.
- **Incidente de seguridad:** evento que compromete, o tiene el potencial de comprometer, la confidencialidad, integridad o disponibilidad de la información.

- **Tercero:** cualquier persona o entidad ajena a la organización que interactúe con sus activos de información

7.5 GESTION DE RIESGOS

La gestión de riesgos de proveedores se realiza de acuerdo con la *Guía para la gestión integral del riesgo* y sus componentes adicionales. Esta guía se evalúa de manera anual mediante el comité de riesgo establecido

7.6. CONTACTO CON EL PROVEEDOR Y/O CONTRATISTA

Todo proveedor y contratista en el desarrollo de sus funciones que pueda tener acceso a la información, sistemas de información o recursos de COS S.A.S en general debe:

- Contar con su respectiva verificación de idoneidad y estará sujeto a verificación de la documentación e información suministrada.
- Contar con un contrato por escrito y firmado, adicionalmente se anexará una cláusula o documento de garantía de confidencialidad.
- El proveedor y/o contratista, subcontratistas y/o sobreveedores y sus funcionarios deben conocer y dar cumplimiento a la política de seguridad de la información bajo los términos establecidos por COS S.A.S.

  El proveedor deberá proporcionar la información necesaria a COS S.A.S, de los funcionarios que ejecutaran las actividades contractuales.
- Todo incumplimiento por parte del proveedor y/o contratista a la política y acuerdos contractuales o términos normativos establecidos por COS S.A.S en lo que respecta a seguridad de la Información será causal de finalización del contrato y se procederá con las respectivas gestiones judiciales a que haya lugar.
- No se evitarán los mecanismos y actividades de gestión establecidos por COS S.A.S que permitan proteger frente a las amenazas que les puedan afectar las redes y a las aplicaciones que las utilizan.

- Se identificarán tanto las características de seguridad, los niveles de servicio y los mecanismos de gestión para garantizar la seguridad del servicio de redes prestadas por proveedores o contratista.

7.7 ejecución de las funciones contractuales por parte del proveedor

Toda la información relacionada con las actividades de COS S.A.S se considera confidencial.

El proveedor deberá cumplir las funciones y obligaciones aplicadas a la utilización de los sistemas de información según la normativa establecida por COS S.A.S.

La infraestructura tecnológica se ubicará en zonas seguras y protegidos con el fin de reducir los riesgos derivados de las amenazas externas, es responsabilidad del proveedor la seguridad de dichos equipos en caso de ser utilizados.

7.8 Uso de infraestructura tecnológica

Se protegerá la infraestructura tecnológica, que así lo necesite, contra fallos de provisión en el suministro eléctrico, por lo tanto, la conexión de cualquier equipamiento a los circuitos tanto eléctrico como de comunicaciones deberá ser validad por el área de tecnología, con el fin de evitar interceptaciones o daños.

Se deberá solicitar validación previa y se implementarán medidas de control indicadas, sobre toda la infraestructura tecnológica que por necesidades puntuales se deban ubicar fuera de las áreas protegidas en COS S.A.S o fuera de la organización.

Todo equipo tecnológico propiedad o en administración COS S.A.S no podrá salir de las instalaciones sin una autorización otorgada por el jefe de Seguridad Física, esta autorización se debe realizar por medio de correo electrónico, de acuerdo con las Políticas de traslado de equipos de COS S.A.S.

COS S.A.S facilitará, en función de las necesidades contractuales, procedimientos de operación actualizados a los proveedores y/o contratistas que los necesiten

Se prohíben los cambios sobre la infraestructura y los recursos tecnológicos, de llegar a ser necesarios la aprobación es directamente del Gerente General de COS S.A.S

COS S.A.S facilitara al proveedor o contratista, áreas locativas y/o equipos tecnológicos para el desarrollo de las actividades contractuales.

En función de la criticidad y/o riesgo del servicio contratado, los cambios en la prestación del servicio deberán ser validados previamente por COS S.A.S.

Se prohíbe al proveedor o contratista la ejecución de códigos no autorizados.

La configuración de los equipos garantizará que el código autorizado funciona de acuerdo con lo definido en la normativa establecida al respecto.

De acuerdo, a la labor a realizar por parte de los proveedores o contratistas, no se autorizan la toma de fotografías a las áreas seguras de COS S.A.S, solo el jefe de Infraestructura, el jefe de Seguridad Física y Control Interno puede autorizar el acceso a estas áreas de acuerdo con sus términos contractuales

7.9 Uso de unidades extraíbles

La utilización de unidades extraíbles de información deberá ser validada previamente por el área de Seguridad de la Información con la finalidad exclusiva recogida en el contrato de relación.

A la finalización de la relación contractual con la empresa, las unidades extraíbles facilitados al proveedor para el desarrollo de sus funciones deberán ser devueltos.

El uso y almacenamiento de información en unidades extraíbles y la manipulación de los soportes estará regulado mediante la normatividad establecida por COS S.A.S.

Se prohíbe el acceso a la documentación de COS S.A.S, ubicada tanto en medios magnéticos o físicos, a la que no se haya dado acceso expreso para el fin descrito en la prestación del servicio contratado.

Sobre los intercambios de información realizados entre el proveedor de servicio y COS S.A.S se

establecerán, en función de la criticidad considerada por COS S.A.S controles normativos, procedimentales y técnicos que protejan el intercambio de dicha información.

7.10. Intercambio de información

El intercambio de información y el tratamiento de esta, quedará regulado mediante el correspondiente acuerdo o contrato de relación entre COS S.A.S el proveedor y/o contratista receptor de la misma.

En los casos en los que la prestación del servicio incluya el tránsito de información, se implementarán por parte del proveedor o contratista los controles normativos y técnicos que eviten el uso indebido o el deterioro de esta. COS S.A.S se reservará el derecho de auditar estos controles o requerir la implementación de protecciones adicionales.

COS S.A.S podrá requerir que la información transmitida mediante mensajería electrónica esté adecuadamente protegida por parte del proveedor y/o contratista, requiriendo el cumplimiento de una normativa específica y/o la implementación de controles técnicos auditables.

Se prohíbe la transmisión de información de COS S.A.S a otras organizaciones. En caso de necesidad para la prestación del servicio contratado, el proveedor de servicio deberá solicitar a COS S.A.S la debida autorización y estará vinculada la información en los acuerdos contractuales de ambas partes.

En función de los niveles de clasificación y los requerimientos legales establecidos, COS S.A.S solicitará controles de seguridad específicos y que podrían ser auditados.

7.11. Supervisión

Se realizarán, por parte de COS S.A.S, controles para verificar que los requerimientos de seguridad establecidos de forma previa a la prestación de servicio han sido implementados correctamente y se mantienen en el tiempo.

Los servicios prestados serán supervisados y revisados periódicamente, en función del tipo de servicio se podrán establecer auditorías de cumplimiento.

COS S.A.S dispondrá de elementos de monitorización que permitan la auditoría de las actividades, las excepciones y eventos de seguridad del proveedor o contratista en función de las necesidades de la organización, disponiendo de estos registros durante el tiempo que se considere con el fin de servir como prueba forense y/o en la supervisión del control de accesos.

Se supervisará el uso de los sistemas de información, por parte del proveedor o contratista y esta información se tratará periódicamente.

Las actividades de administración y operación que pudieran ser realizadas por parte del proveedor o contratista de servicio sobre los sistemas de información COS S.A.S serán registradas.

7.12. Acceso de la RED

El proveedor y/o contratista únicamente tendrá acceso a aquellos recursos de red, aplicaciones e información que sean necesarios para el desempeño de las labores propias del servicio contratado. Los derechos de acceso a la misma serán los mínimos posibles en función de dichas necesidades. Las reglas de control de accesos se establecerán de acuerdo con la “necesidad de saber”.

Se proporcionará al proveedor acceso a los servicios de red requeridos para la prestación del servicio contratado.

Las conexiones externas de un proveedor y/o contratista a la infraestructura tecnológica de COS S.A.S, deberán ser previamente validadas. En función del análisis del riesgo a la conexión, se requerirán controles de seguridad auditables.

Se prohíbe el acceso físico y lógico a los puertos de diagnóstico y de configuración de la infraestructura tecnológica de COS S.A.S, en caso de requerirse por definición del servicio, se registrarán dichos accesos.

Con base a la arquitectura de red segregada, las conexiones a las mismas se realizarán en función de las necesidades concretas de conectividad para la prestación del servicio. Se prohíbe la configuración de rutas o accesos no autorizados por COS S.A.S.

El acceso a la información será restringido en función a su necesidad de conocer para los servicios contratados a cada proveedor o contratista.

7.13. Notificación e incidentes de seguridad de la informacion

El proveedor o contratista estará obligado a notificar cualquier incidente de seguridad que se produzca en la prestación del servicio. Esta notificación deberá realizarse a la mayor brevedad a través del gerente de control interno o área de Seguridad de la Información. Además, se emplearán los elementos de supervisión alertas y vulnerabilidades de que se dispone para detectar incidentes de seguridad de la información.

Cualquier punto débil, en relación con la seguridad de la información, deberá ser notificado al área de Seguridad de la Información. No se deberá intentar comprobar ningún punto débil de seguridad que sospeche que existe.

La omisión en la notificación de incidentes de seguridad de la información por parte del proveedor será tratada como un incumplimiento a lo contractual y a las políticas vigentes de COS S.A.S.

7.14. Terminación segura de la relación con el proveedor

- Al término de la relación contractual, se deberá revocar de forma inmediata todo acceso físico y lógico que se le haya otorgado al proveedor para el desempeño de sus funciones. Esto incluye, pero no se limita a: credenciales de usuario, accesos remotos, dispositivos de autenticación y permisos en instalaciones físicas o sistemas tecnológicos.
- El proveedor deberá tratar la información de **COS S.A.S** conforme a los principios de confidencialidad, integridad y disponibilidad, aplicando medidas de protección durante toda la vigencia del contrato y hasta la eliminación total de dicha información.
- Debe determinarse la propiedad intelectual de todo desarrollo, documentación, base de datos o

material generado en el marco de la relación contractual con **COS S.A.S.**

- Se garantizará que la información propiedad de **COS S.A.S** pueda ser devuelta en un formato estructurado, legible y compatible que permita su portabilidad a otros sistemas o proveedores sin pérdidas de integridad ni dependencia tecnológica.
- La finalización de la relación con el proveedor deberá quedar debidamente registrada mediante actas, listas de verificación, certificaciones y cualquier otra evidencia que respalde el cumplimiento de los controles de seguridad aplicables.
- Todos los activos proporcionados por la organización al proveedor deberán ser devueltos en condiciones adecuadas.
- En caso de que el proveedor haya procesado o almacenado información de **COS S.A.S,** se exigirá la eliminación o destrucción segura de la misma. Este proceso deberá estar debidamente documentado y aprobado por el área de seguridad de la información de cos. La destrucción deberá ser certificada mediante acta de entrega.
- Los proveedores deberán seguir cumpliendo, incluso después de finalizada la relación, las cláusulas contractuales referentes a la confidencialidad, no divulgación, no reutilización de información y otras disposiciones legales establecidas en el acuerdo original

8.POLÍTICA PARA DISPOSITIVOS MÓVILES

8.1. OBJETIVO

Con esta política se informan las condiciones de uso de los dispositivos móviles y las aplicaciones que sean necesarias para los trabajos realizados, indicando al personal autorizado las condiciones de operar los dispositivos móviles dentro de COS S.A.S. y el compromiso que conlleva utilizar el dispositivo dentro de la compañía.

8.2. ALCANCE

La presente política aplica para todo el personal interno o externo que cuente con la autorización de ingreso de dispositivo móviles, incluyendo celulares, relojes inteligentes, laptops, tabletas táctiles, reproductores digitales, cámaras fotográficas y de video, así como cualquier accesorio que permita la transferencia de información (voz, fotos, textos o video) para sus labores dentro de la compañía de **COS S.A.S.**

8.3. DESARROLLO

Las presentes Condiciones de Uso, y las Condiciones Particulares que, en su caso, le sean de aplicación. Se debe hacer un uso adecuado de los servicios y/o contenidos de las aplicaciones móviles y a no emplearlos para realizar actividades ilícitas o constitutivas de delito, que atenten contra los derechos de terceros y/o que infrinjan la regulación sobre propiedad intelectual e industrial, o cualesquiera otras normas del ordenamiento jurídico aplicable.

Es responsabilidad de tecnología hacer entrega de equipos móviles propiedad de la compañía con cifrado según la política de uso de controles criptográficos. De igual manera, el usuario será responsable de la devolución de los dispositivos móviles proporcionados por la organización en condiciones adecuadas, cuando estos dejen de ser requeridos, ya sea por finalización del vínculo contractual, desvinculación laboral. En caso de que los dispositivos contengan información confidencial, esta deberá ser transferida a la organización y eliminada de manera segura conforme a los procedimientos establecidos por el área de Seguridad de la Información.

En particular, el Usuario se compromete a no trasmitir, introducir, difundir y poner a disposición de terceros, cualquier tipo de material e información (datos contenidos, mensajes, dibujos, archivos de sonido e imagen, fotografías, software, guardar información confidencial etc.) que sean contrarios a la ley, la moral, el orden público.

Las presentes Condiciones de Uso y en su Caso, a las Condiciones Particulares que le sean de aplicación en ningún caso limitativo o excluyente, el Usuario se compromete a:

• No introducir o difundir contenidos o propaganda de carácter racista, xenófobo, pornográfico, de apología del terrorismo o que atenten contra los derechos humanos.

• No introducir o difundir en la red programas de datos (virus y software nocivo) susceptibles de provocar daños en los sistemas informáticos del proveedor de acceso, sus proveedores o terceros usuarios de la red Internet.

• No difundir, transmitir o poner a disposición de terceros cualquier tipo de información, elemento o contenido que atente contra los derechos fundamentales y las libertades públicas reconocidos constitucionalmente y en los tratados internacionales.

• No difundir, transmitir o poner a disposición de terceros cualquier tipo de información, elemento o contenido que constituya publicidad ilícita o desleal.

• No transmitir publicidad no solicitada o autorizada, material publicitario, "correo basura", "cartas en cadena", "estructuras piramidales", o cualquier otra forma de solicitación, excepto en aquellas áreas (tales como espacios comerciales) que hayan sido exclusivamente concebidas para ello.

• No introducir o difundir cualquier información y contenidos falsos, ambiguos o inexactos de forma que induzca a error a los receptores de la información.

• No suplantar a otros usuarios utilizando sus claves de registro a los distintos servicios y/o contenidos de los Portales.

• No difundir, transmitir o poner a disposición de terceros cualquier tipo de información, elemento o contenido que suponga una violación de los derechos de propiedad intelectual e industrial, patentes, marcas o copyright que correspondan a los titulares de los Portales o a terceros.

• La toma de fotografías y/o videos está prohibida dentro de las instalaciones que contengan información o contenido informático. Su realización solo será permitida y supervisada por el área de seguridad de la información.

