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. POLÍTICA DE ASIGNACIÓN Y RETIRO DE USUARIOS

2.1. Objetivo

Establecer las directrices para la creación, modificación y eliminación 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 contratación del personal creando y asignando los respectivos usuarios hasta el momento de su desvinculación eliminando todos los usuarios correspondientes asignados y la interacción de novedades en temas de perfilamiento y/o modificación de accesos.

2.3. Áreas responsables

- Administración de Usuarios
- Soporte IT
- Jurídico
- Seguridad de la Información
- Formación y calidad
- Operación

2.4 Directrices

2.4.1 Ingreso

2.4.1.1 Aviso de ingreso

Se debe enviar una notificación de creación de nuevo usuario al área de Administración de Usuarios 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 Dominio que permita su control de acceso a los recursos compartidos de forma estricta.

La base de datos de usuarios y contraseñas del dominio es administrada y mantenida de forma confidencial y el área de Tecnología es la responsable de su administración.

2.4.1.2 Información de usuario contratación COS

Las cuentas de usuarios (Username o logon name) del dominio 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 (Firts 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 “User must change password at next logon”.

Nota: Validar proceso específico de creación de usuarios (Claro y otras campañas).

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 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 (Firts 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 “User must change password at next logon”.

Nota: Validar proceso específico de creación de usuarios (Claro y otras campañas).

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 - 8 a 14 caracteres (Debe contener un número, letras mayúsculas y minúsculas y un carácter especial)
- Complejidad de la contraseña - Habilitada
- Umbral de bloqueo de cuentas – 3 intentos inválido

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

2.5 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 usuarios.

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

2.6 Retiro

2.6.1 Aviso de retiro

En caso de retiro del personal de la compañía, se debe notificar al área de Administración de Usuarios mediante un GLPI en un tiempo máximo de 24 horas y enviar correo con la documentación de retiro (Carta de retiro). Esta notificación debe incluir los nombres completos del usuario, identificación (PEP o No. de pasaporte para extranjeros), motivo de retiro, fecha de retiro y campaña de esta persona.

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

2.6.2 Backup de la información en el computador

En caso de requerirse backup de la información del equipo, se debe realizar la solicitud al área de Soporte IT por medio de un caso en GLPI indicando el repositorio donde se debe almacenar la información y el motivo de la solicitud del proceso.

Este proceso es autorizado por el Director de Seguridad de la Información.

2.6.3 Backup del archivo de correo electrónico PST

El jefe inmediato solicita por medio de correo electrónico y/o caso en GLPI al área de Soporte IT el backup del archivo del correo electrónico (PST) configurado de forma local, se debe incluir este archivo en la copia de seguridad de la información del punto anterior. Si se requieren los correos para una nueva persona que reemplaza la saliente, se

configurará en el equipo las dos cuentas de correo, tanto el de la persona saliente como el de la persona entrante posterior a la autorización por parte de Seguridad de la Información.

Cuando el usuario solicite por GLPI un correo con dominio Claro, este proceso se realiza por medio del área de Administración de Usuarios.

2.6.4 Cancelación cuenta de usuario en el directorio activo

El área de usuarios da de baja en el directorio activo a los usuarios retirados. De acuerdo, a la base consolidada y recibida por medio de un caso en GLPI y los documento “Cartas retiro” reportados por correo electrónico por parte del área jurídica.

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

2.6.5 Eliminación cuenta de correo electrónico

El personal autorizado debe remitir al área de Seguridad de la Información la solicitud de eliminación de la cuenta de correo electrónico Claro por medio de un caso en GLPI.

Para los correos corporativos, el área de Jurídico envía una base general de retiros o eliminaciones por medio de correo electrónico y el área de Seguridad de la Información confirma el bloqueo o eliminación de la cuenta.

2.6.6 Referencias

Procedimiento de creación, modificación y eliminación de usuarios.

3. POLÍTICAS DE BACKUP

3.1 Política de backups de información

El siguiente manual está dirigido al personal de COS S.A., el cual implica los procedimientos y procesos a tomar en cuenta para garantizar los servicios de BACKUP de la información.

3.2 Objetivo

Contrarrestar las interrupciones en las actividades de los servidores administrados, manteniendo la integridad y disponibilidad de la información, así como protegiendo sus procesos críticos contra los efectos de fallas importantes, contra desastres y asegurando su recuperación oportuna.

3.3 Descripción del Procedimiento

3.3.1 Responsabilidades

3.3.1.1 Administradores

Es responsabilidad de los administradores de los servidores de la Red de Datos de COS conocer, adoptar e implementar la presente política de BACKUP; también son los responsables de mantener actualizadas las políticas y procedimientos consignados en este documento.

3.3.1.2 De los usuarios

Es responsabilidad de cada usuario conservar una copia de seguridad de todos sus archivos: Los usuarios son responsables por sus datos y los de los clientes finales, ya sea que los mismos se encuentren en sus máquinas.

3.3.1.3 Archivos que deben tener copia de Respaldo

1. Servidor completo (incluyendo sistema operativo) en caso de servidores virtuales.
2. Software Base (Paquete y/o lenguajes de programación con los cuales han sido desarrollados o interactúan nuestros aplicativos corporativos)
3. Software aplicativo (Considerando tanto los programas fuentes, como los programas objetos correspondientes, y cualquier otro software o procedimiento que también trabaje con los datos, para producir los resultados con los cuales trabaja el usuario final). Se deben considerar las copias de los listados fuentes de los programas definitivos, para casos de problemas.
4. Datos y estructura de datos (Bases de Datos, Índices, tablas de validación, contraseñas, tablespaces, usuarios, roles, configuraciones y todo archivo necesario para el funcionamiento de los Sistemas de Información de la compañía y la pronta recuperación de los mismos en caso de fallas).
5. Archivos generados por los sistemas y usuarios en base a su gestión o utilización.
6. Archivos de configuración de hardware de red.

3.3.2 Tipos de Respaldo

3.3.2.1 Completo

El tipo de operación de BACKUP más básico y completo es el BACKUP completo. Como su propio nombre indica, este tipo de BACKUP copia la totalidad de los datos en otro juego de soportes, que puede consistir en cintas, discos, o en un DVD o CD. La ventaja principal de la realización de un BACKUP completo en cada operación es que se dispone de la totalidad de los datos en un único juego de soportes. Esto permite restaurar los datos en un tiempo mínimo, lo cual se mide en términos de objetivo de tiempo de recuperación (RTO). No obstante, el inconveniente es que lleva más tiempo realizar un BACKUP completo que de otros tipos (a veces se multiplica por un factor 10 o más), y requiere más espacio de almacenamiento.

Por lo tanto, sólo se suelen realizar BACKUPs completos periódicamente. Los centros de datos que manejan un volumen de datos (o de aplicaciones críticas) reducido pueden optar por realizar un BACKUP completo cada día, o más a menudo aún en ciertos casos. Lo normal es que en las operaciones de BACKUP se combine el BACKUP completo con BACKUPs incrementales o diferenciales.