• No difundir, transmitir o poner a disposición de terceros cualquier tipo de información, elemento o contenido que suponga una violación del secreto de las comunicaciones y la legislación de datos de carácter personal.

• No transmitir mensajes de ataque escrito o verbal (notas de voz) a los diferentes empleados de la compañía, estén o no en el grupo de difusión de la información.

• Mantener la separación de uso privado de negocio del dispositivo y no utilizar los medios proporcionados o compartidos para uso o beneficio personal.

• Reportar de manera inmediata cualquier incidente de seguridad de la información relacionado con la perdida de integridad, confidencialidad y disponibilidad de información que involucre directamente a COS.

• Proteger los dispositivos móviles del uso no autorizado. Los usuarios deberán configurar mecanismos de autenticación seguros en sus dispositivos (PIN, contraseñas complejas, reconocimiento biométrico) y activar el bloqueo automático tras períodos de inactividad (en caso de que aplique.)

• Usar los dispositivos con especial cuidado en lugares públicos, oficinas abiertas, lugares de reunión y otras áreas no protegidas para que evitar leer la información confidencial por terceros que puedan hacerlo, por ejemplo, usar filtros de pantalla de privacidad.

• No introducir o difundir contenidos o propaganda de carácter racista, xenófobo, pornográfico, de apología del terrorismo o que atenten contra los derechos humanos.

• No introducir o difundir en la red programas de datos (virus y software nocivo) susceptibles de provocar daños en los sistemas informáticos del proveedor de acceso, sus proveedores o terceros usuarios de la red Internet.

• No difundir, transmitir o poner a disposición de terceros cualquier tipo de información, elemento o contenido que atente contra los derechos fundamentales y las libertades públicas reconocidos constitucionalmente y en los tratados internacionales.

• No difundir, transmitir o poner a disposición de terceros cualquier tipo de información, elemento o contenido que constituya publicidad ilícita o desleal.

• No transmitir publicidad no solicitada o autorizada, material publicitario, "correo basura", "cartas en cadena", "estructuras piramidales", o cualquier otra forma de solicitación, excepto en aquellas áreas (tales como espacios comerciales) que hayan sido exclusivamente concebidas para ello.

• No introducir o difundir cualquier información y contenidos falsos, ambiguos o inexactos de forma que induzca a error a los receptores de la información.

• No suplantar a otros usuarios utilizando sus claves de registro a los distintos servicios y/o contenidos de los Portales.

• No difundir, transmitir o poner a disposición de terceros cualquier tipo de información, elemento o contenido que suponga una violación de los derechos de propiedad intelectual e industrial, patentes, marcas o copyright que correspondan a los titulares de los Portales o a terceros.

• La toma de fotografías y/o videos está prohibida dentro de las instalaciones que contengan información o contenido informático. Su realización solo será permitida y supervisada por el área de seguridad de la información.

• No difundir, transmitir o poner a disposición de terceros cualquier tipo de información, elemento o contenido que suponga una violación del secreto de las comunicaciones y la legislación de datos de carácter personal.

• No transmitir mensajes de ataque escrito o verbal (notas de voz) a los diferentes empleados de la compañía, estén o no en el grupo de difusión de la información.

• Mantener la separación de uso privado de negocio del dispositivo y no utilizar los medios proporcionados o compartidos para uso o beneficio personal.

• Reportar de manera inmediata cualquier incidente de seguridad de la información relacionado con la perdida de integridad, confidencialidad y disponibilidad de información que involucre directamente a COS.

• Proteger los dispositivos móviles del uso no autorizado. Los usuarios deberán configurar mecanismos de autenticación seguros en sus dispositivos (PIN, contraseñas complejas, reconocimiento biométrico) y activar el bloqueo automático tras períodos de inactividad (en caso de que aplique.)

• Usar los dispositivos con especial cuidado en lugares públicos, oficinas abiertas, lugares de reunión y otras áreas no protegidas para que evitar leer la información confidencial por terceros que puedan hacerlo, por ejemplo, usar filtros de pantalla de privacidad.

8.4 Control de uso de celular

Para tener control sobre el uso de celulares dentro de la compañía, entendiendo los riesgos por las posibles fugas de información, el acceso se restringe según función en la entidad y se autoriza únicamente a los siguientes cargos:

- Gerentes
- Directores
- Jefes
- Coordinadores
- Lideres
- Formadores
- Supervisores
- Reporting

Nota: El personal no autorizado para el uso de dispositivos móviles debe guardar su equipo en los LOCKER asignados o con el líder autorizado para la custodia del dispositivo mientras se ejecutan sus labores; en todo caso no debe ser manipulado en zonas operativas. Las excepciones deben ser autorizadas expresamente y deben poder ser corroboradas visualmente el carné del colaborador.

Para el personal autorizado, según el cargo en el carné teniendo en cuenta los cargos mencionados anteriormente, será inherente la aprobación de portar el dispositivo móvil (celular) dentro de la operación solo para usos corporativos, sin embargo, deberán acercaren al área de control interno para la entrega del distintivo y ser comunicado por medio de un memorando informativo la aceptación de las responsabilidades de su uso.

Para el resto de personal que no está autorizado por su cargo se deberá solicitar su autorización vía correo electrónico a la gerencia de control interno mcuevas@groupcosbpo.com con copia al jefe de sistemas de gestión Ivan.gamboa@groupcosbpo.com describiendo el nombre, cedula, cargo, campaña o área y alcance del uso del celular, esta estará sujeta a revisión de riesgos antes de su aprobación. Para el personal que se encuentre en proceso de cambio de cargo, deberá adjuntar al correo la aprobación del assesment junto con la información base ya mencionada, este personal debido a que en su carné aun no cuenta con cambios a nivel contractual por el proceso de periodo de prueba debe tener el Stickers de identificación el cual ratifica que se tiene excepciones.

La violación o incumplimiento, ya sea total o parcial, de los anteriores puntos mencionados, se califica como falta grave que dará lugar al debido proceso administrativo.

8.5. Conducta de Usuarios

COS S.A.S. no garantiza que los que hagan uso de sus dispositivos móviles utilicen los

contenidos y/o servicios de este de conformidad con la ley, la moral, el orden público, ni las presentes Condiciones Generales y, en su caso, las condiciones Particulares que resulten de aplicación. Asimismo, no garantiza la veracidad y exactitud, exhaustividad y/o autenticidad de los datos proporcionados por los Usuarios.

COS S.A.S. no será responsable, indirecta ni subsidiariamente, de los daños y perjuicios de cualquier naturaleza derivados de la utilización de los Servicios y Contenidos de la aplicación por parte de los Usuarios o que puedan derivarse de la falta de veracidad, exactitud y/o autenticidad de los datos o informaciones proporcionadas por los Usuarios, o de la suplantación de la identidad de un tercero efectuada por un Usuario en cualquier clase de actuación a través de las aplicaciones móviles por lo tanto, el uso del dispositivo no implica la obligación por parte de COS S.A.S. de comprobar la veracidad, exactitud, adecuación, idoneidad, exhaustividad y actualidad de la información suministrada a través de las aplicaciones o móviles.

COS S.A.S. no se responsabiliza de las decisiones tomadas a partir de la información suministrada a través de las aplicaciones ni de los daños y perjuicios producidos en el Usuario o terceros con motivo de actuaciones que tengan como único fundamento la información obtenida en las aplicaciones o moviles.

COS S.A.S garantiza que los controles aplicados a los usuarios con autorización de uso de dispositivos móviles perseveran las disponibilidad, integridad y confidencialidad de la información. Teniendo en cuenta que el incumplimiento de la política de Seguridad de la información por el uso inadecuado de los dispositivos móviles, acarrearán procesos disciplinarios según la gravedad del incumplimiento como se determina en el reglamento interno de trabajo.

9.POLÍTICA DE CONTROLES CRIPTOGRÁFICOS

9.1 OBJETIVO

El objetivo principal de esta política es establecer los principios y los requisitos obligatorios para el uso y la gestión de la criptografía dentro de la organización. Buscamos asegurar la confidencialidad, integridad y disponibilidad de la información y los sistemas, protegiéndolos contra accesos no autorizados, modificaciones o divulgaciones.

9.2. ALCANCE

Esta política se aplica a todos los activos de información para al uso de algoritmos de cifrado como herramientas de protección y control.

9.3 RESPONSABLES

a) **Seguridad de la información:** debe velar por el cumplimiento de la presente política.

b) **Propietario de activo de información:** Debe implementar, gestionar y aplicar técnicas, herramientas de cifrado y controles criptográficos. Además, es responsable de la gestión y generación de claves.

   Clasificar la información bajo su responsabilidad.

   Determinar los requisitos de protección criptográfica para la información clasificada, basándose en la evaluación de riesgos.

c) **Personal:** Garantizar el cifrado de la información pública reservada y clasificada que traten dentro del desarrollo de sus actividades para con la compañía.

8.5 DEFINICIONES

a) Cifrado: Que está escrito con letras, símbolos o números que solo pueden comprenderse si se dispone de la clave (llave criptográfica) necesaria para descifrarlos

b) Cifrado simétrico: Utiliza la misma llave criptográfica para cifrar y descifrar información. El receptor podrá descifrar el mensaje recibido si y sólo si conoce la clave con la cual el emisor ha cifrado el mensaje.

c) Cifrado asimétrico: utiliza dos llaves diferentes y relacionadas matemáticamente para el cifrado y descifrado de mensajes. Si la información es cifrada con una llave, únicamente puede ser descifrada por otra llave. Hashing: funciones matemáticas que generan una cadena hexadecimal conocida como “digest”, “hash” o “resumen” de longitud fija a partir de un mensaje de longitud variable. Dichas funciones son unidireccionales debido a que no permiten la obtención del mensaje a partir del hash generado, mismo que en teoría es único para cada mensaje.

d) **Llaves criptográficas:** Son códigos (algoritmos) que se generan de forma automática y se guarda en un directorio especial durante la instalación. Habitualmente, esta información es una secuencia de números o letras mediante la cual, en criptografía, se especifica la transformación del texto plano en texto cifrado, o viceversa.

e) **Control de cifrado:** Mediante la evaluación de riesgos el propietario de la información y el Gerente de Seguridad de la Información y ciberseguridad, se identificará el nivel requerido de protección, tomando en cuenta el tipo y la calidad del algoritmo de cifrado utilizado y la longitud de las claves criptográficas a utilizar.

9.5. LINEAMIENTOS

La compañía debe garantizar la confidencialidad e integridad de los documentos designados como privados y/o confidenciales utilizando sistemas y técnicas criptográficas para la protección de la información. Los propietarios de los activos y sistemas de información deben implementar mecanismos de protección y control que estén alienados con esta política.

9.5.1 La Protección de claves criptográficas: Establecer la técnica o tipo de clave criptográfica para la recepción y transmisión de datos:

a) **Técnicas de clave secreta** (criptografía simétrica), cuando dos o más actores comparten la misma clave y ésta se utiliza tanto para cifrar información como para descifrarla.

b) **Técnicas de clave pública** (criptografía asimétrica), cuando cada usuario tiene un par de claves: una clave pública (que puede ser revelada a cualquier persona) utilizada para cifrar

y una clave privada (que debe mantenerse en secreto) utilizada para descifrar. Las claves asimétricas utilizadas para cifrado no deben ser las mismas que se utilizan para firmar digitalmente. Todas las claves serán protegidas contra modificación y destrucción, y las claves secretas y privadas serán protegidas contra copia o divulgación no autorizada.

9.5.2 Periodo de cifrado: Establecer el tiempo de caducidad de una clave criptográfica. Este periodo de vida útil no puede ser mayor a un (1) año.

- Establecer fechas de activación y desactivación de las claves criptográficas para que solo se puedan usar durante el periodo de tiempo definido.
- Cambiar o actualizar las claves criptográficas, incluyendo las reglas sobre cuando cambiar las claves.

1.1. Manejo y la administración de llaves de cifrado: Administrar las llaves criptográficas en procura de la prevención de modificaciones, pérdidas, divulgación o destrucción de las llaves de cifrado.

1.2. Generación de llaves y certificados digitales: Generar certificados digitales y/o llaves compartidas, públicas y privadas en máquinas ubicadas en zonas seguras con controles de acceso físico adecuados, utilizando software autorizado, por parte de personal autorizado y capacitado, siguiendo las especificaciones de seguridad del presente documento.

1.3. Validación de llaves públicas y firmas digitales: Contar con analistas capacitados con conocimientos necesarios para verificar la autenticidad de certificados, firmas y llaves públicas, con el fin de preservar la confidencialidad de la información.

1.4. Distribución de llaves: Establecer canales seguros con clientes, terceros, sucursales o áreas de la organización, para la entrega segura de llaves criptográficas.

1.5. Almacenamiento de llaves: **C**ustodiar las llaves criptográficas de acuerdo con los riesgos asociados a las mismas, garantizando un entorno seguro con protección a nivel físico y lógico.

1.6. Copias de seguridad: generar copia de seguridad a las llaves criptografías de manera regular.

- Todas las copias de seguridad deben estar cifradas mediante las técnicas criptográficas definidas por el administrador del activo de información para garantizar que la información confidencial esté protegida.

1.7. Destrucción de llaves: Eliminar las llaves criptográficas a nivel electrónico y físico garantizando una destrucción segura de la información, impidiendo una posible recuperación futura de las mismas.

En caso de que las llaves criptográficas se vean comprometidas o si un usuario autorizado para el conocimiento de las llaves abandona la organización, deben ser revocadas o archivadas.

9.6. REGISTROS QUE REQUIEREN CIFRADO

Los registros críticos del COS se protegerán contra pérdida, destrucción y falsificación. Algunos registros pueden requerir una retención segura para cumplir requisitos legales o normativos, así como para respaldar actividades esenciales de la organización.

TIPOS DE REGISTRO	DESCRIPCIÓ CONTROL CRIPTOGRÁFICO	TIEMPO DE VIDA ÚTIL	MEDIO DE ALMACENAMIENTO	RESPONSABLE
BASES DE DATOS	Todos los sistemas que manipulan información cuentan con directivas de seguridad que aplican controles criptográficos. Toda la información digitada en las aplicaciones desarrolladas por Montechelo es cifrada en el proceso de envío hacia las bases de datos. En la comunicación se utiliza el protocolo TLS para la encriptación de las peticiones. En las bases de datos se almacenan los datos cifrados según el envío del código y los datos sensibles (determinados con anterioridad en el levantamiento del proyecto) son enmascarados en su almacenamiento en las bases de datos.	Tiempo contractual con las campañas	Almacén de llaves del servidor	DBA – Data Engineering

GRABACIONES TELECOMUNICACIONES	El proceso de encriptación se ejecuta con la aplicación de GPG. Es un derivado libre de PGP y su utilidad es la de cifrar y firmar digitalmente, siendo además multiplataforma, se cifra asimétricamente creando la pareja de claves (pública y privada) GPG nos permite elegir el tipo de clave que queremos usar, hay opciones que solo permiten firmar y otras que permiten firmar y cifrar, en este caso usamos DSA y Elgamal.	Ocho (8) días después de entregar la información al cliente.	NAS Nube	Analista de telecomunicaciones senior
VERSIONAMIENTO DE APLICACIONES	Los controles criptográficos generados automáticamente por el código de una aplicación son una forma común de autenticación en línea. Estas llaves son únicas y se generan cada vez que un usuario se autentica en la aplicación, y su única finalidad es verificar la	Una vez que la sesión finaliza o el usuario cierra la aplicación, el token deja de existir inmediatamente. Esto significa que los tokens son	N/A	Líder de desarrollo

	identidad del usuario para la sesión en curso. Es importante destacar que las llaves no se almacenan en ningún momento. Una vez que el usuario se autentica con éxito, el token se genera automáticamente y se envía al servidor. El servidor verifica la llave y si es correcta, concede acceso al usuario para la sesión en curso. En resumen, los tokens son una medida de seguridad importante que ayuda a proteger la información personal y confidencial del usuario al mismo tiempo que garantiza un acceso seguro y rápido a la aplicación.	temporales y no pueden ser reutilizados para otra sesión o propósito de autenticación.		
INFORMACIÓN CORPORATIVA - PORTÁTILES	La generación de claves de encriptación en los equipos portátiles de la compañía se realiza por medio de una GPO (política de grupo) del	La clave de encriptación sobre estos dispositivos finaliza al presentarse cualquiera de	Computador portátil	Analista de infraestructura tecnológica

	directorio activo utilizando la herramienta Bitlocker.	estos dos escenarios: Esta se elimina una vez el equipo se baja del dominio. Esta se elimina una vez el equipo es formateado.		
FILE SERVER	Son unidades de almacenamiento que se encriptan bajo una herramienta, utiliza llaves designadas para subir o visualizar la información.	Tiempo contractual con las campañas, su eliminación es por medio de un método de borrado seguro.	Las llaves criptográficas del servidor (file server) son almacenadas en una unidad dentro del servidor, con un backup incremental en la nube.	Analista senior de infraestructura tecnológica Analista de infraestructura tecnológica
SFTP	Este es un protocolo transferencia de archivos seguro, donde se tiene un	Se da sobre la conexión y caduca una	Disco storage del servidor	Analista de infraestructura tecnológica

	método de encriptación AES 256 sobre el canal de conexión. Al usuario se le asigna un usuario y contraseña / cliente externo para el ingreso a realizar la gestión sobre la información ya sea que le compartan o que el comparta con la operación.	vez la campaña se da de baja o se eliminan los usuarios de la campaña.		
VPN	Las VPN SSL permiten el acceso remoto seguro a la red corporativa de COS mediante un túnel cifrado con protocolo SSL/TLS, protegiendo la integridad de los datos. Para garantizar la seguridad, es esencial que los dispositivos cumplan con estrictas políticas de seguridad, como sistemas operativos compatibles, validación mediante herramientas como Host Check de Fortinet y autenticación multifactor (MFA). Estas medidas aseguran que solo	Con caducidad periódica controlada de contraseñas de cada 30 días, entiéndase como cambio de contraseña de usuario de red.	N/A	Administrador de redes y conectividad

	dispositivos seguros y actualizados puedan acceder a la red, reduciendo el riesgo de brechas de seguridad y accesos no autorizados.			

10.POLITICA DE USO DE CORREO ELECTRONICO

10.1. OBJETIVO

Establecer las directrices para el uso adecuado, seguro y responsable del correo electrónico corporativo, con el fin de proteger la confidencialidad, integridad y disponibilidad de la información que se transmite por este medio, prevenir el uso indebido y reducir los riesgos asociados a la pérdida o fuga de información.

10.2. ALCANCE

Esta política aplica a todos los colaboradores de COS S.A.S que tengan acceso al correo electrónico corporativo, independientemente de su nivel jerárquico. Incluye el uso del correo electrónico en dispositivos corporativos y personales cuando estos se utilicen para fines laborales y estén aprobados.

10.3. RESPONSABLES

Todo empleado con acceso a una cuenta de correo electrónico corporativo es responsable de su uso conforme a esta política, asegurando en todo momento un manejo adecuado y seguro del servicio.

10.4. DEFINICIONES

- Correo electrónico corporativo: servicio de mensajería electrónica proporcionado por la organización para fines laborales, identificado generalmente por un dominio institucional (ej. usuario@empresa.com).
- Información sensible: cualquier dato que, si se divulga, modifica o elimina sin autorización, pueda afectar la confidencialidad, integridad o disponibilidad de la información de la organización. Incluye, entre otros, datos personales, financieros, estratégicos o protegidos por ley.

- Firma electrónica corporativa: identificación estandarizada al final de cada correo que incluye el nombre, cargo, datos de contacto del remitente y, en algunos casos, un aviso legal o de confidencialidad.
- IMAPS (Internet Message Access Protocol Secure): protocolo seguro para la recepción de correos electrónicos que permite acceder a los mensajes directamente desde el servidor, manteniéndolos almacenados en él. Utiliza cifrado SSL/TLS para proteger la información durante la transmisión.
- POP3S (Post Office Protocol version 3 Secure): protocolo seguro para la descarga de correos electrónicos desde un servidor al dispositivo local. A diferencia de IMAPS, normalmente elimina los mensajes del servidor una vez descargados. También emplea cifrado SSL/TLS para proteger la información transmitida.
- SMTPS (Simple Mail Transfer Protocol Secure): protocolo seguro para el envío de correos electrónicos. Utiliza cifrado SSL/TLS para garantizar que los mensajes enviados no puedan ser interceptados ni modificados durante su transmisión.
- Activo de información: cualquier recurso que tenga valor para la organización en términos de información. Puede incluir datos, sistemas, aplicaciones, bases de datos, infraestructura tecnológica, documentos electrónicos, y otros elementos que almacenen, procesen o transmitan información.

5.LINEAMIENTOS

Se asignará una cuenta de correo electrónico a los colaboradores de COS S.A.S dependiendo de sus funciones cuya propiedad únicamente pertenece a la compañía y/o al cliente si es el caso y son asignados exclusivamente como herramienta de trabajo en desarrollo del contrato de marco de prestación de servicios celebrado entre las partes.

Por lo tanto, se relacionan a continuación los deberes de los colaboradores y las prohibiciones.

- El empleado al que se le asigne la cuenta de correo electrónico acepta la responsabilidad sobre el cuidado y buen uso que debe tener sobre la dirección de correo electrónico, su usuario y contraseña asignada, los cuales son personales e intransferibles, no podrá cederla a ningún título y hacerse sustituir por terceros en la utilización de esta ni en el ejercicio de los derechos que se le confiere.
- A través del correo electrónico asignado al usuario para el desarrollo de sus funciones, no podrá recibir ni enviar mensajes de contenido, suscripción y/o asuntos personales que no sean en el desarrollo del objeto del contrato.
- No enviar información incompleta, errónea, carente de veracidad, sin soportes que lo sustenten y sin autorización previa de la compañía.
- No atentará contra el buen funcionamiento del correo electrónico, usuario o contraseña asignados.
- No divulgará las claves de acceso (Identificación o Perfil de Usuario y Contraseña) debido a que las mismas son personales e intransferibles, siendo responsable de su uso.
- Las contraseñas de correo son administradas por el área de Soporte y es su responsabilidad no divulgar las claves de correo electrónico y hacer el uso adecuado de las credenciales.
- Se abstendrá de cambiar, modificar, o eliminar cualquier tipo de información confidencial de la compañía de la cuenta de correo electrónico asignado.
- Evitará cargar documentos y/o archivos que puedan contener información maliciosa y/o virus.
- No enviara información de la compañía a correos personales.
- La información confidencial preferiblemente debe ir con clave de acceso.

- Será responsable por los daños y perjuicios ocasionados a la compañía por el uso indebido del mismo.
- El usuario tiene prohibida la destinación de dichos programas para actividades que salgan del rango de sus funciones, so pena de responder frente a terceros por el uso indebido de los mismos.

- La sincronización de clientes de correo se realizará únicamente con protocolos seguros, POP3S, IMAPS, SMTPS.
- En el protocolo POP3S es responsabilidad de los usuarios la custodia y confidencialidad de los archivos de datos de clientes de correo.
- En el protocolo IMAPS es responsabilidad del administrador del correo la custodia, confidencialidad y respaldo de la información.
- La firma corporativa debe reflejar de forma el nombre del titular de la cuenta de correo electrónico, con el fin de asegurar la correcta identificación del remitente. No se permite el uso de firmas que representen a terceros, seudónimos, nombres genéricos o cualquier otra denominación distinta al propietario legítimo del correo.
- En los mensajes de correo electrónico que contengan información confidencial se debe configurar el siguiente aviso legal:

  "Este mensaje y sus anexos pueden contener información confidencial o legalmente protegida y no puede ser utilizada ni divulgada por personas diferentes a su destinatario. Si por error, recibe este mensaje, por favor avise inmediatamente a su remitente y destruya toda copia que tenga del mismo. Cualquier uso, divulgación, copia, distribución, impresión o acto derivado del conocimiento total o parcial de este mensaje sin autorización del GROUPCOS será sancionado de acuerdo con las normas legales vigentes. De otra parte, al destinatario se le considera custodio de la información contenida y debe velar por su confidencialidad, integridad y privacidad. Las opiniones contenidas en este mensaje electrónico no relacionadas con la actividad de esta empresa no necesariamente representan la opinión de GROUPCOS"

- Los colaboradores deben reportar de manera inmediata cualquier incidente de seguridad que afecte la confidencialidad, integridad y disponibilidad de la información al área de seguridad de la información a través de correo osi@groupcos.com.co

4.10. Protección de la privacidad de los datos

Garantiza la protección de la información de acuerdo con las leyes vigentes en materia de protección de la privacidad de los datos y reconocerá la titularidad de esta a COS S.A.S. y/o cliente si es el caso, de los correos electrónicos enviados y recibidos con sus anexos o archivos adjuntos.

5.10. Control mediante lastas blancas

Se aplica a usuarios con acceso a activos críticos, administración de activos confidenciales o considerados vitales para los clientes y consiste en restringir la posibilidad de envío de mensajes a un grupo de dominios o cuentas específicas autorizadas.

Este control lo que busca es minimizar los riegos a los que está expuesto la información confidencial de la compañía, como: bases de datos de los clientes, bases de datos propias, información sensible de los clientes, empleados o externos, imágenes, pantallazos o videos de cualquier tipo de información que se considere sensible o confidencial en la organización y garantizar el cumplimiento de la ley 1581 de 2012.

6. Uso correo electrónico dispositivos móviles u otros medios

Para tener control sobre el uso de este servicio, que es un riesgo para la compañía por las posibles fugas de información, el acceso se restringe según cargo o función en la entidad, el cual se describe de la siguiente manera:

Cargo	Categoría
Gerentes	Autorizado
Directores	Autorizado
Coordinadores	No Autorizado
Lideres	No Autorizado

Gestor de Negocios	No Autorizado
Jefes	No Autorizado
Analistas Senior	No Autorizado
Gestor Documental	No Autorizado
PQR	No Autorizado
Analistas	No Autorizado
Reclutador	No Autorizado
Recepcionista	No Autorizado
Asistente Contable	No Autorizado
Desarrolladores	No Autorizado
Supervisores	No Autorizado
Team Leader	No Autorizado
Asesor	No Autorizado
BackOffice	No Autorizado
Datamarshall	No Autorizado
Workforce	No Autorizado
Controller	No Autorizado

La violación o incumplimiento, ya sea total o parcial, de los anteriores puntos mencionados, se califica como falta grave que dará lugar al debido proceso administrativo.

11.POLITICA DE TRANSFERENCIA DE INFORMACION

11.1 OBJETIVO

Definir los lineamientos para proteger el intercambio de información entre colaboradores, áreas y terceros, por cualquier medio electrónico.

11.2 ALCANCE

Esta política aplica a toda la información contenida en los sistemas de información, bases de datos, electrónicos de la compañía, alojados en cualquier medio electrónico (servidores, estaciones de trabajo, medios de almacenamiento removibles, etc.) que requiera ser entregada.

10.3. Responsables

Todos los empleados son responsables de asegurar el debido tratamiento y cumplimiento a esta política, de los niveles de seguridad y de la adecuada transferencia de información.

10.4 Definiciones

1)Confidencialidad: Propiedad que determina que la información no esté disponible ni sea revelada a individuos, entidades o procesos no autorizados.

2)Disponibilidad: Propiedad de que la información se accesible y utilizable por solicitud de una entidad autorizada.

3)Integridad: Propiedad de salvaguardar la exactitud y estado completo de los activos.

4)Incidente de seguridad de la información: Un evento o serie de eventos de seguridad de la información no deseada o inesperada, que tienen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información.

5)SGSI: Sistema de Gestión de Seguridad de la Información, parte del sistema de gestión global, basada en un enfoque hacia los riesgos globales de un negocio, cuyo fin es establecer, implementar, operar, hacer seguimiento, revisar, mantener y mejorar la seguridad de la información.

6)SI: Seguridad de la Información, preservación de la confidencialidad, la integridad y la disponibilidad de la información; además, puede involucrar otras propiedades tales como: autenticidad, trazabilidad (Accountability), no repudio y fiabilidad.

5.11 Lineamientos

El intercambio de información de la empresa, entre organizaciones o terceras partes debe estar controlado y se deben cumplir todas las legislaciones y normas que correspondan. Para mantener una adecuada protección de la información de la organización se establecen controles de intercambio por medio de la utilización.

- Los empleados no deben enviar información sensible del proyecto por medios no autorizados.
- Los empleados no deben mantener conversaciones confidenciales en lugares públicos y oficinas abiertas.
- En caso de mantener una conversación delicada, confidencial o sensible se debe comenzar con un descargo de responsabilidad para que los presentes sepan el nivel de clasificación y los requisitos de manejo de lo que están a punto de escuchar.
- No se deben dejar mensajes en contestadores automáticos que puedan reproducirse por personas no autorizadas.
- Los empleados no deben transferir información confidencial o privada a cuentas de correos electrónicos personales.