3.3.2.2 Incremental

Una operación de BACKUP incremental sólo copia los datos que han variado desde la última operación de BACKUP de cualquier tipo. Se suele utilizar la hora y fecha de modificación estampada en los archivos, comparándola con la hora y fecha del último

BACKUP. Las aplicaciones de BACKUP identifican y registran la fecha y hora de realización de las operaciones de BACKUP para identificar los archivos modificados desde esas operaciones.

Como un BACKUP incremental sólo copia los datos a partir del último BACKUP de cualquier tipo, se puede ejecutar tantas veces como se desee, pues sólo guarda los cambios más recientes. La ventaja de un BACKUP incremental es que copia una menor cantidad de datos que un BACKUP completo. Por ello, esas operaciones se realizan más deprisa y exigen menos espacio para almacenar el BACKUP.

3.3.2.3 Diferencial

Una operación de BACKUP diferencial es similar a un BACKUP incremental la primera vez que se lleva a cabo, pues copiará todos los datos que hayan cambiado desde el BACKUP anterior. Sin embargo, cada vez que se vuelva a ejecutar, seguirá copiando todos los datos que hayan cambiado desde el anterior completo. Por lo tanto, en las operaciones subsiguientes almacenará más datos que un BACKUP incremental, aunque normalmente muchos menos que un BACKUP completo. Además, la ejecución de los BACKUPs diferenciales requiere más espacio y tiempo que la de los BACKUPs incrementales, pero menos que la de los BACKUP completos.

3.3.3 Archivos que deben tener copia de Respaldo

1. Servidor completo (incluyendo sistema operativo) en caso de servidores virtuales.

2. Software Base (Paquete y/o lenguajes de programación con los cuales han sido desarrollados o interactúan nuestros aplicativos corporativos)
3. Software aplicativo (Considerando tanto los programas fuentes, como los programas objetos correspondientes, y cualquier otro software o procedimiento que también trabaje con los datos, para producir los resultados con los cuales trabaja el usuario final). Se deben considerar las copias de los listados fuentes de los programas definitivos, para casos de problemas.
4. Datos y estructura de datos (Bases de Datos, Índices, tablas de validación, contraseñas, tablespaces, usuarios, roles, configuraciones y todo archivo necesario para el funcionamiento de los Sistemas de Información de la compañía y la pronta recuperación de los mismos en caso de fallas).
5. Archivos generados por los sistemas y usuarios en base a su gestión o utilización.
6. Archivos de configuración de hardware de red.

3.3.4 Clasificación de la información

- **Publico**: Información que puede ser conocida y utilizada sin autorización por cualquier Persona, sea empleado de la Empresa o no.

- **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.

- **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.

Nota: alguna información física preferiblemente se sella con la información correspondiente a su tipo.

Criterio de VALOR:

- **Alta:** Esta es una información de gran sensibilidad para la compañía. Incluye, pero no está restringida a: Documentos de junta deliberaciones sobre intercambio de mercancías (COMEX), análisis estratégico, investigaciones con un impacto al material a nivel de la compañía, Balances de negocios. Los cuales si se divulgan por fuera de la compañía causarían un daño grave y perdida potencial de venta comercial o reputación para COS. Tal información tan solo se debe comunicar a un número de personas estrictamente limitado y predefinido.
- **Media:** Esta es información cuya divulgación no autorizada probablemente dañe o impacte negativamente las actividades de COS (conocimiento específico, acciones del mercado, reporte financiero interno a nivel de unidad de negocios, propiedad intelectual o legal, información confidencial de terceros, planes de negocios, etc.) Tal información no debería ser difundida ampliamente dentro de la compañía, sino que debería compartirse internamente según se necesite solamente. Ej.: Dentro de

un cierto número de personas directamente envueltas en relación a un tema o proyecto específico.

- **Baja:** Esta es información que debería retenerse dentro de COS. El acceso debería limitarse a los empleados de COS. Es probable que la información no cause perdida o daño serio a la compañía puesto que no es estratégica (ejemplo: tablas de organización, comunicación interna), pero que, no obstante, la divulgación ilimitada se debe evitar. Este es el nivel de clasificación estándar.

3.3.5 Rutinas de seguimiento y control

Para prevenir fallas en la restauración de datos de servidores, la información almacenada en los backups debe ser verificada mensualmente y en forma íntegra. Para ello se deben realizar rutinas de control de backups.

Las mismas consisten en la prueba integral de los respaldos, desde su restauración desde el servidor de backup a otro de testeo (duplicado del servidor original en producción), descompresión e importación de datos hasta las pruebas correspondientes de funcionamiento (según el sistema que se esté recuperando). Ya que, por cuestiones de volúmenes de datos y tiempos, sería imposible realizar la comprobación de todos los backups de COS, se tomarán muestras de entre 5 y 10 backups aleatoria y rotativamente, para llevar adelante este proceso.

Con esto se podrá evidenciar que los datos grabados se pueden obtener correctamente al momento de ser necesarios. Las pruebas se deberán formalizar en un acta escrita y firmada por los responsables.

3.3.6 Destrucción del BACKUP

La información en un medio de respaldo será destruida de dos formas:

1. **Reutilización del medio para otro uso**: El encargado de la administración y manejo de los BACKUPS deberá tener definido un rol para la reutilización de los medios, para esto debe llevar el control del contenido actual de cada respaldo. Cuando se reutilice la cinta se debe actualizar la información del medio.
2. **Daño físico del medio de respaldo**: Deberán hacerse en forma periódica pruebas de restauraciones de información en un área temporal con el fin de probar el buen estado del medio de respaldo. Si se comprueba que el medio tiene un daño y no puede leerse su contenido, se debe destruir físicamente y documentar su último contenido. Se debe tratar de rescatar la mínima cantidad de información y guardarla en otro medio.

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	Mantenimiento de las etapas y actividades involucradas en la	Ejecutar las diferentes actividades para

durante la contingencia y el retorno a la normalidad.	gestión de la continuidad de negocio de COS de manera permanente.	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

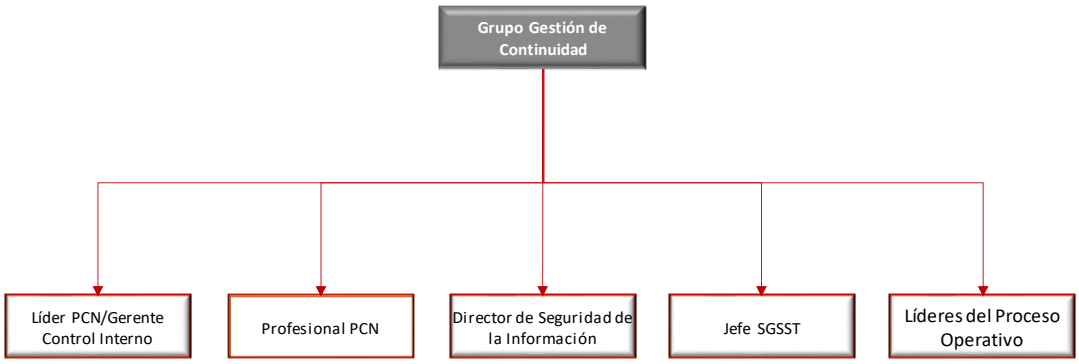
Corresponderá al Grupo Gestión de Crisis tomar Toma de decisiones en el marco de la comunicación con los grupos de continuidad, operación y crisis relacionadas con aspectos críticos de carácter legal y/o normativo, de servicio, de operación, de imagen y/o financieros que sean necesarias durante las situaciones 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

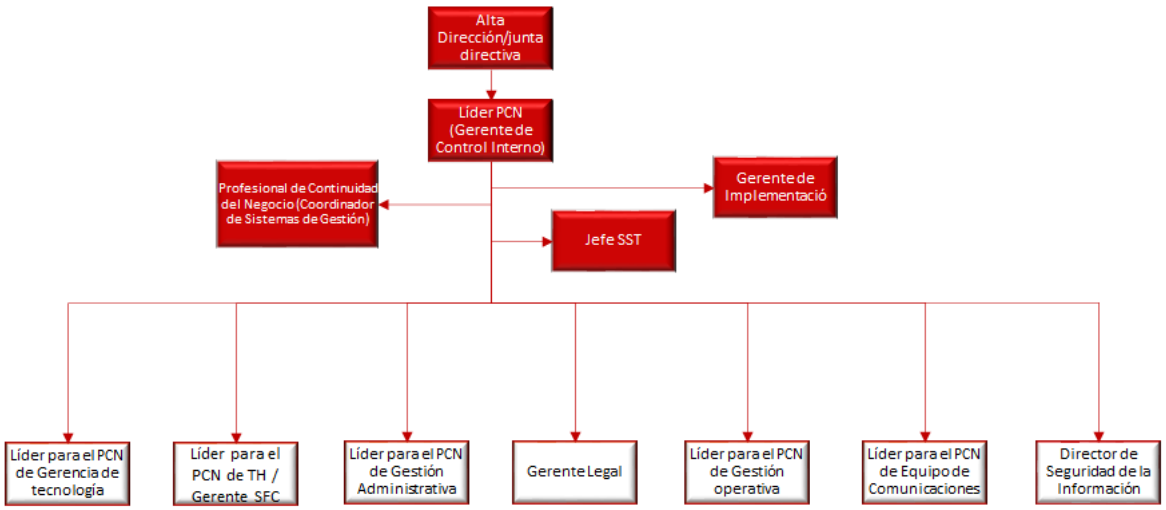
Este Grupo es el encargado de ejecutar las diferentes actividades para restablecer los procesos críticos. El Grupo Operativo, será convocado bajo la Instrucción del Grupo Gestión de Crisis; estará conformado por:

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, LÓGICOS Y SERVICIOS Y ACCESOS A REDES

5.1 Generalidades

Esta política se basa en la premisa o principio de que todo acceso está prohibido, a menos que se permita formalmente, garantizando el mínimo privilegio posible para el ingreso a las instalaciones, sistemas de información, código fuente, sistemas operativos, servicios de TI, activos a nivel de red, aplicaciones externas, y demás activos de la información de COS, con el propósito que estén disponibles única y exclusivamente para los propietarios, custodios y usuarios de la información que deban acceder para el ejercicio de sus funciones, aprobados por el director de seguridad de la información.

5.2 Objetivo

Establecer los lineamientos que aseguren únicamente los accesos físicos y/o lógicos autorizados a los activos de información, al sistema de información COS ya la información que se encuentre en el alcance del SGSI de COS.

5.3 Lineamientos

5.3.1 Responsabilidades de los usuarios:

Los usuarios de acceso a herramientas, que se entreguen son de su uso exclusivo y responsabilidad de cada usuario como responsable. Las siguientes son faltas motivo de cancelación de contrato, ya que van en contra de la confidencialidad y el buen manejo de la información:

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

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, está prohibido.

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

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, las cuales deben quedar en un anexo de este documento.

Esta información se encuentra contenida en el Formato de acta de entrega de usuarios.

Todos los funcionarios o terceros que tengan un usuario para el acceso a la información y plataforma de tecnología deberán conocer y cumplir con su uso de esta Política específica, donde se dictan pautas sobre derechos y deberes con respecto al uso adecuado de los usuarios, así como políticas de protección de usuario desatendido, escritorio y pantalla limpia.

5.3.2 Acceso físico

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

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.

Todo personal que no pertenezca a la organización debe registrarse 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, deben portar el carné de visitante de COS en un lugar visible para facilitar su identificación.

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 de un miembro de la

alta dirección o de la dirección de seguridad de la información, 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.

Está prohibido la toma de fotografías y grabaciones al interior de las instalaciones, salvo aprobación de un miembro de la alta dirección o de la dirección de seguridad de la información mediante caso cargado en la plataforma GLPI.

Cada responsable debe realizar depuraciones cuando ya no se requieran de las agendas de toma de notas las cuales no deben tener datos sensibles.

En caso de que tenga habilitado tableros 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.

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.

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.

El personal de talento humano debe otorgar el acceso físico de manera controlada al personal que se encuentra en etapa de formación y capacitación inicial para su ingreso en áreas restringidas autorizadas. Puesto 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 requerirles el uso visible del carné corporativo o del que lo identifique en proceso de formación. Para el enrolamiento de huellas y habilitación de accesos a las áreas restringidas deben seguir el protocolo establecido por el área de Talento humano.

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.

Se debe asegurar la visualización y enfoque de puntos de acceso por medio de cámaras del Circuito Cerrado de Televisión (CCTV) de COS a las áreas seguras y a tableros eléctricos.

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 y durante 5 años después de ello.

Cuando un cliente externo solicita cámaras del CCTV, se debe realizar por medio formal en la plataforma integral de procesos, a través del Gerente de cuenta. Estas solicitudes deben estar aprobadas por el(a) Coordinador(a) de Riesgos y Cumplimiento. 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 sea autorizado por el(a) Coordinador(a)

de Riesgos y Cumplimiento, la alta dirección o sea requerido por una autoridad gubernamental competente.

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.

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.

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:

- 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.
- Oficinas para atención presencial de titulares. Áreas de gestión documental.
- Salas de Juntas, y oficinas 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.

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

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.

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 o agencia respectiva.

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.

Se cuenta con seguridad perimetral en las instalaciones de COS

- Circuito de Televisión Cerrada (Cámaras) - CCTV
- Controles de Acceso y Biometría
- Torniquetes
- Celaduría Privada
- Identificación con Carné

El instructivo de seguridad física describe el proceso y controles de manera detallada.

5.3.3 Protocolo de seguridad física para la atención presencial de clientes

Todos los visitantes deben registrase en la Recepción. Si el visitante trae un equipo del listado antes mencionado se debe registrar al ingreso y salida en la recepción de las oficinas.

Ninguno de los dispositivos mencionados se puede utilizar dentro de las áreas de operación. Sólo sí cuenta con la autorización formal y escrita del(a) Coordinador(a) de Riesgos y Cumplimiento o si se trata de un requisito contractual.

El uso del celular en la operación no está autorizado en las áreas seguras.

Está prohibido la toma de fotografías y/o grabación de videos o audios al interior de nuestras instalaciones.

5.3.4 Control de acceso a la información

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.

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.

Tanto la información de los clientes de COS como la información de gestión debe tener designada un propietario, el cual es responsable de administrar y controlar el acceso a esta información. El propietario de la información debe ser un funcionario a nivel de

Gerencia o equivalente, y debe autorizar de manera formal cualquier solicitud de acceso a esta información.