- El envío autorizado de información confidencial, a través de llamadas, mensajería electrónica, WhatsApp o correo electrónico a cuentas aprobadas, debe realizarse mediante cifrado utilizando los métodos de seguridad establecidos.
- La transferencia de datos externa se debe realizar por medio de SFTP, se debe tener en cuenta que en caso de contingencia los envíos por mail deben ser cifrados.
- Todos los equipos de la compañía deben contar con una solución de detección y prevención de códigos maliciosos (antivirus), debe instalarse en alistamiento de equipos nuevos y verificarse en cada intervención, mantenimiento o soporte. Este punto se menciona en la política de uso de equipos tecnológicos.
- En los mensajes de correo electrónico que contengan información confidencial se debe configurar el siguiente aviso legal:
- “Este mensaje y sus anexos pueden contener información confidencial o legalmente protegida y no puede ser utilizada ni divulgada por personas diferentes
- a su destinatario. Si por error, recibe este mensaje, por favor avise inmediatamente a su remitente y destruya toda copia que tenga del mismo. Cualquier uso, divulgación, copia, distribución, impresión o acto derivado del conocimiento total o parcial de este mensaje sin autorización del GROUPCOS será sancionado de acuerdo con las normas legales vigentes. De otra parte, al destinatario se le considera custodio de la información contenida y debe velar por su confidencialidad, integridad y privacidad. Las opiniones contenidas en este mensaje electrónico no relacionadas con la actividad de esta empresa no necesariamente representan la opinión de GROUPCOS”
- El acceso a páginas y aplicaciones se determinará siguiendo el procedimiento de matriz de roles y privilegios, donde se revisará, evaluará y aprobará según el riesgo el uso de herramientas por parte del área de seguridad de la información.
- Listas blancas: se aplica a usuarios con acceso a activos críticos, administración de activos confidenciales o considerados vitales para los clientes y consiste en restringir la posibilidad de enviar correos electrónicos a uno o varios dominios externos. Ver política de uso de correo electrónico.

- La información restringida no debe ser almacenada en dispositivos móviles. Sin embargo, en el caso de que no haya alternativa y el funcionario requiera deben seguir las siguientes acciones de carácter obligatorio:
- Activar el cifrado de los datos en el dispositivo móvil y a continuación almacenar la información a ser transportada.
- Borrar la información del dispositivo móvil en el momento que ya no se requiera su almacenamiento en éste.
- Si es una memoria USB o disco duro externo, el transporte de información restringida se debe realizar mediante contenedores o espacios cifrados.
- Al guardar información restringida de COS en medios como celulares, tabletas y demás tecnologías móviles se deben activar las opciones de borrado remoto de la información almacenada en el dispositivo en caso de robo o pérdida de este, si éste las soporta.
- En caso de que el equipo soporte conexión vía bluetooth, se deben proteger estas conexiones mediante contraseña y haciendo que esta no se encuentre visible a todos los equipos.
- La información que circula en medios informáticos durante su trasporte físico debe estar protegida contra acceso no autorizado, uso inadecuado o corrupción. Ver política de traslado de equipos.
- Los colaboradores deben reportar de manera inmediata cualquier incidente de seguridad que afecte la confidencialidad, integridad y disponibilidad de la información al área de seguridad de la información a través de correo osi@groupcos.com.co

5.1.11 clasificación de la informacion

La clasificación de los activos se puede identificar con las marcas de agua de las siguientes etiquetas:

- Publico: Información que puede ser conocida y utilizada sin autorización por cualquier Persona, sea empleado de la Empresa o no. La información clasificada como pública no requiere marca de agua.

- Privado: Información que no puede ser divulgada ya que afecta la intimidad personal, intereses organizacionales y puede ser solicitada solo por autoridades judiciales.
- Confidencial: Información que sólo puede ser conocida y utilizada por un grupo de empleados para realizar su trabajo y que cuya divulgación o uso no autorizados podría ocasionar pérdidas significativas para la empresa.

5.2.11 Responsabilidad legal y consecuencias: Debido a que el uso inadecuado en la transferencia de información puede causar fuga de información restringida de la compañía o de sus clientes, los trabajadores pueden ser sujeto de sanciones que podrán llegar hasta la terminación del contrato de trabajo, sin perjuicio de las acciones legales a que haya lugar, según las leyes aplicables vigentes.

12.POLITICA DE TRASLADO DE EQUIPOS

1.12 OBJETIVO

Establecer directrices del área tecnológica para la correcta gestión, autorización y movimiento y/o traslado de equipos de la compañía asegurando su integridad y restringiendo el acceso.

2.12 ALCANCE

La presente política aplica a todos los equipos de cómputo, servidores y periféricos de la compañía e inicia con el movimiento o salida de algún dispositivo para diferentes fines. El proceso finaliza una vez las áreas involucradas del traslado den cumplimiento de las directrices establecidas.

3.12 RESPONSABLES

a. Coordinador de seguridad física
b. Jefe de soporte
c. Líder de proceso
d. Analista IT

e. Administrador de redes y conectividad

f. Administrador de redes y seguridad

g. Administrador de antivirus

4.12. DEFINICIONES

a. **Laptop:** un computador portátil o laptop es un equipo personal que puede ser transportado fácilmente. Muchos de ellos están diseñados para soportar software y archivos igual de robustos a los que procesa un computador de escritorio.

b. **Desktop:** se denomina computadora de escritorio, computador de escritorio, ordenador de sobremesa u ordenador fijo a un tipo de ordenador personal, diseñado y fabricado para ser instalado en una ubicación estática, como un escritorio o mesa, a diferencia de otras computadoras similares, como la computadora portátil, cuya ubicación es dinámica.

c. **GLPI:** software de libre distribución bajo la licencia GPL (Licencia pública General), que facilita la administración de recursos informáticos; GLPI es un software de mesa de ayuda para el registro y atención de solicitudes de servicio de soporte técnico, con posibilidades de notificación por correo electrónico a usuarios y el mismo personal de soporte, al inicio avances o cierre de una solicitud.

5.12 LINEAMIENTOS

La información que circula en medios informáticos durante su trasporte físico debe estar protegida contra acceso no autorizado, uso inadecuado o corrupción. Se deben aplicar los siguientes controles:

a. Los medios informáticos o de transporte físico de información de la empresa deben estar lo suficientemente protegidos contra robo o daño físico que pueda ocurrir durante su transporte.

b. Usar transportes o mensajeros fiables.

c. Todo equipo de red o periférico por trasladar debe ser embalado y protegido correctamente con cajas de cartón y protectores de icopor para el caso de laptop / desktop

PC o servidores críticos, los objetos más delicados deben ir embalados con papel filme industrial y/o huacas de madera de forma que se protejan contra golpes fuertes.

d. Las solicitudes de traslado de equipos deben ser formalmente presentadas por personal de mayor jerarquía, quien deberá especificar las observaciones pertinentes al traslado, incluyendo la razón del cambio de ubicación y el estado de los periféricos (como mouse, teclado, diadema). Además, estas solicitudes deberán ser revisadas para evaluar su viabilidad y, posteriormente, ser autorizadas a través del sistema GLPI por las áreas de Tecnología correspondientes.

e. Se debe realizar una verificación del segmento de red para asegurar que no se pierdan los accesos por campaña, tomando en cuenta la dirección MAC del equipo. Asimismo, se debe garantizar el acceso del usuario bajo los parámetros de navegación permitidos antes del traslado del equipo, verificando tanto la IP como la MAC. Posteriormente, se validará que la navegación del usuario sea correcta y acorde con los permisos previamente establecidos.

f. El área de IT será responsable de generar un RFC con la información detallada de los equipos a trasladar. Además, garantizará la trazabilidad del proceso mediante el almacenamiento de las evidencias correspondientes y el RFC en el sistema GLPI.

g. El área de IT debe establecer los controles adecuados para la gestión del inventario de equipos tecnológicos entre sedes o ciudades. Asimismo, debe garantizar que, en la sede de destino, se realice una inspección detallada de los equipos, a fin de verificar que coincidan con el inventario registrado, asegurando la correcta entrega y recepción de los mismos.

h. Solo personal autorizado puede abrir los equipos de cómputo y/o manipular sus componentes internos, en caso contrario será sancionado con las acciones disciplinarias a que haya lugar.

i. Si por necesidad de reparación o servicio se necesita retirar de la empresa temporalmente cualquier equipo de cómputo, es necesario que el dueño del activo notifique al coordinador de Seguridad Física mediante correo electrónico para la autorización de salida de los equipos.

j. La información que no necesita transferirse con el equipo debe eliminarse de forma segura de antes del traslado. Se debe tener en cuenta la política de borrado, entrega y destrucción de medios.

13.POLITICA USO DE EQUIPOS TECNOLOGICO

1.13 OBJETIVO

Establecer lineamientos para el uso correcto de los equipos tecnológicos (computador de escritorio, Laptop, Tablets, Celulares), asignados al personal de **COS S.A.S.**, con el propósito de velar por el buen manejo de las herramientas de trabajo suministradas por la Compañía, para proteger la información de la compañía y para el desarrollo exclusivo de las tareas asignadas dentro de los procedimientos del cargo y únicamente al interior de la empresa.

2.13 Alcance

Esta política es aplicable a todos los equipos tecnológicos proporcionados por la organización, incluyendo computadoras de escritorio, laptops, dispositivos móviles, equipos de red, y cualquier otro dispositivo utilizado para el acceso o procesamiento de información corporativa.

3.12 responsables

Todos los empleados, contratistas, proveedores y terceros que utilicen estos equipos en el marco de sus actividades laborales son responsables de asegurar el debido tratamiento y cumplimiento a esta política.

4.12. Definiciones

a. **Equipo tecnológico**: se refiere a cualquier dispositivo, herramienta o sistema que utiliza tecnología para realizar tareas específicas. En el contexto de una organización, los equipos tecnológicos son los recursos electrónicos y digitales utilizados para el procesamiento, almacenamiento, comunicación y manejo de información.

b. **Laptop:** un computador portátil o laptop es un equipo personal que puede ser transportado fácilmente. Muchos de ellos están diseñados para soportar software y archivos igual de robustos a los que procesa un computador de escritorio.

5.12 Lineamientos

a. Los equipos tecnológicos (computador de escritorio, portátil o Laptop, Tablets, Celulares), asignados al personal de COS, por ningún motivo deben salir de la compañía excepto con autorización de la gerencia de implementación.

b. Los colaboradores de COS por ningún motivo deben ingresar equipos tecnológicos personales a la operación sin autorización, ni ejecutar aplicaciones desde los mismos, de llegar ser necesarios se debe realizar la solicitud mediante correo electrónico a la gerencia administrativa y gerencia de control interno solicitando la aprobación del uso dentro de la empresa y el motivo por el cual lo requiere.

c. De no contar con el permiso se debe retirar el equipo de las instalaciones de la empresa o no continuar con el uso de este. Su ingreso es considerado falta grave en el reglamento interno de trabajo.

d. Al Ingreso de algún equipo ajeno a la compañía debe registrarse en la recepción sin excepción y almacenarse en los gabinetes o LOCKERS asignados.

e. El control de acceso a todos los sistemas o aplicativos de la compañía debe efectuarse por medio de autenticación con nombres de usuario y contraseñas únicas para cada funcionario (Log-in). Las cuentas de usuario y contraseñas son de uso personal, intransferible y privilegiado. Este punto se contémplela en la política de control de accesos físicos y lógicos.

f. Todos los equipos de la compañía deben contar con una solución de detección y prevención de códigos maliciosos (antivirus), debe instalarse en alistamiento de equipos nuevos y verificarse en cada intervención, mantenimiento o soporte.

g. Está prohibida la instalación o el uso de software no autorizado, así como la modificación de la configuración de seguridad.

h. No se permite el uso de los dispositivos para actividades ilegales, ofensivas o que violen políticas internas.

i. El acceso a la administración de los **sistemas operativos y aplicaciones** de los equipos de cómputo es restringido para todos los usuarios finales, este acceso sólo es autorizado para el personal del área de tecnología con fines exclusivamente de configuraciones de soporte, quienes deben garantizar el correcto y seguro funcionamiento de los sistemas de procesamiento de la información.

j. El acceso a páginas y aplicaciones se determinará siguiendo el procedimiento de matriz de roles y privilegios, donde se revisará, evaluará y aprobará según el riesgo el uso de herramientas por parte del área de seguridad de la información.

k. Se prohíbe el ingreso y uso de medios de almacenamiento extraíbles como; memorias USB, unidades de disco duro, tarjetas de memoria, CD y DVD. Asimismo, todos los equipos de cómputo de la compañía deberán tener bloqueados los puertos físicos destinados a dispositivos periféricos.

l. Los sistemas operativos y aplicaciones deben mantenerse actualizados con los últimos parches de seguridad, preferiblemente de forma automática o gestionada por el área de TI.

m.Se prohíbe el almacenamiento de información en el disco local C de los equipos de cómputo. Los medios de almacenamiento de información autorizados son aquellos proporcionados por COS, los cuales deben contar con un método de cifrado de acuerdo con la política de controles criptográficos.

n. Todos los usuarios deben terminar las sesiones activas cuando finalicen sus labores.

o. El usuario debe bloquear su equipo al retirarse de su área de trabajo por cualquier motivo y solo será desbloqueado por medio del usuario y contraseña de red.

p. El sistema debe bloquear automáticamente el equipo luego de tres minutos de usuario inactivo y solo será desbloqueado por medio del usuario y contraseña de red.

q. Todos los equipos de cómputo, dispositivos móviles y activos tecnológicos asignados deben ser protegidos físicamente contra pérdida, robo o daño. El personal es responsable de su custodia, tanto dentro como fuera de las instalaciones de la organización. En caso de que se presente alguno de estos

r. incidentes por mal uso de los equipos, se considerará una falta grave conforme al Reglamento Interno de Trabajo, dando lugar al inicio del debido proceso administrativo correspondiente.

s. Los colaborares que tengan un equipo portátil corporativo aginado para desempeñar sus labores dentro o fuera de la empresa por terminación de contrato o desvinculación de la empresa deben hacer la devolución del equipo y el área de soporte llevara a cabo lo definido en el procedimiento de recepción y reasignación de equipos.

t. En caso de necesitarse la eliminación de información sensible o confidencial debe realizarse conforme al procedimiento de entrega Borrado y destrucción de medios establecido por seguridad de la información.

u. Toda conexión inalámbrica en equipos corporativos deberá ser solicitada formalmente al área de Tecnología mediante la creación de un caso en la plataforma de gestión de servicios (GLPI). Esta solicitud permitirá garantizar la
correcta configuración de la red, asegurando el cumplimiento de los controles de seguridad establecidos por la organización.

14.POLITICADE AUTORIZACION DE SISTEMAS Y APLICACIONES

1.14 OBJETIVO

Establecer los lineamientos y verificación de los sistemas y aplicaciones dentro de la organización, asegurando que solo aquellos que han sido debidamente evaluados y aprobados sean implementados y utilizados.

2.14. ALCANCE

Este procedimiento aplica para todas las solicitudes de sistemas y aplicativos para poner en producción dentro de la compañía.

3.14. RESPONSABLES

a. **Seguridad de la información**: encargados de evaluar y revisar la seguridad informática de los nuevos aplicativos y sistemas para ser autorizados antes de la implementación de estos en la compañía.
b. **Tecnología:** responsables de la implementación e instalación de nuevos sistemas y aplicaciones autorizados en la organización.