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 asignada.

El(a) Gerente de IT e Innovación tiene la responsabilidad de custodiar la información almacenada en los servidores, aplicaciones, y demás sistemas de información de la organización.

Los documentos físicos que contengan información confidencial deben ser gestionados de manera controlada y organizados de acuerdo con lo descrito en el listado maestro de registros.

A nivel operativo, la autorización de acceso a los usuarios se encuentra asociada a roles y funciones asignadas autorizadas, por ello todos los usuarios registrados, son asignados a grupos con permisos predeterminados (Estos privilegios están separados por campaña).

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.

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

Cualquier tipo de conexión desde sitios externos a COS debe realizarse a través de canales cifrados.

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.

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”.

5.3.5 Política de utilización de los servicios de red

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.

5.3.6 Autenticación de usuarios para conexiones externas

La Dirección de Seguridad de la Información contempla como servicios de conexiones externas SSL, VPN y primarios para funcionarios que requieran conexión remota a la red de datos corporativa.

5.3.7 Identificación de equipos de red

La Dirección de Seguridad de la Información controlará e identificará los equipos conectados a su red, mediante el uso de controladores de dominio, asignación manual de IP o por DHCP y portal cautivo para la conexión WIFI.

5.3.8 Protección de los puertos de configuración y diagnostico remoto.

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.

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.

5.3.9 Separación de redes.

- La seguridad para las conexiones WIFI será WPa2 o superior.
- Dentro de la red de datos institucional se restringirá el acceso a:
- Mensajería instantánea.
- La telefonía a través de internet.
- Correo electrónico comercial no autorizado.
- Descarga de archivos de sitio peer to peer.
- Conexiones a sitios de streaming no autorizado.
- Acceso a sitios de pornografía.

- Servicios de escritorio remoto a través de internet.
- Cualquier otro servicio que vulnere la seguridad de la red o degrade el desempeño de la misma.

5.3.10 Control de enrutamiento de red.

La Gerencia de IT e Innovación proveerá a través de sus ISPs (Proveedor de Servicio de Internet) el servicio de internet corporativo, el cual será administrado por la Gerencia de IT e Innovación y será el único servicio de internet autorizado. El uso de internet estará regulado por la Política de Seguridad de la Información.

5.3.11 Ingreso seguro en operaciones.

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.

5.3.12 Ingresos a programas especiales

El acceso a programas especiales será autorizado y controlado por la dirección de seguridad de la información y estará sujeta a la matriz de matriz de roles y privilegios definida por la organización.

5.3.13 Creación, deshabilitación y accesos de usuarios

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.

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.

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.

5.3.14 Sistemas de autenticación usuarios

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 8 a 14 caracteres.
- La contraseña debe incluir números, letras mayúsculas y minúsculas.
- La recordación debe ser de 24 contraseñas. Debe ser cambiada mínimo cada 20 días.
- No puede repetirse la contraseña por lo menos durante los últimos 24 cambios.

- No puede contener palabras, nombres o estar relacionada con la cuenta de usuario.

5.3.15 Gestión de Identidades

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.
- No puede contener palabras, nombres o estar relacionada con la cuenta de usuario. 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.

5.3.16 Sistemas de administración de contraseñas

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

5.3.17 Gestión de derechos de acceso privilegiado

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.

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

Para ello, la Gerencia de IT e Innovación asegura estos accesos a través de firewall, cuando se trata de recursos por proyecto, y/o reglas de proxy en caso de permisos puntuales por usuario, de igual forma cuando se requiera habilitación de correo electrónico con dominio corporativo externo con previa autorización del cliente y bajo responsabilidad de los dueños del riesgo y propietarios de los activos de la información.

Cuando se requiera otorgar permisos a nuevos recursos o a recursos normalmente no autorizados por el dueño de los riesgos, la Dirección de Seguridad de la Información aprobará dichas solicitudes asegurando que las pruebas piloto a cargo de tecnología no representen riesgos para la seguridad de la información o éstos sean tratados. Teniendo en cuenta el documento de aceptación compartida de los riesgos firmado por el cliente y por COS.

5.3.18 Sistemas operativos y aplicaciones

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.

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. El uso de estas cuentas debe cumplir con el numeral de "**Gestión de Identidades**", del presente documento.

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 IT e Innovación, conjuntamente, es obligación de los colaboradores de tecnología autorizados garantizar el correcto y seguro funcionamiento sobre los activos de seguridad de la información.

5.3.19 Gestión de accesos en cambios de área o proyecto

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.

Si el colaborador tiene correo electrónico corporativo, este no será deshabilitado. Únicamente serán eliminados los permisos de salida de correo a dominios diferentes a los de COS. Conjuntamente se debe realizar entrega de información a quien ocupe el cargo o en su defecto, si el puesto anterior aún es vacante, la información debe ser entregada al jefe inmediato.

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.

5.3.20 Gestión de accesos para aplicaciones externas

En COS se permite exclusivamente para la operación del negocio aplicaciones que no son desarrolladas internamente, 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.

La Gerencia de IT e Innovación 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, debe ser notificado y autorizado por la dirección de seguridad de la información.

5.3.21 Conexiones en redes

Se debe controlar el acceso lógico a los servicios de TI, su administración y uso con las siguientes políticas:

- Cada proyecto o departamento de la organización debe contar con un segmento de red independiente, mediante el uso de VLANs.
- Cada vez que haya traslado físico de proyectos, éste debe trasladarse con el segmento de red (VLAN) asignado.
- No se deben aplicar accesos por Firewall a la VLAN del proyecto que se encontraba en el área a donde se realizará el traslado.
- El enrutamiento a través de todos los segmentos de red debe ser controlado y administrado por
- los equipos firewall de la Organización.
- Cualquier tipo de enrutamiento entre redes de la organización debe ser filtrado a través de listas de acceso. El firewall debe controlar el tráfico de los distintos segmentos de red a través de listas de acceso independientes.
- Las reglas por defecto para permitir tráfico sin restricción no son permitidas dentro de la organización.

- El acceso sin restricciones a Internet no está permitido dentro de COS. Los únicos funcionarios autorizados con tal acceso son los miembros de la Alta Dirección.
- En caso requerir acceso a páginas específicas en Internet, la Gerencia encargada debe hacer a la Gerencia de IT e Innovación una solicitud formal con la justificación del requerimiento, adicionalmente deben contar con el visto bueno de la dirección de seguridad de la información.
- Cualquier cambio de segmento de red, VLAN o en las listas de acceso de los equipos de enrutamiento debe ser autorizado por la Gerencia de IT e Innovación.
- Las redes inalámbricas deben ser independientes de la infraestructura misional y contar con seguridad WPA2-AES.

5.3.22 Revisión de derechos de acceso

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

Estas revisiones deben incluir, aunque no están limitados a las siguientes verificaciones:

- 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.

Estas revisiones deben ser objeto de verificación 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 ESCRITORIO PANTALLA LIMPIA Y USUARIO DESATENDIDO

6.1 Objetivo

Considerando que la información es el activo más importante de la empresa, se define la política de escritorio limpio, pantalla limpia y usuario desatendido, garantizando que la confidencialidad, integridad y disponibilidad de la información no se vean comprometidas.

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 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.

6.4 Desarrollo

ÍTEM	ACTIVIDAD	RESPONSABLES	REGISTROS
1	**Escritorio Limpio y seguro:** Retirar de los escritorios o lugares visibles la información que haya sido utilizada sin importar el medio en que se encuentre. No se pueden tener papeles, esferos en las operaciones, el personal jerárquico puede suministrarles donde tomar nota, estos papeles no deben salir de la operación y no es obligatorio que se brinden (en algunos casos cuando se requiera si no hay otra forma de pasar información para algún soporte o ayuda sobre dato relevante o cuenta).	Colaboradores Cos	N/A
2	No utilizar documentos con información confidencial para reciclaje.	Personal autorizado	Documentos impresos

3	Proteger la información siempre que abandone su escritorio, sin importar el tiempo de ausencia.	Colaboradores Cos	N/A
4	Restringir el uso de fotocopiadoras y otra tecnología de reproducción a personal o usuarios no autorizados.	Personal autorizado	N/A
5	Retirar inmediatamente de las impresoras los documentos que contengan información confidencial.	Personal autorizado	N/A
6	Velar que las salas de reuniones permanezcan cerradas y será exclusivo para reuniones de trabajo.	Seguridad física	N/A
7	Todo equipo (computadoras, aire acondicionado, ventiladores, y otros) que fuere utilizados en las salas de reuniones, deben permanecer apagados, así mismo se deben retirar los documentos utilizados para evitar exposición y/o pérdida de información.	Seguridad física Personal autorizado	N/A
8	Queda prohibido tener líquidos, sin tapa en sus puestos de trabajo (especialmente en operación), que pudieran dañar documentos originales y/o	Colaboradores Cos Seguridad	N/A

	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.	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	N/A
10	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	Equipos de computo

11	Queda prohibido decorar las pantallas de los equipos con stickers, sellos, papeles diferentes a las labores a realizar.	Colaboradores Cos	Equipos de computo
12	**Usuario desatendido:** Todos los usuarios deben terminar las sesiones activas cuando finalicen sus labores.	Colaboradores Cos	N/A
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	N/A
15	El sistema debe bloquear automáticamente el equipo luego de cinco minutos de usuario inactivo y solo será desbloqueado por medio del usuario y contraseña de red.	Colaboradores Cos	N/A
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.	Colaboradores Cos	N/A

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	N/A
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	N/A
	El no cumplimiento de la presente política se **sancionará de conformidad** con lo establecido en el Reglamento Interno de trabajo de la empresa.		

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 Contrato con el proveedor y/o contratista.

Todo proveedor y contratista en el desarrollo de sus funciones 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 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 del proveedor 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 se dé 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.

7.3 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.

7.4 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 y tenga que 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 por el director de IT, o personal, esta autorización se

debe realizar por correo electrónico o por la herramienta Help Desk, de acuerdo a las Políticas de traslado de equipos de COS.

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 las infraestructuras 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, aéreas 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 con la necesidad de labor a realizar de los proveedores o contratistas no se autorizan la toma de fotografías a las áreas tecnológicas de **COS S.A.S,** solo en Director de Tecnología puede autorizar el acceso a estas áreas de acuerdo con sus términos contractuales.

7.5 Uso de unidades Extraíbles

La utilización de soportes extraíbles de información deberá ser validada previamente por el Director 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, los soportes extraíbles facilitados al proveedor para el desarrollo de sus funciones deberán ser devueltos.

El uso y almacenamiento de información en soportes extraíbles y la manipulación de los soportes estará regulado mediante la normatividad establecida en **COS.**

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** 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.

7.6 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 implantación de protecciones adicionales.

COS podrá requerir que la información transmitida mediante mensajería electrónica esté adecuadamente protegida por parte del proveedor 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** solicitara controles de seguridad específicos y que podrían ser auditados.

7.7 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 y se mantienen en el tiempo correctamente

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.

7.8 Acceso a 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 de 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 o contratista a infraestructuras 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 las infraestructuras 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 validos previamente por **COS seas**.

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

7.9 Notificación e incidentes de seguridad de la información.

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 Director de Seguridad de la Información. Se emplearán además 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 a través del Director 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 la contractual y a las presentes políticas.

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.

Nota: el personal administrativo y cargos directivos en adelante cuentan con el permiso de ingresar el equipo **celular** para fines laborales, personal operativo 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.

8.2 Alcance

La presente política aplica para todo el personal interno o externo que cuente con la autorización de ingreso de dispositivo 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.

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 no está permitida dentro de las instalaciones que contengan algún tipo de información o contenido informático, solo se autorizara por medio del Director de Seguridad de la Información o Gerencia de Tecnología y bajo supervisión del área de Seguridad de la información o tecnología.
- 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.

8.4 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.

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 SOBRE EL USO DE CONTROLES CRIPTOGRÁFICOS

9.1 Introducción

COS velará porque la información de la empresa, clasificada como confidencial o restringida, será cifrada al momento de almacenarse y/o transmitirse por cualquier medio.

9.2 Objetivo

Proteger la confidencialidad, autenticidad o integridad de la información. Para esto deben utilizarse sistemas y técnicas criptográficas para la protección de la información que se considera en estado de riesgo y para la cual otros controles no suministran una adecuada protección.

La información criptográfica en el lugar de operación incluye toda la información en dispositivos y hardware en el lugar de operación, y también la información custodiada en espacios de archivo o copia de seguridad.

9.3 Normas dirigidas a la Gerencia de IT e Innovación

Almacenar y/o transmitir la información digital clasificada como confidencial o restringida bajo técnicas de cifrado con el propósito de proteger su confidencialidad e integridad.

Verificar que todo sistema de información o aplicativo que requiera realizar transmisión de información confidencial o restringida, cuente con mecanismos de cifrado de datos.

Desarrollar y establecer estándares para la aplicación de controles criptográficos.

9.4 Normas generales

- ✓ Cifrado de la información utilizando un algoritmo aprobado por el Gerente de Tecnología e Innovación
- ✓ Mediante el uso de hardware criptográfico validado por el Gerente de Tecnología e Innovación.
- ✓ Mediante un sistema de almacenamiento físico seguro.
- ✓ Cifrado de la información en la capa de transporte bajo protocolo TLS.

9.5 Se utilizarán controles criptográficos en los siguientes casos

Protección de claves de acceso a sistemas, datos y servicios, transmisión de información clasificada, fuera del ámbito de la compañía, resguardo de información, cuando así surja de la evaluación de riesgos realizada por el propietario de la información y el Director de Seguridad de la Información.

9.6 Algoritmos de cifrado y tamaños de clave

9.6.1 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.

Algoritmo	Longitud de Clave
AES256	2048
AES256	4096

9.6.2 Cifrado Asimétrico

Cada entidad 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.

Algoritmo	Longitud de Clave

RSA	≥ 2048 bits
DSA	≥ 2048 bits
RSA	≥ 2048 bits
SHA2	≥ 256 bits

9.7 Control de Cifrado

Mediante la evaluación de riesgos que llevará a cabo el propietario de la información y el Director de Seguridad de la Información, 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. Al implementar la Política del Organismo en materia criptográfica, se considerarán los controles aplicables a la exportación e importación de tecnología criptográfica.