4.14. DEFINICIONES

a. **Sistemas:** en el contexto de tecnología de la información (TI), un sistema informático o sistema de software se compone generalmente de hardware, software y datos que interactúan para cumplir con una función específica dentro de una organización.
b. **Aplicaciones:** una aplicación (también conocida como software de aplicación) es un tipo de programa informático diseñado para realizar tareas o procesos específicos para el usuario. Las aplicaciones permiten a los usuarios realizar una amplia gama de funciones, desde la edición de texto hasta la gestión de datos, pasando por la navegación web o la realización de cálculos complejos.
c. **CVEs:** CVEs son un estándar para la identificación de vulnerabilidades y exposiciones de seguridad en software y hardware. Un CVE es una referencia pública a una vulnerabilidad de seguridad específica en un producto o servicio. Cada CVE tiene un identificador único y público, que permite a las organizaciones y a los administradores de sistemas hacer un seguimiento, abordar y mitigar los riesgos de seguridad relacionados con esa vulnerabilidad.
d. **Software:** el software es un conjunto de instrucciones, programas y datos que permiten a un dispositivo (como una computadora o un smartphone) realizar tareas o resolver problemas específicos.
e. **Antivirus:** es un tipo de software diseñado para detectar, prevenir y eliminar programas maliciosos (como virus, troyanos, malware, ransomware, etc.) de un sistema informático.

1. LINEAMIENTOS

a. Para los sistemas de información de información nuevos, actualizaciones y nuevas versiones se deben establecer programas de prueba para aceptación y criterios de aceptación relacionados antes de su aprobación y uso.
b. Todos los sistemas y aplicaciones solicitados para su uso dentro de la organización y que requieran instalación en los sistemas de COS deben ser sometidos a una rigurosa revisión bajo el enfoque de “confianza cero”, que implica “nunca confiar y siempre verificar”. Se debe tener en consideración, la necesidad, la procedencia y la solicitud por parte del cliente (según aplique).
c. Todas las campañas y/o áreas solicitantes del uso o instalación de aplicativos y sistemas deben contar con la matriz de roles y privilegios actualizada y aprobada por seguridad de la información.
d. Se debe revisar el funcionamiento del aplicativo, validación de código en caso de ser desarrollo externo o interno, que permisos y que tipo de alcance requiere en un sistema.
e. Se debe verificar si el producto requiere una licencia para su funcionamiento. En caso afirmativo, se solicitará al creador de la solicitud que proporcione la información del proveedor de la licencia.
f. Se debe verificar la reputación de la aplicación o CVEs, asegurándose de que cuente con certificados válidos y actualizaciones de seguridad vigentes.
g. Todos los instaladores deben ser revisados en un entorno seguro aislado de la red (Sandbox) para ejecutar el escaneo de vulnerabilidades con las herramientas establecidas antes de su aprobación y uso.
h. Las páginas web y servidores serán sometidos al escaneo de vulnerabilidades según solicitud de acuerdo con el procedimiento de identificación, análisis y remediación de vulnerabilidades.
i. Las autorizaciones de aplicaciones o sistemas deben especificar cualquier tipo de condición para la instalación de estos.

j. No se aprueba ningún sistema o aplicación que represente un riesgo potencialmente malicioso para la compañía o que sea para uso ajeno a las actividades de la empresa.

k. Los instaladores de software aprobados por seguridad de la información serán almacenados en la ruta compartida con el área de tecnología, personal encargado y autorizado para realizar la instalación de software en los equipos de cómputo de COS.

15.POLITICA USO DE WHATSAPP

1.15. Objetivo

La presente política está dirigida al personal de COS S.A.S. y establece las directrices para el uso de WhatsApp Web. Su objetivo es controlar el uso de esta herramienta dentro de la compañía, para evitar posibles fugas de información y proteger tanto la información interna como externa a la que tienen acceso los colaboradores de COS S.A.S. Además, busca minimizar los incidentes de seguridad derivados de la utilización de este tipo de software, el cual facilita la filtración de información y dificulta el establecimiento de medidas de control sobre los datos que se transmiten a través de estas aplicaciones.

2.15. Alcance

Esta política aplica a todos los empleados de COS S.A.S que, en el ejercicio de sus funciones, utilicen WhatsApp Web. Su cumplimiento es obligatorio cuando esta

herramienta este aprobada, se use para fines laborales o desde equipos que tengan acceso a información corporativa.

3.15 responsables

Gerencia tecnológica: es responsable de implementar, configurar y monitorear las medidas de seguridad necesarias para garantizar el uso seguro de WhatsApp Web.

Además, debe asegurar que se apliquen políticas de control para evitar fugas de información y ofrecer soporte en la gestión de incidentes.

Área de seguridad de la información: Controlar e implementar políticas de control para la seguridad de la información. Además, monitorear e identificar amenazas por medio del antivirus.

Cargos autorizados: Cumplir con los criterios de seguridad de la información con el fin de no afectar la disponibilidad, integridad y confidencialidad de la información, dando el uso corporativo a la herramienta.

4.Definiciones

- **WhatsApp Web**: extensión del servicio de mensajería WhatsApp que permite acceder a los mensajes desde un navegador web sincronizado con el dispositivo móvil del usuario. Su uso en entornos corporativos debe estar regulado para prevenir riesgos de seguridad y fugas de información**.**
- **Fuga de información:** pérdida, divulgación no autorizada o exposición de información confidencial o sensible, ya sea de forma intencional o accidental, que puede afectar la confidencialidad, integridad o disponibilidad de los activos de información de la organización**.**
- **Ley 1581 de 2012:** normativa colombiana que establece disposiciones generales para la protección de datos personales. Regula el tratamiento, almacenamiento y circulación de datos, y exige a las organizaciones implementar medidas para garantizar los derechos de los titulares de la información.
- **Firewall:** dispositivo o solución de seguridad perimetral, que permite controlar el tráfico de red, prevenir accesos no autorizados y proteger los sistemas frente a amenazas externas mediante filtros y políticas de seguridad.
- **Antivirus:** software diseñado para detectar, bloquear y eliminar programas maliciosos (malware), tales como virus, troyanos, spyware y ransomware. Es una herramienta fundamental en la protección de equipos y sistemas informáticos.

- **Malware:** (del inglés malicious software) es un término general que se refiere a cualquier tipo de software malicioso diseñado para infiltrarse, dañar, interrumpir, robar o, de otro modo, comprometer la operación normal de sistemas informáticos, redes o dispositivos.
- **Incidente de seguridad:** cualquier evento que comprometa, la confidencialidad, integridad o disponibilidad de los activos de información. Puede incluir accesos no autorizados, pérdida de dispositivos, malware, o errores humanos que afecten la seguridad de la información.

5.15 Control

Este control lo que busca es minimizar los riegos a los que está expuesto la información confidencial de la compañía, como: bases de datos de los clientes, bases de datos propias, información sensible; 2 o más datos de un cliente, funcionarios o externos (garantizar ley 1581), imágenes, pantallazos o videos de cualquier tipo de información que se considere sensible o confidencial en la organización.

- El acceso a WhatsApp Web se gestiona a través del firewall, el cual asigna permisos de forma controlada en función del usuario de red, se realizá mediante la dirección MAC del equipo. Esto permite establecer un control de acceso estático, garantizando que solo los usuarios autorizados puedan utilizar esta herramienta.
- Se encuentran implementadas políticas de prevención de pérdida de datos mediante la solución de seguridad endpoint, que permiten restringir o autorizar la transferencia de archivos. Esta aplicación de política estará sujeta al alcance solicitado para el uso del WhatsApp Web.
- La consola de antivirus es monitoreada continuamente por el equipo de seguridad de la información y seguridad técnica, permitiendo la detección de alertas y amenazas, incluyendo posibles programas potencialmente no deseados (PUA) o malware presentes en los equipos de la organización, adicional a esto genera bloqueo de las

páginas WEB categorizadas como maliciosas.

- Los accesos a WhatsApp Web, así como los bloqueos correspondientes, se gestionan mediante reglas definidas en el firewall y el control de tráfico web del antivirus

6.15 autorización

Para tener control sobre el uso de este servicio, que es un riesgo para la compañía por las posibles fugas de información, el acceso se restringe según cargo o función en la compañía, el cual se describe de la siguiente manera:

Cargo	Autorización
Gerentes	Autorizado
Directores	Autorizado
Coordinadores	Autorizado
Lideres	Autorizado
Gestor de Negocios	Autorizado
Jefes	Autorizado
Analistas Senior	Autorizado
Formadores	Autorizado
Supervisores	Autorizado
Workforce	Autorizado
Reporting	Autorizado
Recepcionista	No Autorizado
Asistente Contable	No Autorizado
Desarrolladores	No Autorizado
PQR	No Autorizado
Team Leader	No Autorizado
Asesor	No Autorizado
BackOffice	No Autorizado
Datamarshall	No Autorizado

Analistas	No Autorizado
Controller	No Autorizado
Gestor Documental	No Autorizado
Reclutador	No Autorizado

NOTA: Si se requiere excepciones a lo establecido en esta política se debe solicitar la autorización por medio de **GLPI** o correo electrónico osi@groupcos.com.co, se aplicará la política de autorización de sistemas y aplicaciones, para evaluar si es viable y no se pone en riesgo la información de la compañía. Por contingencia de trabajo en casa, se extiende la aprobación a partir de cargos medios de la compañía.

16. POLITICA DE SEGURIDAD DE LA INFORMACION EN HOMEOFFICE

1.16 Objetivo

Establecer los principios y lineamientos de seguridad de la información que deberán seguir los colaboradores de la empresa cuando trabajen en modalidad de home office debido a una contingencia de continuidad de negocio. Esta política tiene como objetivo garantizar la protección de la información sensible y la continuidad operativa de la organización ante situaciones extraordinarias

2.16. Alcance

Esta política se aplica a todos los empleados y terceras partes, que se encuentran en trabajo en casa, así como para todas las posibles estrategias de continuidad del negocio en **COS**

3.16. Responsables

- Seguridad de la información
- Gerencia de tecnología
- Gerencia de control interno

- Gerencia administrativa
- Seguridad física
- Jefes de áreas

4.16 Definiciones

- **Home Office:** Modalidad de trabajo remoto desde el domicilio del empleado, autorizada por la organización en situaciones excepcionales o de contingencia, con el fin de dar continuidad a las operaciones.
- **Contingencia:** Cualquier situación imprevista que impida el desarrollo normal de las actividades presenciales, como desastres naturales, emergencias sanitarias, fallas en la infraestructura o eventos de seguridad.
- **Dispositivo autorizado**: Equipo previamente aprobado por el área de TI para realizar trabajo remoto, que cumple con los requisitos de seguridad establecidos por la organización.
- **Política de continuidad del negocio:** Conjunto de lineamientos diseñados para mantener la operación de procesos críticos ante eventos disruptivos, dentro del cual se contempla el home office como medida de respuesta.
- **VPN (Virtual Private Network):** Red privada virtual que permite establecer una conexión segura y cifrada entre el dispositivo del usuario y la red corporativa, protegiendo la información transmitida durante el trabajo remoto.
- **MFA (Autenticación Multifactor):** Mecanismo de seguridad que requiere al menos dos factores distintos para verificar la identidad del usuario al acceder a sistemas o recursos corporativos, como contraseña y código enviado al celular. Su uso reduce significativamente el riesgo de accesos no autorizados.
- **Incidente de Seguridad de la Información:** Evento que compromete la confidencialidad, integridad o disponibilidad de los activos de información

de la organización. Ejemplos incluyen accesos no autorizados, pérdida de dispositivos, fugas de datos o ataques informáticos.

- **Cifrado:** Técnica de seguridad que convierte datos legibles en un formato codificado, inaccesible sin una clave o mecanismo de descifrado autorizado. Su propósito es proteger la información durante el almacenamiento o la transmisión, especialmente en entornos remotos.

5.15. Directrices

5.1 Es deber de todos los colaboradores de COS, responsables de procesos, dueños de riesgos, propietarios de activos de la información, responsables de controles y de planes de tratamiento de riesgos, así como custodios y usuarios de información, dar cumplimiento y mantener las mismas premisas de la política general de seguridad de la información y las políticas específicas de la organización durante las etapas de planeación, ejecución, verificación y mejora en todas las actividades en normalidad o contingencia, así mismo, durante todo el ciclo de vida de la información, en cualquier modalidad o rol organizacional, bien sea como encargado de tratamiento de datos cuando se administran datos en el marco de contratos de prestación de servicios o como responsable de tratamiento para las bases de datos en las que aplique dicho rol para COS.

5.2 Solo se permite el trabajo en casa mediante el uso de equipos de COS, con las medidas de seguridad para que se pueda acceder remotamente, utilizar aplicativos y/o gestionar sistemas que contienen información sensible y/o crítica. Las excepciones están a consideración y bajo la responsabilidad de los jefes de cada área.

5.3 En el caso que el teletrabajador realice sus funciones por medio de un equipo de propiedad privada, COS podrá verificar la seguridad de la máquina o hacer una

auditoría o investigación en el momento que se requiera (la cual se puede impedir mediante orden legal).

5.4 La gerencia de tecnología debe definir controles de inventario y salida de equipos de la organización para la modalidad de trabajo en casa, así mismo, los empleados deben recibir los equipos mediante acta de compromiso para retiro de equipos y compromiso de confidencialidad, mediante el cual se obliga a custodiar y mantener protegido tanto el equipo entregado, como la información que podrá consultar y de reportar cual evento, o incidente que ocurra con el dispositivo o la información que pueda contener o transmitir por este.

5.5 Para la salida de equipos corporativos, el responsable del activo deberá notificar al Coordinador de Seguridad Física por medio de correo electrónico, a fin de gestionar y obtener la autorización correspondiente para su retiro.

5.6 La información que no necesita transferirse con el equipo debe eliminarse de forma segura de antes del traslado. Se debe tener en cuenta la política de borrado, entrega y destrucción de medios.

5.7 Una vez el equipo de cómputo sea devuelto a la compañía, el equipo de cómputo será sujeto a auditoría y revisiones para la recepción, con el objetivo de prevenir que ingresen a las redes corporativas el ingreso de software malicioso y verificar que continúe cumpliendo los controles con los que se entregó.

5.8 Los equipos que salgan de las instalaciones de la organización deben cumplir con los mismos controles de acceso mediante contraseñas robustas de complejidad, bloqueo automático por inactividad de 180 segundos.

5.9 Los equipos de cómputo para modalidad de trabajo en casa deben contar con sistemas operativos actualizados que permitan asegurar la aplicación de todos los parches y actualizaciones, así mismos las licencias y la consola de antivirus deben contar con las actualizaciones y revisiones periódicas por el área de seguridad de la información.

5.10 En el proceso de perfilamiento de equipos para trabajo remoto, se deben aplicar los controles necesarios, incluyendo cifrado de disco para proteger la

información en caso de pérdida o robo, y carga de usuario por caché para garantizar el acceso seguro a los sistemas, incluso sin conexión directa a la red corporativa.

5.11 En los equipos de cómputo de propiedad privada se garantizará el acceso a los recursos de software de la entidad y de las campañas por medio de canales de comunicación seguros como VPN.

5.12 El acceso a los recursos de COS y los de la entidad aliada, únicamente debe realizarse mediante canales de comunicación seguros como VPN con un doble factor de autenticación (MFA) basado en token.