9.8 Protección de claves criptográficas

Se implementará un sistema de administración de claves criptográficas para respaldar la utilización por parte del Organismo de los dos tipos de técnicas criptográficas, a saber:

- ✓ **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.

- ✓ **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.

9.9 Se utilizarán dentro del departamento de tecnología elementos de esteganografía:

- ➢ Esteganografía Pura
- ➢ Esteganografía de Clave Secreta
- ➢ Esteganografía en Texto
- ➢ Esteganografía en sistemas operativos y ficheros
- ➢ Esteganografía en Formato de ficheros
- ➢ Esteganografía en contenido multimedia

9.10 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	Periodo de retención	Medio de almacenamiento	Responsable
Bases de Datos	Tiempo contractual	Medios Magnéticos	DBA – Data Engineering
Grabaciones Telecomunicaciones	Tiempo contractual	Medios Magnéticos	Telecomunicaciones
Ficheros de Bases de Datos	N/A	Medios Magnéticos	Operación
Versionamiento de aplicaciones	Tiempo contractual	Medios Magnéticos	Desarrollo

9.11 Manejo y la administración de llaves de cifrado

La administración de las llaves criptográficas es un proceso esencial para el éxito de los controles criptográficos, el cual procura la prevención de modificaciones, pérdidas,

divulgación o destrucción de las llaves de cifrado. Es importante implantar controles de acceso físico adecuados a las máquinas que generan y almacenan las llaves criptográficas.

Las responsabilidades del Sistema de Administración de Llaves criptográficas se enumeran a continuación.

9.11.1 Generación de Llaves y Certificados Digitales.

Los certificados digitales y las llaves compartidas, públicas y privadas son generadas en máquinas ubicadas en zonas seguras con controles de acceso físico adecuados, utilizando software autorizado, por parte de personal autorizado y capacitado y siguiendo las especificaciones de seguridad del presente documento.

9.11.2 Validación de llaves públicas y firmas digitales.

Es de vital importancia que los analistas encargados de manipular las llaves en los procesos de comunicación cuenten con los conocimientos necesarios para verificar la autenticidad de certificados, firmas y llaves públicas, con el fin de preservar la confidencialidad de la información.

9.11.3 Distribución de llaves.

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

9.11.4 Almacenamiento de Llaves.

La custodia de las llaves criptográficas debe desarrollarse de acuerdo con los riesgos asociados a las mismas. Debe garantizarse un entorno seguro con protección a nivel físico y lógico.

9.11.5 Revocación de llaves.

Sustituir llaves criptográficas tras caducidad o compromiso de estas es una actividad prioritaria ante ambas eventualidades.

9.11.6 Destrucción de llaves.

La eliminación de llaves criptográficas a nivel electrónico y físico deben ser actividades que garanticen una destrucción segura de la información, impidiendo una posible recuperación futura de las mismas.

9.11.7 Control de Cambios de la administración de llaves y certificados digitales.

La gestión de las llaves y certificados digitales debe ser sometida a un estricto proceso de control de cambios, mismo que deberá ser auditado periódicamente para asegurar la correcta administración de este importante activo de información por parte del Director de Seguridad de la Información o el personal que él delegue.

10. POLÍTICA DE USO DE CORREO ELECTRÓNICO

10.1 Introducción

La siguiente Política está dirigida al personal de **COS S.A.S**, el cual implica los procedimientos y directrices para tener en cuenta para el uso de correo electrónico.

10.2 Objetivo

Controlar y restringir el uso de correo electrónico a los colaboradores de la compañía para evitar la fuga de información, este debe ser asignado al personal dependiendo de sus funciones. Se asignará una cuenta de correo electrónico (usuario y contraseña) 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.

10.3 Deberes de los colaboradores y 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.

10.4 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.

10.5 Control mediante 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 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.

10.6 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
Formador	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. POLÍTICA Y PROCEDIMIENTOS DE TRANSFERENCIA DE INFORMACIÓN

11.1 Objetivo

Definir los lineamientos, políticas, procedimientos de transferencia de información, mitigando el riesgo de fuga o pérdida de información restringida.

11.2 Alcance

La reglamentación dispuesta en esta guía aplica para todos los empleados de COS.

11.3 Responsables

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

11.4 Definiciones

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

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

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.

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

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.

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.

11.5 Desarrollo

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 COS establece procedimientos y controles de intercambio por medio de la utilización.

11.5.1 Acuerdos de transferencia de Información de COS.

- La información que circula en medios informáticos de COS. Durante su trasporte físico, debe estar protegida contra acceso no autorizado, uso inadecuado o corrupción. Se deben aplicar los siguientes controles.
- Se deben usar transportes o mensajeros fiables.
- Los medios informáticos o de transporte físico de información de la empresa deben estar lo suficientemente protegidos contra daño físico que pueda ocurrir durante su transporte. Todo objeto por trasladar debe ser embalado y protegido correctamente con cajas de cartón y protectores de icopor para el caso de 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.
- Los empleados de COS no deben revelar información sensible del proyecto por medios electrónicos sin cifrado (Llamadas, mensajería electrónica, Correo/WhatsApp/redes sociales), para evitar la escucha o interpretación de su comunicación por personas extrañas.
- Los empleados de COS no deben mantener conversaciones confidenciales en lugares públicos y oficinas abiertas.

- No se deben dejar mensajes en contestadores automáticos que puedan reproducirse por personas no autorizadas.
- Evite enviar información restringida a través de correo electrónico, pero en el caso de que sea estrictamente necesario cifre el correo usando los métodos autorizados.
- 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.
- La información restringida de COS no debe ser almacenada en dispositivos móviles. Sin embargo, en el caso de que no haya alternativa y el funcionario requiera almacenarla en un dispositivo móvil para su transporte, 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.

11.6 Responsabilidad legal y consecuencias.

Debido a que el uso inadecuado en la transferencia de información puede causar fuga de información restringida de COS o de sus clientes, los trabajadores de COS 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. POLÍTICA DE TRASLADO DE EQUIPOS COS

12.1 Objetivo

Establecer las políticas del área Tecnológica que regirán el traslado y acceso físico a los equipos de la empresa, asegurando su traslado, responsables, control y seguridad de estos.

12.2 Alcance

La presente política inicia con la necesidad de traslado o salida de algún equipo de la compañía para diferentes fines, estableciendo las actividades que deben seguir los responsables hasta dar cierre a la gestión.

12.3 Responsables

Coordinador (a) de soporte: Encargado de recibir y administrar las solicitudes del área de tecnología de acuerdo con la necesidad de las campañas.

Líderes de proceso: Encargado de entregar la siguiente información:

- ✓ Enviar la solicitud completa de acuerdo con la solicitud requerida.
- ✓ Deberá reportar cualquier daño y/o deterioro de los equipos informáticos oportunamente.

Analista IT: Verifica constantemente los casos generados en GLPI y correo electrónico para dar solución oportuna de los casos, dependiendo de su prioridad y evitar la caducidad de estos.

Administrador de Redes y Conectividad: Realizar la verificación del segmento para que no se pierdan los accesos por campaña, teniendo en cuenta la MAC.

Administrador de Redes y Seguridad: Garantizar el acceso del usuario bajo la navegación permitida antes del movimiento del equipo, teniendo en cuenta la IP y MAC.

Administrador Junior Antivirus: Validar la correcta navegación sobre los permisos brindados para el usuario.

12.4 Definiciones

a. **Acceso**: Autorización para el uso del activo.

b. **GLPI:** Herramienta de Gestión de casos para centralización de fallas y medición según niveles de servicios establecidos.

c. **Traslado:** Movimiento programado de cualquier activo de la compañía.

12.5 Desarrollo

No.	ACTIVIDAD	RESPONSABLES	REGISTROS
1	**Realizar verificación de la VLAN:** Realizar la verificación del segmento para que no se pierdan los accesos por campaña, teniendo en cuenta la MAC.	Administrador de Redes y Conectividad	Caso GLPI y/o correo electrónico
2	**Perfilamiento de usuarios:** Garantizar el acceso del usuario bajo la navegación permitida antes del movimiento del equipo, teniendo en cuenta la IP y MAC.	Administrador de Redes y Seguridad	Caso GLPI y/o correo electrónico
3	**Validación de navegación:**	Administrador Junior Antivirus	Caso GLPI y/o correo electrónico

	Validar la correcta navegación sobre los permisos brindados para el usuario.		
4	**Acceso físico a los equipos:** Solo personal autorizado puede abrir los equipos de computación y/o manipular sus componentes internos, en caso contrario será sancionado con las acciones disciplinarias a que haya lugar. Véase: **Guía de soporte**.	Analista IT Auxiliar de Almacén	Actas de entrega
5	**Traslado de equipos:** 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 jefe de Seguridad Física mediante correo electrónico la salida del activo.	Analista IT Dueño del activo	jhonn.suarez@groupcos.com.co autorización de traslado de equipos
6	**Compromisos:** El compromiso de los Analistas IT al momento de solicitar el traslado de	Analista IT Auxiliar de Almacén	jhonn.suarez@groupcos.com.co autorización de traslado de equipos

	un equipo informático fuera del site son: El personal autorizado deberá solicitar por medio de correo electrónico el traslado del equipo. El área de almacén realizará el formato de autorización de traslado de equipos, para el control en las diferentes sedes. En el correo deben estar las debidas observaciones del traslado la razón para realizar el cambio de lugar y la condición de los periféricos (mouse, teclado).		

13. POLÍTICA USO DE EQUIPOS TECNOLÓGICOS

13.1 Introducción

COS S.A.S., ha definido y establecido unas políticas para el uso correcto de los equipos tecnológicos (computador de escritorio, portátil o Laptop, Tablets, Celulares), asignados al personal de **COS S.A.S.** (COS), con el propósito de velar por el buen manejo de las herramientas de trabajo suministradas por la Compañía, para el desarrollo exclusivo de

las tareas asignadas dentro de los procedimientos del cargo y únicamente al interior de la empresa.

13.2 Políticas

- 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 del Gerente de implementación u dirección de seguridad de la información.
- Los colaboradores de COS. por ningún motivo deben ingresar equipos tecnológicos personales, a la operación y mucho menos ejecutar aplicaciones desde los mismos, de llegar ser necesarios se debe realizar la solicitud mediante correo electrónico al Gerente de implementación u dirección de seguridad de la información, solicitando la aprobación del uso dentro de la empresa y el motivo por el cual lo requiere.
- 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.
- Al Ingreso de algún equipo ajeno a la compañía debe registrarse en la recepción sin excepción y almacenarse en los gabinetes o LOCKERS asignados.

- Todos los equipos de la compañía deben contar con una solución de detección y prevención de códigos maliciosos, debe instalarse en alistamiento de equipos nuevos y verificarse en cada intervención, mantenimiento o soporte.
- Seguridad de la información tiene la potestad de solicitar revisión de los dispositivos para validación del uso de este y verificación de controles aplicados.

14. POLÍTICA DE AUTORIZACIÓN DE SISTEMAS Y APLICACIONES

14.1 Objetivo

Establecer los lineamientos y verificación de los aplicativos (Software) nuevo que se piensa poner en producción dentro de las instalaciones de la compañía para así mismo autorizar.

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.

14.2 Alcance

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

14.3 Directrices

14.3.1 Generales

El presente procedimiento se encuentra alineado con las políticas de seguridad de la información de **COS** y por lo tanto este se encuentra enfocado al cumplimiento de los requisitos establecidos.

14.3.2 Puntos para revisar:

- Listado de aplicaciones permitidas en Matriz de roles y privilegios
- Procedencia del software o sistema.
- Código de fuente en caso de que sea desarrollo tanto Interno como externo.
- Licencia del software en caso de ser requerido.
- Autorización previa.
- Solicitud por parte de los clientes.
- Vulnerabilidades conocidas (CVEs)
- Aseguramiento de parches al día y Antivirus, para la configuración de nuevas máquinas y antes de instalar el software nuevo.
- Instalación.

14.3.3 Actividades para ejecutar antes de autorizar

N	ACTIVIDAD	RESPONSABLE
1	Realizar verificación de la solicitud (correo o GLPI), necesidad, procedencia y protocolos de seguridad.	Analista Pentesting
2	Revisión del funcionamiento del aplicativo, validación del código en caso de ser desarrollo externo o interno, que permisos y que tanto alcance requiere en un sistema.	Analista Pentesting
3	Verificar si el producto requiere licencia para funcionamiento, con ello se solicita al creador de la solicitud que adjunte quien suministra la licencia del producto.	Analista Pentesting
4	Verificar si se cuenta con una reputación segura de la aplicación y si cuenta con certificados válidos.	Analista de Compliance
5	Hay que asegurar que las maquinas, siempre cuenten con antivirus, con parches al día y firma de virus actualizada.	Analista Pentesting
6	Autorizar el software y especificar cualquier tipo de condición para la instalación del software.	Analista Pentesting

15. POLÍTICA DE USO DE WHATSAPP WEB

15.1 Introducción

La siguiente política está dirigida al personal de **COS S.A.S.**, el cual implican las directrices a tener en cuenta para el uso de mensajería instantánea en este caso del usode WhatsApp Web.

15.2 Objetivo

Controlar el uso de WhatsApp Web en la compañía para así evitar las posibles fugas de informaciónde la compañía, así mismo resguardar y proteger todo tipo de información interna y externa a la que tiene acceso los colaboradores de **COS S.A.S.**

Con el fin de minimizar los posibles incidentes de seguridad relacionados con la utilización de este tipo de software deriva en la facilidad de filtrar información y la complejidad de establecer medidasde control sobre la información que sale a través de estas aplicaciones.

15.3 Responsables

Analista NOC: Monitoreo a los diferentes componentes de red.

Dirección de seguridad de la información: Controlar e implementar políticas de control para la seguridad de la información.

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.

15.4 Control

Este control lo que busca es minimizar los riegos a los que está expuesto la información confidencialde 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.

Para garantizar que se realice el respectivo bloqueo o permitir el acceso se realizar a través del Firewall Watchguard y control de tráfico web de Antivirus con reglas o políticas que permitirán el acceso o denegaran el mismo, estos accesos serán verificados por el Analista de NOC o revisiones periódicas por el director de seguridad de la información.