5.13 Las políticas de correo electrónico deben ser aplicadas mediante listas blancas y permisos sólo a dominios o cuentas autorizadas formalmente, incluyendo los usuarios que desarrollen sus actividades desde trabajo en casa.

5.14 Los equipos de cómputo para la modalidad de trabajo en casa deben tener restringida la navegación, por lo que únicamente deberá estar habilitada para acceso a los recursos de la compañía mediante la VPN, así, una vez el usuario acceda a los recursos de COS, se deben aplicar las mismas restricciones de navegación de la red local de la organización.

5.15 En los equipos de cómputo para la modalidad de trabajo en casa, únicamente se deben disponer los datos mínimos necesarios para la ejecución de la operación. No se debe permitir el almacenamiento de datos en los discos locales.

5.16 Es responsabilidad de los empleados de COS que estén bajo la modalidad de trabajo en casa cumplir con las políticas de seguridad de la información.

5.17 La información confidencial para la prestación de los servicios debe ponerse a disposición de los Asesores únicamente a través del CRM, el canal de telecomunicaciones VICIDIAL y los que el cliente haya autorizado formalmente, en coherencia, solamente la información de apoyo puede disponerse a través de servidor de archivos en carpetas compartidas de acceso exclusivo por el personal

de la campaña. Por lo tanto, no está autorizado el uso de Excel o bases en equipos en trabajo en casa.

5.18 La información sensible en los equipos a utilizar para el trabajo en casa debe ser cifrada, o enmascarada.

5.19 El equipo provisto para el desarrollo de trabajo en casa debe impedir la instalación de aplicaciones sin autorización.

5.20 El equipo provisto para el desarrollo de trabajo en casa sólo debe usarse para temas laborales.

5.21 El soporte sobre equipos en modalidad de trabajo en casa debe realizarse de forma remota con herramientas seguras, únicamente por personal autorizado del área de tecnología.

5.22 Se deben mantener los controles mediante correlacionador de logs y eventos de firewall perimetrales, adicionalmente contar con sistema concentrador de registros para el monitoreo de las actividades en las máquinas conectadas al sistema, su funcionamiento y verificación se encuentra bajo responsabilidad de Seguridad de la Información.

5.23 El área de Seguridad de la Información y la gerencia de control interno, realizará asesoría, acompañamiento, previsión de riesgos y emisión de conceptos para apoyar las decisiones de las áreas.

5.24 Se deben mantener las técnicas de monitoreo y control de calidad a todas las campañas según los objetivos de calidad y aseguramiento del servicio.

5.25 Independientemente de la modalidad, en este caso el trabajo en casa, el 100% de llamadas deben ser grabadas, en cumplimiento normal de los controles y políticas en la gestión de los servicios, con base en las condiciones contractuales pactadas con cada aliado.

5.26 Todos los empleados deben firmar un acuerdo de confidencialidad según su responsabilidad, el cual se adjunta a su historia laboral, el cual debe incluir los riesgos y responsabilidades de la modalidad de trabajo en casa.

5.27 Los equipos de cómputo de asesores utilizados para modalidad de trabajo en casa deben cumplir las políticas para asegurar las restricciones del uso de redes inalámbricas o Wi-Fi públicas, de igual manera, no deben contar con tarjeta de Red inalámbrica.

5.28 Los empleados deben comprometerse a proteger físicamente y de manera apropiada el equipo asignado. En caso de pérdida del dispositivo o de información de la compañía o cualquier aliado estratégico deben reportarlo inmediatamente a través del correo **saro@groupcos.com.co / osi@groupcos.com.co** y su jefe directo, de demostrarse responsabilidad del empleado, se realizarán los debidos descuentos con base en la reglamentación aplicable.

5.29 Los empleados deben evitar dejar expuesto el equipo o información sensible en vehículos, zonas comunes o durante traslados.

5.30 Los empleados no deben permitir que el equipo sea utilizado por terceras personas o miembros de la familia.

5.31 Los empleados no deben utilizar servicios de computación en la nube para almacenar información confidencial, por ejemplo: WeTransfer, OneDrive, Google drive, iCloud, entre otros.

5.32 Los empleados no deben utilizar el correo electrónico para procesos de los aliados externos en los que se requiera intercambiar información de clientes. Todo el manejo de información y datos personales de clientes debe realizarse a través de aplicativos y canales seguros autorizados.

5.33 Si los empleados sospechan que su usuario de acceso remoto (si aplica) ha sido comprometido, o en caso de presentarse eventos o incidentes de seguridad de la información, deben reportarlo de inmediato, a través del correo **saro@groupcos.com.co / osi@groupcos.com.co** y su jefe directo

5.34 Los empleados deben verificar que la información recibida por correo electrónico o relacionada con la descarga de aplicaciones provienen de fuentes oficiales y confiables para evitar la infección por software malicioso.

5.35 En cuanto a cargos operativos no se autoriza el intercambio de archivos con información confidencial o datos personales, a través de aplicaciones de mensajería como (WhatsApp, Telegram, Skype, entre otros).

17.POLITICA DE SEGURIDAD EN RECURSO HUMANO

1.17 OBJETIVO

Establecer los lineamientos de acuerdo con la legislación, reglamentarios y contractuales para que los empleados conozcan sus responsabilidades en cuanto a la seguridad de la información y sean aptos para los roles definidos por la compañía.

2.17. ALCANCE

La política de la seguridad de la información del recurso humano aplica para todos los colaboradores de Customer Operation Success.

3.17. RESPONSABLES

- Selección
- Contratación
- Jurídico
- Habilidades Blandas
- Seguridad de la Información

4.17 DEFINICIONES

- **Seguridad de la Información**: conjunto de medidas, políticas y procedimientos destinados a proteger la confidencialidad, integridad y disponibilidad de la información, ya sea en formato físico o digital.
- **Recurso Humano**: todo el personal vinculado a la organización ya sea de forma permanente, temporal, pasantes o terceros que accedan a los sistemas o información de la empresa.

- **Confidencialidad**: principio que garantiza que la información solo sea accesible a las personas autorizadas y evita su divulgación no autorizada.
- **Integridad**: propiedad que asegura que la información no ha sido alterada o modificada de forma no autorizada, manteniendo su exactitud y completitud.
- **Disponibilidad**: garantía de que la información y los sistemas están accesibles y utilizables cuando se necesiten.
- **Acceso a la Información**: permiso otorgado a un individuo para consultar, modificar o administrar información según los niveles de autorización definidos por la organización.
- **Violación de la Seguridad de la Información**: cualquier incidente en el que se comprometa la confidencialidad, integridad o disponibilidad de la información.
- **Responsabilidad del Usuario**: obligación del personal de cumplir con las políticas y procedimientos establecidos para proteger los activos de información.
- **Acceso No Autorizado**: entrada, uso o manipulación de información o sistemas por parte de una persona que no cuenta con los permisos correspondientes.
- **Acuerdo de confidencialidad: c**ompromiso legal que firman los empleados o terceros para proteger la información sensible a la que tengan acceso durante su relación con la organización.
- **Ciclo de Vida del Empleado**: etapas de la relación laboral desde el reclutamiento, incorporación, permanencia y salida del empleado, durante las cuales deben aplicarse controles de seguridad.

5.LINEAMIENTOS

5.1.17 SELECCIÓN

Es deber del jefe grupo de contratación adscrito a la gerencia de selección, formación y calidad asegurar la contratación del personal idóneo para los cargos,

roles y responsabilidades estipulados dentro del Sistema de Gestión de Seguridad de la Información (SGSI) incluido el personal a tiempo completo, a tiempo parcial, temporal o recursos de proveedores externos.

Dando cumplimiento a lo anterior se deben realizar las siguientes actividades de verificación:

- Verificación de currículum vitae (CV)
- Verificación de calificaciones académicas y profesionales reclamadas
- Verificación de identidad independiente como: cedula de ciudadanía, permiso de protección temporal (PPT) u otro documento aceptable y autorizado por el estado colombiano.
- Toma de exámenes médicos ocupacionales de ingreso para cada aspirante.
- Verificación de antecedentes judiciales por medio del reporte de consulta generado por Visor judicial S.A.S. En caso de no lograr consulta por el proveedor de servicio establecido para esta actividad, se realizarán las siguientes actividades de manera temporal:
- Verificación de antecedentes disciplinarios de la Procuraduría
- Verificación de antecedentes fiscales de la Contraloría
- Verificación en registro nacional de medidas correctivas (RNMC)
- Verificación de antecedentes judiciales (PONAL)
- Verificación de reportes en entidades financieras
- Verificación de las referencias laborales y personales

- A los cargos del staff administrativo que considere necesarios se les debe realizar visita domiciliaria.
- Para quienes desempeñan funciones de seguridad de la información, es fundamental asegurarse de que sean competentes para realizar el trabajo y confiables.
- Las gerencias de cada proceso serán responsables de definir si se requieren controles de verificaciones adicionales y cuáles serían para los cargos críticos.

- En caso en las que las verificaciones no se puedan completar de manera oportuna, se debe retrasar la incorporación del aspirante a la empresa como actividad de mitigación hasta que se haya terminado la revisión previa a la firma del contrato.
- Los controles de revisión de antecedentes judiciales deben realizarse anualmente para confirmar la idoneidad continua del personal, se definen los siguientes cargos y áreas para la revisión, (sin limitarse al personal que considere seguridad de la información

Áreas	**Cargos**
- Financiero - Legal - Tecnología e innovación - Seguridad de la información - Control interno - Comercial - Seguridad física	- Gerentes - Directores - Jefes

5.2 TOMA DE CONCIENCIA, EDUCACIÓN Y FORMACIÓN EN LA SEGURIDAD DE LA INFORMACIÓN

Es deber del área de seguridad de la información diseñar las capacitaciones relativas a la seguridad de la información, para que el área de E-learning asegure su divulgación y sensibilización al ingreso y durante el desarrollo de la relación contractual de los colaboradores, con el objetivo de garantizar la toma de conciencia de las responsabilidades de seguridad de la información, cumplir con lo establecido dentro del marco legal, contractual y normativo vigente y aplicable y el conocimiento de la política de seguridad de la información

5.3. PROCESO DISCIPLINARIO

Cualquier incumplimiento de las normas establecidas en el presente documento acarrea el levantamiento de eventos y/o incidentes de seguridad de la información, los cuales conllevan a la aplicación de las medidas disciplinarias establecidas por la compañía.

Customer Operation Success basa todas las medidas sancionatorias teniendo en cuenta lo estipulado en la legislación aplicable, en la Ley 1273 de 2009, el manual del código de conducta, el reglamento interno de trabajo, procedimiento y tratamiento de incidentes de seguridad de la información, el contrato laboral y su cláusula de confidencialidad de la información, estos documentos se encuentran publicados en lugares físicos y/o virtuales con acceso permitido al 100% del personal contratado.

5.4. TERMINACIÓN LABORAL

Todo el personal que termine su relación contractual con la empresa debe entregar todos los activos de información que le han sido dispuestos para el desarrollo del objeto del contrato, legalizando los siguientes registros.

- Carta de renuncia aceptada y firmada por su jefe inmediato y el gerente del área
- En caso de tratarse de personal líder en retiro, éste debe desarrollar un acta de entrega del cargo.
- Formato paz y salvo retiro de personal
- Formato entrevista de retiro

5.5. ACUERDO DE CONFIDENCIALIDAD

El acuerdo de confidencialidad establece las responsabilidades del personal en materia de seguridad de la información. El 100% del personal deberá firmar este acuerdo de confidencialidad antes de recibir acceso a los activos de información o tecnológicos de **Customer Operation Success**. El cumplimiento de estos

acuerdos será exigible durante la relación laboral y permanecerá vigente incluso después de su finalización.

5.6.SEGREGACIÓN DE FUNCIONES

Customer Operation Success basa la creación de sus cargos y manuales de funciones, tanto operativos como administrativos, en el principio de segregación de funciones, con el objetivo de garantizar que toda acción, transacción o requerimiento generada por un funcionario, sea aprobada por otro funcionario diferente de mayor jerarquía, de tal manera que se eviten conflictos de interés y posibles eventos que atenten contra la seguridad de la información que maneja la compañía.

Por lo anterior, la alta dirección de **Customer Operation Success** delega la validación de este principio al área de seguridad de la información, y por ello estimula la trazabilidad de todas las acciones realizadas en los sistemas de operación, aplicaciones, actividades y controles.

18.POLITICA DE BORRADO Y DESTRUCCIONDE MEDIOS

1.OBJETIVO

Garantizar el cumplimiento para el retiro, destrucción, eliminación y la verificación que no se puede restablecer los activos de la información borrados y destruidos de GroupCOS, tanto a nivel físico como lógico por parte de los propietarios y/o responsables de toda la gestión de la información durante todo su ciclo de vida.

2.ALCANCE

Esta política aplica para todos los componentes y dispositivos que almacenen información física y/o lógica y que por razones de uso deban ser retirados, destruidos o eliminados.

3. RESPONSABILIDADES

- **GERENTE DE IT E INNOVACIÓN:** Aplicar aquellos métodos definidos para el retiro, borrado y destrucción de medios.
- **GERENTE DE OPERACIÓN / CUENTA:** Solicitar el requerimiento para el retiro, borrado y destrucción de medios de información de las campañas.
- **GERENTE DE ÁREA:** Solicitar el requerimiento para el retiro, borrado y destrucción de medios de información de las áreas administrativas.
- **JEFE DE OPERACIÓN:** Establecer el canal de comunicación con el cliente para solicitar el requerimiento de retiro, borrado y destrucción de medios de información de las campañas
- **SEGURIDAD DE LA INFORMACIÓN:** Revisar las actas de Entrega, Borrado y Destrucción de Medios, y registrar en la bitácora la información borrada y/o destruida.

4.DEFINICIONES

- **BORRADO SEGURO:** Medida de seguridad mediante la cual se establecen métodos y técnicas para la eliminación definitiva de datos, de modo que la probabilidad de recuperarlos sea mínima.
- **DESTRUCCION:** procedimiento necesario para garantizar que la información existente en un medio de almacenamiento no pueda ser recuperada a través de alguna técnica especializada y no pueda ser recuperada a través de alguna técnica especializada.
- **ACTIVO DE INFORMACIÓN:** Recurso del sistema de seguridad de la Información, necesario para que la empresa funcione y consiga los objetivos que se ha propuesto la alta dirección.

- **PROPIETARIO DE ACTIVO DE INFORMACIÓN**: Es el cargo que crea un activo de información y, por ende, tiene la facultad de definir su clasificación y los derechos de acceso que tienen los demás usuarios.

RESPONSABLE DE ACTIVO DE INFORMACIÓN: Es el cargo o grupo de trabajo encargado de administrar, implementar y monitorear los controles de seguridad que el propietario de los activos haya definido, con el fin de garantizar la confidencialidad, integridad y disponibilidad de la información

5.18 LINEAMIENTOS

- El borrador de la información lógica debe cumplirse según los niveles y tiempos de retención definidos en el contrato con cada cliente, y se debe realizar a través de herramientas seguras y certificadas.
- Los medios físicos (documentos) deben ser destruidos por medio de la trituradora de papel y verificados por muestro por parte de Seguridad de la Información.