15.5 Autorizaciones

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 describede la siguiente manera:

Cargo	Autorización
Gerentes	Autorizado
Directores	Autorizado
Coordinadores	Autorizado
Lideres	Autorizado
Gestor de Negocios	Autorizado
Jefes	Autorizado
Analistas Senior	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
Formador	No Autorizado

NOTA: Si se requiere excepciones a lo establecido en esta política se debe solicitar la autorización por medio de **GLPI**, 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. POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN EN HOME OFFICE POR COVID-19

16.1 Objetivo

Establecer las directrices de control para el personal que desarrolle sus labores en modalidad de trabajo en casa, con el fin de mitigar y controlar posibles contagios dentro de las instalaciones como prioridad del cuidado del personal sin dejar a un lado en el aseguramiento de la continuidad de los procesos y seguridad de la información durante la contingencia por la situación sanitaria mundial relacionada con la pandemia por el coronavirus **COVID-19**.

16.2 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 que se establezcan o se puedan establecer durante el curso de la pandemia con fines de continuidad del negocio en **COS**.

16.3 Directrices

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**.
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.

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)

3. La Dirección 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.
4. 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. 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.

6. 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.

   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.

7. El acceso a los recursos de **COS** y los de la entidad aliada, únicamente debe realizarse mediante canales de comunicación seguros como VPN.
8. 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.
9. 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.
10. 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.

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.

11. 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.
12. La información sensible en los equipos a utilizar para el trabajo en casa debe ser cifrada, o enmascarada.
13. El equipo provisto para el desarrollo de trabajo en casa debe impedir la instalación de aplicaciones sin autorización.
14. El equipo provisto para el desarrollo de trabajo en casa sólo debe usarse para temas laborales.
15. 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.
16. 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 del Director de Seguridad de la Información.

17. El Director 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.
18. Se deben mantener las técnicas de monitoreo y control de calidad a todas las campañas según los objetivos de calidad y aseguramiento del servicio.
19. 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.
20. 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.
21. 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.
22. 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.

23. Los empleados deben evitar dejar expuesto el equipo en vehículos, zonas comunes o durante traslados.
24. Los empleados no deben permitir que el equipo sea utilizado por terceras personas o miembros de la familia.
25. Los empleados no deben utilizar servicios de computación en la nube para almacenar información confidencial, por ejemplo: wetransfer, onedrive, google drive, icloud, entre otros.
26. 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.
27. 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
28. Los empleados deben verificar que la información recibida por correo electrónico o relacionada con la descarga de aplicaciones que hacen referencia al **COVID-19**

provienen de fuentes oficiales y confiables para evitar la infección por software malicioso.

29. 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. POLÍTICA DE LA SEGURIDAD DE LA INFORMACIÓN DEL RECURSO HUMANO

17.1 Generalidades

La alta dirección en conjunto con el director de seguridad de la información se permite en comunicar y poner a disposición de sus colaboradores la política de seguridad en el recurso humano.

17.2 Objetivo

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

17.3 Lineamientos

17.3.1 Selección

Es deber del gerente de talento humano asegurar la contratación del personal idóneo para los cargos, roles y responsabilidades estipulados dentro del Sistema de Gestión de Seguridad de la Información.

Dando cumplimiento a lo anterior se deben realizar como mínimo las siguientes actividades: verificación de antecedentes judiciales:

- Velicación de antecedentes disciplinarios de la Procuraduría
- Velicación de las referencias laborales y personales
- A los cargos críticos se les debe realizar visita domiciliaria.
- El 100% del personal de la compañía debe firmar un acuerdo de confidencialidad y la autorización para la verificación del historial crediticio en centrales de riesgo.

17.3.2 Toma de conciencia, educación y formación en la seguridad de la información

Es deber del director de seguridad de la información diseñar las capacitaciones relativas a la seguridad de la información y ambiente de control, para que el área de formación y capacitación aseguren su divulgación y sensibilización al ingreso y durante el desarrollo de la relación contractual de los colaboradores y contratistas, con el objetivo de asegurar la toma de conciencia de las responsabilidades de seguridad de la información. Cumplir

lo establecido dentro del marco legal, contractual y normativo vigente y aplicable. Conocimiento de la Política de Seguridad de la Información.

17.3.3 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.

COS S.A.S 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 de tratamiento de eventos e incidentes de seguridad de la información**, el contrato laboral y su cláusula de confidencialidad de la información, las cuales se encuentran publicadas en lugares físicos y/o virtuales con acceso permitido al 100% del personal contratado.

17.3.4 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

17.3.5 Acuerdo de confidencialidad

El 100% del personal debe firmar y cumplir los acuerdos de confidencialidad adquiridos con COS S.A.S durante y después de la relación laboral.

17.3.6 Segregación de funciones

COS SAS 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 COS SAS

Por lo anterior, la alta dirección de COS SAS delega la validación de este principio al director 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. POLÍTICA DE ENTREGA BORRADO Y DESTRUCCIÓN DE MEDIOS

18.1 Objetivo

Garantizar el cumplimiento del retiro, la destrucción y eliminación de los medios de almacenamiento de información tanto a nivel físico como a nivel lógico por parte de los propietarios y de los responsables de la gestión de los activos de información de la compañía durante todo su ciclo de vida.

18.2 Alcance

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

18.3 Responsables

- Gerente de I.T. e Innovación: garantizar el cumplimiento del presente documento, aplicando aquellos métodos definidos para el retiro, borrado y destrucción de medios.
- Gerentes de operaciones: propietarios de los activos de información de las campañas.
- Gerentes de área: propietarios de los activos de información de COS.
- Coordinadores de operaciones y jefes de operaciones: responsables de la gestión de los activos de información de las campañas durante todo su ciclo de vida.

- Coordinadores de área y jefes de área: responsables de la gestión de los activos de información de COS durante todo su ciclo de vida.
- Seguridad de la información: área encargada de verificar y firmar el acta de borrado y destrucción de medios enviada por el área o campaña de COS responsable de la gestión de los activos de información.

18.4 Directrices

- La Gerencia de I.T. e Innovación será responsable de dar cumplimiento al presente documento, aplicando aquellos métodos definidos para el retiro, borrado y destrucción de medios, según el procedimiento de entrega, borrado y destrucción de medios.
- Para el borrado seguro de la información histórica de los clientes, se debe tener en cuenta los niveles y tiempos de retención definidos en el contrato.
- El borrado seguro de la información de los clientes se debe realizar a través de herramientas de borrado seguro y de bajo nivel que no permita su recuperación.
- Los medios físicos deben ser destruidos por medio de la trituradora de papel y se debe hacer la disposición adecuada de acuerdo con los lineamientos del sistema de gestión ambiental.

18.5 Anexos

- Formato de solicitud borrado y destrucción de medios.
- Acta entrega, borrado y destrucción de medios.
- Procedimiento de entrega, borrador y destrucción de medios.

19. 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	17/02/22	Gerente Control Interno	17/02/22
08	Revisión y actualización de las siguientes políticas: - Política de asignación, modificación y retiro de usuarios - Política de continuidad del negocio	Analista Compliance	18/01/2023	18/01/2023	Gerente Control Interno	18/01/2023

	- 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.					