  Adicional se debe disponer de los residuos de acuerdo con los lineamientos del sistema de gestión ambiental.
- Las áreas propietarias de los activos de información son responsables de dar cumplimiento a los lineamientos definidos en este documento.
- En caso de que un proveedor y/o contratista haya procesado o almacenado información de **COS S.A.S,** se exigirá la eliminación o destrucción segura de la misma. Este proceso deberá estar debidamente documentado y aprobado por el área de seguridad de la información de cos. La destrucción deberá ser certificada mediante acta de entrega. Este punto se menciona en la *política de seguridad de la información para proveedores y contratistas.*
- Antes de la reventa o donación de equipos de cómputo a organizaciones benéficas, se debe realizar el borrado seguro de la información y eliminar cualquier etiqueta o marca identificativa del activo y de COS S.A.S.

- Se debe eliminar de forma segura todos los datos de un dispositivo de almacenamiento antes de reutilizarse empleando técnicas para hacer que la información original no se pueda recuperar en lugar utilizar la función de eliminación estándar. Para la realización de esta gestión se toma en cuenta el proceso registrado dentro del *Procedimiento de Entrega, Borrado y destrucción de medios.*
- Los equipos dañados que contengan medios de almacenamiento deben pasar por una evaluación de riesgos para determinar si los elementos deben destruirse físicamente en lugar de enviarse a reparar o desecharse. Este proceso se debe realizar de acuerdo con el p*rocedimiento de disposición final de activos tecnológicos.*

19. Política de seguridad de la información

Customer Operation Success, Considera a la información como un activo de vital importancia y el aseguramiento de la información cumpliendo los requisitos aplicables, su Confidencialidad, disponibilidad e integridad de la información como prioridad para realizar con normalidad sus operaciones y actividades. Por tanto, establece los mecanismos para su protección, medios de soporte, comunicación y tratamiento de todo tipo de amenazas, las cuales pueden ser internas o externas, deliberadas o accidentales.

Customer Operation Success, garantiza el apoyo al proceso de planificación, implementación, revisión y mejora del sistema de gestión de la seguridad de la información, asumiendo con ello, el compromiso de proteger los recursos de la información.

Customer Operation Success, establece los mecanismos para respaldar la difusión y actualización, tanto de la presente política como de los demás componentes del sistema de gestión de seguridad de la información.

20.POLITICA DE GESTION DE MEDIOS REMOVIBLES

1.20. OBJETIVOS

Establecer los lineamientos para el uso y control de medios removibles, con el fin de minimizar el riesgo de pérdida, modificación y divulgación no autorizada de información.

2.20. ALCANCE

Esta política aplica a todos los colaboradores, contratistas, proveedores y terceros que tengan acceso a los sistemas de información de, recursos tecnológicos o infraestructura de la compañía.

3.20. RESPONSABLES

Todos los empleados de la compañía son responsables de conocer, comprender y aplicar las disposiciones de esta política.

Las responsabilidades específicas se detallan a continuación:

- Jefe de sistemas de información: Definir y actualizar y divulgar y hacer cumplir la política.
- Área TI: Aplicar controles técnicos que bloquean el uso de medios removibles no autorizados y administrar el acceso a SFTP.
- Empleados y terceros: Cumplir con esta política y reportar cualquier incumplimiento
- Auditoría Interna: Verificar el cumplimiento de esta política mediante controles

4.20. DEFINIDO

- **Información:** Datos relacionados con significado y propósito para la empresa.
- **Privada:** Información que no puede ser divulgada, afectando la intimidad personal o los intereses organizacionales. Solo puede ser solicitada por autoridades judiciales.

- **Confidencial:** Información de uso exclusivo para un grupo específico de empleados, cuya divulgación o uso no autorizado podría ocasionar pérdidas significativas para la empresa.
- **Pública:** Información que puede ser conocida y utilizada sin autorización por cualquier persona, sea empleado o no de la empresa.
- **Activo de Información:** Información con valor significativo y esencial para COS, que requiere protección adecuada.
- **Disponibilidad:** Garantía de acceso a la información y activos asociados por usuarios autorizados cuando lo requieran.
- **Confidencialidad:** Garantía de que la información no está disponible o divulgada a personas, entidades o procesos no autorizados:
- **Integridad:** Protección de la exactitud y el estado completo de los activos.
- **fuga de información:** define como la divulgación, acceso, copia, transmisión, robo o pérdida no autorizada de información sensible o confidencial.
- **Criptografía**: Disciplina que agrupa principios, medios y métodos para transformar datos para ocultar su contenido, establecer su autenticidad, prevenir su modificación no detectada, prevenir su repudio o uso no autorizado.
- **Cifrado:** Transformación de datos mediante criptografía para producir datos ininteligibles (cifrados) y asegurar su confidencialidad. Técnica útil para prevenir fugas de información, monitoreo no autorizado y acceso no autorizado a repositorios de información.

- **Control:** Toda actividad o proceso destinado a mitigar o evitar un riesgo. Incluye políticas, procedimientos, guías, estructuras organizacionales y buenas prácticas (administrativas, tecnológicas, físicas o legales).

- **Propietario de Activo de Información:** Cargo que crea un activo de información y tiene la facultad de definir su clasificación y los derechos de acceso.

- **Responsable de Activo de Información:** Cargo o grupo de trabajo encargado de administrar, implementar y monitorear los controles de seguridad definidos por el propietario del activo.

- **Colaboradores**: Responsable de utilizar la información para llevar a cabo sus funciones laborales.

- **Medio Removible:** Componente de hardware extraíble utilizado para el almacenamiento de información (cintas, discos duros externos, CD, DVD, unidades USB, etc.). El acceso a estos medios es controlado por el área de Infraestructura Tecnológica y el área encargada del antivirus de la compañía. Cualquier excepción debe ser avalada por la Dirección de Seguridad de la Información y sujeta a nivel contractual o aceptación de riesgos.

- **Medios Electrónicos Extraíbles:** Medios capaces de almacenar datos digitalizados, fáciles de extraer y transportar entre sistemas informáticos (Ej. CD-ROM, DVD-ROM, USB y DD externos).

5. LINEAMIENTOS PARA LA GESTION DE MEDIOS REMOVIBLES

1.Prohibición absoluta del uso de dispositivos USB u otros medios removibles físicos

En concordancia con la estrategia de seguridad de COS, el uso de memorias USB, Discos externos u otros dispositivos físicos removibles está completamente prohibido. Esta medida busca evitar fugas de información, instalación de malware y accesos no autorizados.

2.Uso obligatorio de programas seguros para la transferencia de información:

La única vía autorizada para compartir archivos o información entre usuarios o sistemas internos o externos es, será a través de plataformas seguras de transferencia, como el protocolo SFTP u otras previamente aprobadas por el área de TI y Seguridad de la Información

3.Controles técnicos obligatorios:

Se debe garantizar el bloqueo de puertos USB en los equipos de la organización mediante políticas técnicas (GPO, Software, MDM, antivirus entre otros).

Se deben implementar herramientas que detecten y reporten intentos de conexión de medios removibles no autorizados.

4.Gestión de excepciones:

Cualquier solicitud de uso temporal de medios removibles debería ser autorizada previamente por seguridad de la información mediante un proceso documentado por medio de correo electrónico. Las excepciones serán limitadas, justificadas, registradas y auditadas.

5.Auditoria y revisiones

Se realizan verificaciones periódicas para validar el cumplimiento de esta política y la eficacia de estos controles implementados. Para esto será responsable el equipo de seguridad de la información y los auditories de control interno.

6.Sanciones por incumplimiento:

Cualquier violación a esta política será tratada conforme al reglamento interno de trabajo y podrá conllevar a medidas disciplinarias.

21.POLITICA USO ACEPTABLE DE ACTIVOS DE INFORMACION

1.OBJETIVO

Establecer las directrices para el uso adecuado y responsable de la información, los sistemas de información, las redes, los dispositivos y otros activos relacionados con la información propiedad de la compañía o bajo su custodia. Esta política busca proteger la confidencialidad, integridad y disponibilidad de la información, asegurar el cumplimiento de las leyes y regulaciones aplicables, y mitigar los riesgos de seguridad.

2.ALCANCE

Esta política aplica a todos los empleados (permanentes, temporales, contratistas), consultores, terceros y cualquier otra persona que tenga acceso o haga uso de la información y los activos de la compañía independientemente de su ubicación física o el tipo de dispositivo utilizado.

3.RESPONSABLES

La aplicación y el cumplimiento de esta política es responsabilidad de todos los involucrados con la información y los activos de COS S.A.S. Los roles específicos incluyen:

- **Gerencia General:** Responsable de aprobar esta política, asegurar la provisión de recursos necesarios para su implementación y garantizar el compromiso de la organización con su cumplimiento
- **Jefe de Sistemas de Gestión:** Supervisar la implementación, mantenimiento y mejora continua de esta política y de los controles de seguridad asociados. Es el

punto de contacto para consultas y la gestión general de la seguridad de la información.

- **Propietarios de la Información:** Responsables de asegurar que la información y los activos bajo su custodia sean utilizados de acuerdo con esta política y que se apliquen los controles adecuados a su clasificación.
- **Custodios de la Información (Equipo de TI/Seguridad):** Responsables de implementar y mantener los controles de seguridad técnicos y operativos sobre los activos de información, de acuerdo con las directrices de esta política.
- **Usuarios de la Información:** Todos los empleados, contratistas y terceros que acceden o utilizan los activos de COS S.A.S son responsables de leer, comprender y cumplir con esta política, así como de reportar cualquier incidente o sospecha de uso inaceptable.

4.DEFINICIONES

Para efectos de esta política, se entenderá por:

- **Activos de Información:** Cualquier información o sistema relacionado con el procesamiento de información que tiene valor para la compañia y, por ende, necesita ser protegido. Esto incluye datos (digitales y físicos), software, hardware, redes, equipos de comunicación, servicios de TI y conocimiento de la organización.

- **Usuarios/Colaborador:** Cualquier persona sujeta a esta política que tiene acceso o hace uso de la información y los activos de COS S.A.S.

- **Uso Aceptable:** El uso de los activos de la organización de una manera que cumple con las políticas internas, las leyes aplicables y no compromete la seguridad, la integridad, la confidencialidad o la disponibilidad de la información y los sistemas.

- **Uso Inaceptable:** Cualquier uso de los activos de la organización que viola esta política, compromete la seguridad, la integridad, la confidencialidad o la disponibilidad de la información, o infringe leyes y regulaciones.

- **Confidencialidad:** Propiedad de que la información no sea puesta a disposición o sea revelada a individuos, entidades o procesos no autorizados.

- **Integridad:** Propiedad de la exactitud y completitud de la información, así como de sus métodos de procesamiento.

- **Disponibilidad:** Propiedad de ser accesible y utilizable bajo demanda por una entidad autorizada.

- **Información Confidencial:** Datos sensibles de COS S.A.S o de sus clientes, cuya divulgación no autorizada podría causar un daño significativo.

- **Dispositivos Corporativos:** Hardware (computadoras, laptops, tabletas, teléfonos móviles, etc.) propiedad de COS S.A.S o gestionado por la organización para fines laborales.

- **Phishing:** Intento fraudulento de obtener información sensible como nombres de usuario, contraseñas y detalles de tarjetas de crédito, a menudo por correos electrónicos que parecen provenir de fuentes confiables.

5.Principios Generales del Uso Aceptable

Todos los usuarios deben:

- Utilizar los activos de información de **COS S.A.S de** manera ética, legal y responsable.

- Proteger la información y los activos contra el acceso no autorizado, la divulgación, la modificación, la destrucción o la interrupción.
- Cumplir con todas las políticas y procedimientos de seguridad de la información establecidos por **COS S.A.S**
- Informar de inmediato cualquier incidente o sospecha de incidente de seguridad de la información mediante los canales autorizados.
- Entender que los activos de la organización son principalmente para fines comerciales. El uso incidental y razonable para fines personales puede ser permitido, siempre y cuando no interfiera con las responsabilidades laborales, no consuma recursos excesivos, no viole esta política o cualquier otra política de la organización, y no comprometa la seguridad.
- **6.Lineamientos Específicos de Uso**
-
- **6.1. Correo Electrónico y Comunicación**

- No utilizar el correo electrónico corporativo para actividades ilegales, no éticas, ofensivas, discriminatorias, acosadoras o que puedan dañar la reputación de la organización.
    - No enviar información **confidencial** a destinatarios no autorizados
    - No compartir información por medios no autorizados
    - Tener precaución con enlaces y archivos adjuntos de correos electrónicos sospechosos (**phishing**).
    - No utilizar la dirección de correo electrónico corporativa para suscripciones personales masivas o actividades de **spam**.

6.2. Uso de Internet y Redes

El acceso a Internet debe ser principalmente para fines relacionados con el trabajo.

No acceder, descargar, distribuir o almacenar contenido ilegal, inapropiado, ofensivo o pornográfico.

No realizar actividades que puedan causar un impacto negativo en el rendimiento de la red, como la descarga de archivos grandes no relacionados con el trabajo o el uso excesivo de ancho de banda.

No eludir los controles de seguridad de la red: firewalls, filtros de contenido etc.

No participar en actividades de piratería informática, **hacking** o cualquier forma de ciberdelincuencia.

6.3. Dispositivos y Hardware

- Solo utilizar dispositivos autorizados y configurados por **COS S.A.S para** acceder a información corporativa.
- Mantener los dispositivos físicos seguros y protegidos contra robo o daño.
- No instalar software no autorizado o sin licencia en los dispositivos corporativos.
- Reportar la pérdida o robo de cualquier dispositivo corporativo de inmediato.

6.4. Software y Aplicaciones

- Solo utilizar software y aplicaciones con licencia y aprobados por **COS S.A.S** no descargar ni instalar software de fuentes no confiables.
- Asegurar de que el software de seguridad (**antivirus, antimalware**) esté actualizado y funcionando correctamente.
- No compartir licencias de software con personas no autorizadas.

6.5. Contraseñas y Autenticación

- Utilizar **contraseñas fuertes** y únicas para todas las cuentas de la organización.
- No compartir contraseñas, estas son únicas e intransferibles

- Cambiar las contraseñas regularmente, según las directrices de Política de Control de Acceso Lógicos y Físicos de la organización.
- Bloquear el equipo o cerrar sesión cuando se aleje del puesto de trabajo.

6.6. Información Confidencial y Clasificada

- Manejar la información confidencial y clasificada de acuerdo con la política de clasificación de la información de **COS S.A.S.**
- No divulgar información confidencial a personas no autorizadas, incluyendo familiares, amigos o personal externo.
- Proteger la información confidencial tanto en formato digital como físico.
- Eliminar la información y los activos de forma segura cuando ya no sean necesarios, siguiendo los procedimientos de borrado y destrucción seguros.

6.7. Redes Sociales y Comunicación Externa

- Ejercer discreción y profesionalismo al interactuar en redes sociales.
- No divulgar información confidencial o propietaria de **COS S.A.S en** plataformas públicas.
- Si se publica contenido relacionado con la organización, dejar claro que es una opinión y no la posición oficial de la empresa.

7. Monitoreo y Auditoría

COS S.A.S se reserva el derecho de monitorear y auditar el uso de todos sus activos de información y comunicaciones, incluyendo correos electrónicos, historial de navegación, archivos y datos almacenados en los sistemas corporativos, con el fin de garantizar el cumplimiento de esta política, proteger los activos de la organización y cumplir con las obligaciones legales. Los usuarios no deben tener expectativa de privacidad con respecto al uso de los activos de la organización.

8. Consecuencias del Incumplimiento

El incumplimiento de esta Política de Uso Aceptable puede resultar en:

- **Acciones disciplinarias**, que pueden incluir la suspensión o terminación del empleo o la relación contractual.
- **Acciones legales**, si la violación implica actividades ilegales.

22. POLITICA DE PROPIEDAD INTELECTUAL

1.22 OBJETIVO

El objetivo de esta política es garantizar el cumplimiento de las normativas y acuerdos contractuales relacionados con la propiedad intelectual, con el fin de prevenir sanciones administrativas y acciones legales (civiles o penales) que puedan afectar a COS y/o a sus empleados por el incumplimiento de estas disposiciones.

2.22. ALCANCE

Esta política aplica a todo el personal de COS y a todos los activos de información existentes dentro de la compañía.

3.22 RESPONSABLES

- **Gerencia General:** Es responsable de aprobar esta política, asegurar la asignación de recursos necesarios para su implementación y garantizar el compromiso de la organización con su cumplimiento.
- **Jefe de Sistemas de Gestión:** Es responsable de supervisar la ejecución, el mantenimiento y la actualización de esta política.
- **Propietarios del Activo:** Son responsables de identificar, clasificar y proteger la propiedad intelectual bajo su cargo, asegurando la aplicación de controles adecuados y aprobando los accesos a los activos relacionados.
- **Empleados y Terceros:** Deben cumplir con esta política y reportar cualquier incumplimiento.

4.22 DEFINICIONES

- **Cliente:** Persona u organización que recibe o podría recibir un servicio
- **Software:** Conjunto de instrucciones o programas que dirigen a un ordenador para realizar tareas específicas.
- **Licencia de Software:** Contrato legal que establece los términos y condiciones bajo los cuales un usuario puede utilizar el software.

5.22 LINEAMIENTOS

5.1.22 Adquisición de Software

- Todo el software debe adquirirse a través de los canales autorizados de la organización y contar con la aprobación de las áreas de Seguridad de la Información y Tecnología.
- Cada adquisición debe verificarse y documentarse, incluyendo las licencias de uso correspondientes y asegurando que sean adecuadas para las necesidades y el modelo de negocio.
- Se debe priorizar la adquisición de software que permita escalar las operaciones de COS sin incurrir en costos de licenciamiento excesivos o limitaciones legales.
- Se debe mantener un inventario centralizado y actualizado de todo el software licenciado.
- Se debe asignar un responsable o "dueño" del activo de información para gestionar y rastrear el inventario de licencias.

5.2.22 Uso del Software

- El software licenciado solo debe ser utilizado por el personal autorizado y según los términos específicos de la licencia.
- Se prohíbe estrictamente el uso múltiple de una licencia única, la distribución o la instalación no autorizada de software.

- Se prohíbe el uso de software sin licencia o catalogado como "pirata".
- Se prohíbe la instalación de software personal o no relacionado con las actividades laborales en los equipos de la organización.
- Las licencias de suscripción o mantenimiento deben renovarse antes de su vencimiento para evitar interrupciones en el servicio y posibles incumplimientos.
- Se debe garantizar que el uso de software y recursos licenciados se alinee estrictamente con la cantidad y tipo de licencias adquiridas, evitando cualquier exceso en su utilización.

5.3.22 Formación y Concienciación

- Se capacitará a todo el personal sobre la importancia de la propiedad intelectual, los riesgos asociados al software ilegal y el uso correcto del software licenciado.
- Se comunicarán periódicamente las actualizaciones o recordatorios de la política

5.4.22 Consecuencias del Incumplimiento:

- Las sanciones disciplinarias por el incumplimiento de esta política están descritas en el reglamento interno de trabajo, y pueden variar desde una amonestación hasta la terminación del contrato, dependiendo de la gravedad de la infracción.
- Además, se informará sobre las posibles consecuencias legales para la organización y para el individuo en caso de infracciones de propiedad intelectual, tales como multas, demandas y daño a la reputación.

5.5.22 Auditorías y Verificaciones

- Se realizarán revisiones periódicas para verificar el cumplimiento de las licencias de software instaladas y en uso.

5.6. 22Revisión y Actualización

- Esta política debe ser revisada y actualizada anualmente o cuando ocurran cambios significativos en las operaciones, el marco legal o las herramientas de software, para asegurar su relevancia y efectividad.

23.POLITICA DE CLASIFICACION DE LA INFORMACION

1.23 OBJETIVO

Esta política establece el marco para la clasificación, protección y gestión de la información manejada por la compañía, con el fin de garantizar su confidencialidad, integridad y disponibilidad.

2.23 ALCANCE

Esta política aplica a toda la información que COS crea, recibe, procesa, almacena y transmite, sin importar su formato (digital, físico, verbal) o ubicación (instalaciones de COS, dispositivos remotos). Cubre a todos los empleados, contratistas, proveedores, socios comerciales y cualquier tercero que tenga acceso a la información de COS o de sus clientes, así como a todos los sistemas, aplicaciones, redes e infraestructuras utilizadas para el procesamiento de dicha información en

3.23 RESPONSABLES

La aplicación y cumplimiento de esta política es responsabilidad de todos los involucrados con la información de COS.

Los roles específicos son:

- **Gerencia General**: Asegurar la provisión de recursos, aprobar la política y garantizar su cumplimiento

- **Jefe de Sistemas de Gestión**: Supervisar la implementación, mantenimiento y mejora continua de la política y los controles asociados.

.

- **Propietarios de la Información:** Clasificar la información bajo su responsabilidad, asegurar la aplicación de controles adecuados y aprobar accesos

- **Custodios de la Información:** Implementar y mantener los controles de seguridad técnicos y operativos sobre la información, de acuerdo con su clasificación.
- **Contratación:** Asegurar que las responsabilidades de seguridad de la información sean parte de las descripciones de puesto, gestionar el proceso de inducción y desvinculación, y apoyar en la aplicación de acciones disciplinarias.

4.23 DEFINICIONES

Para efectos de esta política, se establecen las siguientes definiciones:

- **Activo de Información:** Cualquier información o sistema relacionado con el procesamiento de información que tiene valor para COS y, por ende, necesita ser protegido.
- **Confidencialidad:** Información que sólo puede ser conocida y utilizada por un grupo de empleados para realizar su trabajo y que cuya divulgación o uso no autorizados podría ocasionar pérdidas significativas para la empresa.
- **Integridad:** Propiedad de la exactitud y completitud de la información, así como de sus métodos de procesamiento.
- **Disponibilidad:** Propiedad de ser accesible y utilizable bajo demanda por una entidad autorizada.
- **Clasificación de la Información:** Proceso de categorizar la información basándose en su nivel de sensibilidad y el impacto que su divulgación, alteración o destrucción no autorizada podría tener para COS o sus clientes.
- **Propietario de la Información:** Individuo o departamento responsable de la información, quien determina su clasificación, asegura la aplicación de los controles adecuados y aprueba los accesos.

- **Custodio de la Información:** Individuo o equipo técnico responsable de la implementación y el mantenimiento de los controles de seguridad sobre la información.
- **Usuario de la Información**: Cualquier persona que accede, procesa o utiliza la información de COS.
- **Información de Autenticación**: Datos, generalmente secretos o privados, utilizados para verificar la identidad de un usuario, proceso o dispositivo (ej. contraseñas, claves, certificados, tokens, datos biométricos).
- **Necesidad de Conocer:** Principio de seguridad que establece que el acceso a la información debe limitarse estrictamente a aquellas personas que requieran dicha información para el desempeño de sus funciones y responsabilidades.
- **Mínimo Privilegio**: Principio de seguridad que establece que un usuario o proceso solo debe tener los derechos de acceso estrictamente necesarios para realizar sus tareas autorizadas.

5.23 NIVELES DE CLASIFICACION

COS establece los siguientes niveles de clasificación de la información, basados en el impacto potencial de su divulgación, alteración o destrucción no autorizada:

Tipo de Información	Impacto	Definición	Controles de Acceso	Información de Autenticación	Etiquetado
Publica	Ninguno o insignificante	Información que puede ser conocida y utilizada sin autorización por	Mínimos, enfocados en asegurar la disponibilidad y exactitud de	no requieren uso de contraseñas al ser de dominio publico	Puede no ser necesario, o etiquetado como **"Pública"**

		cualquier persona, sea empleado de la empresa o no.	la información pública. No requiere controles de acceso ni autenticación especiales		
Privada	Bajo. Inconvenientes operativos o daño menor a la reputación.	Información que no puede ser divulgada ya que afecta la intimidad personal, intereses organizacionales y puede ser solicitada solo por autoridades judiciales	Acceso basado en la necesidad de negocio para el personal de COS.	Contraseñas que cumplan con los requisitos de complejidad y longitud estándar de COS.	Se recomienda etiquetar como "**privada**"

Confidencial	Moderado a Alto. Daño significativo a las operaciones, la reputación, la situación financiera o el cumplimiento legal de COS o de sus clientes. Esta es la clasificación predeterminada para la mayoría de los datos de clientes en un entorno BPO	Información que sólo puede ser conocida y utilizada por un grupo de empleados para realizar su trabajo y que cuya divulgación o uso no autorizados podría ocasionar pérdidas significativas para la empresa.	Estrictamente limitado al personal autorizado bajo el principio de "necesidad de conocer" y "mínimo privilegio". Requiere un proceso formal de aprobación y revisión periódica de permisos. Se debe implementar la segregación de funciones cuando sea factible. Los registros de acceso deben ser monitoreados.	Contraseñas que cumplan con los requisitos de complejidad y longitud estándar de COS.	Se recomienda etiquetar como **"Confidencial"**

6.23 LINEAMIENTOS DE CLASIFICACIÓN DE LA INFORMACIÓN

6.1.23 Responsabilidades en la Clasificación de la Información

- El propietario del activo de información es el responsable principal de clasificar la información. Debe notificar a la empresa sobre la clasificación asignada para que se implementen las medidas necesarias que garanticen su disponibilidad, confidencialidad e integridad.
- Todo aplicativo o sistema de información debe tener un "**propietario**" asignado. Este propietario definirá los niveles de privacidad de la información que contenga, así como los usuarios y permisos específicos de cada uno sobre ella.
- El propietario de la información es responsable de mantener su clasificación actualizada, reflejando cualquier cambio en las operaciones, procesos o requisitos de la empresa.
- El propietario de la información puede reclasificarla cuando lo considere necesario. Al hacerlo, debe asegurar el cambio de rótulo o etiqueta y notificar a los usuarios afectados sobre la nueva clasificación.
- Los propietarios de los activos de información designarán a los responsables de dichos activos, quienes colaborarán en la gestión y el cumplimiento de las políticas de seguridad.
- Es un deber de los responsables de los activos de información clasificar la misma, siguiendo estrictamente las directrices establecidas en esta política.
- Todos los usuarios son responsables de familiarizarse y adherirse a esta política de seguridad. Si tienen dudas sobre el manejo apropiado de la información, deben consultar al propietario correspondiente.

6.2.23 Manejo y Etiquetado de la Información

- La información, datos y documentos, deben ser marcados de forma clara y visible con su nivel de clasificación, a excepción de la información pública. Esto asegura que todos los usuarios conozcan su nivel de sensibilidad.

6.3.23 La Reclasificación de la información:

La clasificación de la información debe revisarse al menos una vez al año, o cuando se cree un nuevo activo que no esté contemplado en el inventario actual. Esta revisión será coordinada por el responsable de Seguridad de la Información, junto con los dueños de los activos.

La reclasificación puede realizarse ante:

- Cambios regulatorios o contractuales.
- Modificaciones en el uso, acceso o sensibilidad de la información.
- Incidentes de seguridad o auditorías internas.

El objetivo es asegurar que la información esté correctamente clasificada y protegida conforme a su nivel de sensibilidad y a los riesgos asociados

6.4.23 Seguridad en la Transmisión y Almacenamiento

- Se deben implementar mecanismos de control de acceso a la información que sean apropiados y proporcionales a su nivel de clasificación.
- Los empleados y contratistas tienen prohibido retener o tomar información confidencial de la empresa al finalizar su vínculo laboral.
- La información clasificada como confidencial y/o privada que requiera ser transmitida por medios de comunicación públicos debe utilizar esquemas de cifrado para proteger su confidencialidad e integridad.

6.5.23 Destrucción de la Información

- Cuando la información (pública, confidencial y/o privada) ya no sea requerida, debe ser destruida siguiendo estrictamente las directrices del "Procedimiento de Entrega, Borrado y Destrucción de Medios".
- La información pública, confidencial y/o privada almacenada en medios magnéticos debe ser borrada de acuerdo con el "Procedimiento de Entrega, Borrado y Destrucción de Medios".

6.6.23Revelación de Información por Terceros

Los empleados de terceros con los que la empresa COS mantiene acuerdos comerciales no deben revelar información confidencial a otras partes, a menos que el originador de la información haya autorizado explícitamente dicha revelación y la parte receptora haya firmado un acuerdo de confidencialidad.

6.7 Revisión y Actualización

Esta política debe ser revisada y actualizada al menos una vez al año.

CONTROL DE CAMBIOS

Versión	Actualización	Elaborado por	Fecha elaboración	Fecha de revisión	Aprobado por	Fecha aprobación
07	Revisión y actualización de las políticas	Analista Compliance	17/02/2022	17/02/2022	Gerente Control Interno	17/02/202
08	Revisión y actualización de las siguientes políticas: - Política de asignación, modificación y retiro de usuarios	Analista Compliance	18/01/2023	18/01/2023	Gerente Control Interno	18/01/2023

	- Política de continuidad del negocio - Política de control de accesos físicos, lógicos y servicios y accesos a redes - Política de escritorio, pantalla limpia y usuario desatendido - Política de uso de equipos tecnológicos - Política de uso de WhatsApp Web - Política de seguridad de la información en recurso humano Se incluye la política de entrega, borrado y destrucción de medios.					
09	Se Actualización de las políticas de acuerdo con el cambio de la norma ISO 27001:2022	Analista Seguridad de la información	27/05/2025	27/05/2025	Gerente Control Interno	27/05/2025