MANUAL DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

TI-M-003
Versión 4

1. OBJETIVO

Describir el sistema de gestión de seguridad de la información y ciberseguridad del Oleoducto de los Llanos Orientales y el Oleoducto Bicentenario de Colombia (en adelante “las compañías”)

Objetivos específicos

- Proteger los recursos de información de las compañías y la tecnología utilizada para su procesamiento, frente a amenazas, internas o externas, deliberadas o accidentales, con el fin de asegurar la confidencialidad, integridad, disponibilidad, legalidad y confiabilidad de la información.
- Garantizar que el modelo de seguridad de la información y ciberseguridad, se encuentren alineadas a la estrategia de la organización.
- Establecer la estructura de gobierno, los roles, responsabilidades y otros aspectos claves que deben ser tenidos en cuenta por cada persona que interactúa con la información de las Compañías
- Garantizar la implementación de las medidas de seguridad requeridas para asegurar la información de las compañías.
- Mejorar las capacidades internas para la atención de incidentes de seguridad de la información.
- Mejorar la capacidad organizacional para mantener la continuidad en la prestación del servicio.
- Fortalecer la cultura en seguridad de la información y ciberseguridad para los empleados de las compañías, contratistas y terceros, a través charlas, capacitaciones y comunicados
- Potenciar el desarrollo de capacidades de preparación, detección, identificación, escalación contención, análisis, erradicación, recuperación, reporte y lecciones aprendidas incidentes de para la atención de incidentes de seguridad de la información y ciberseguridad.

2. ALCANCE

Este documento es de cumplimiento de todos los colaboradores directos, contratistas y trabajadores en misión de las compañías

3. GLOSARIO

El siguiente es el compendio de términos definiciones y conceptos que son aplicables en los contextos citados a lo largo de todo el documento (adicional a los contenidos en la norma ISO-27001-2013):

Seguridad de la Información: La seguridad de la información se entiende como la preservación de las siguientes características:

- **Autenticidad**: busca asegurar la validez de la información en tiempo, forma y distribución. Asimismo, se garantiza el origen de la información, validando el emisor para evitar suplantación de identidades.

- **Confidencialidad**: se asegura que la información sea accesible sólo a aquellas personas autorizadas a tener acceso a la misma.

- **Confiabilidad de la Información**: que la información generada sea adecuada para sustentar la toma de decisiones y la ejecución de las misiones y funciones.

- **Disponibilidad**: se asegura que los usuarios autorizados tengan acceso a la información y a los recursos relacionados con la misma, toda vez que lo requieran.

- **Integridad**: se salvaguarda la exactitud y totalidad de la información y los métodos de procesamiento.

- **Legalidad**: referido al cumplimiento de las leyes, normas, reglamentaciones o disposiciones a las que está sujeto de las compañías.

- **No repudio**: se refiere a evitar que una entidad que haya enviado o recibido información alegue ante terceros que no la envió o recibió.

- **Trazabilidad**: define que todos los eventos de un sistema deben poder ser registrados para su control posterior.

- **SGSI:** ISO 27001SGSI son las siglas del Sistema de Gestión de Seguridad de la Información al que da lugar la norma ISO 27001. Se entiende por información el conjunto de datos organizados en poder de una entidad que posean valor para la misma, independientemente de la forma en que esté guardada o sea transmitida, de su origen o de la fecha de elaboración.

- **Cuenta de usuario:** En el contexto de la informática, un usuario es aquel que utiliza un sistema informático. Para que los usuarios puedan obtener seguridad, acceso al sistema, administración de recursos, etc., dichos usuarios deberán identificarse con una cuenta de usuario y contraseña.

- **Contraseña:** una serie secreta de caracteres que permite a un usuario tener acceso a un archivo, a un ordenador, o a un programa. En sistemas multiusos, cada usuario debe

incorporar su contraseña antes de que el ordenador responda a los comandos.

- **Ciberseguridad:** ISACA (2016) la define como la protección de los activos de información a través del tratamiento de las diversas amenazas que ponen en riesgo la información que es procesada, almacenada y transportada por los sistemas de información que se encuentran interconectados

- **Ciberespacio:** Es el entorno complejo, resultante de la interacción entre las personas, el software y los servicios en Internet por medio de dispositivos tecnológicos conectados a redes, las cuales no existen en ningún tipo de forma física

- **Ciberincidente:** Evento que se produce en el Ciberespacio que genera una violación o amenaza con efectos adversos reales de seguridad sobre los procesos, servicios, activos físicos o de información de negocio y de la organización, que pueden comprometer su disponibilidad, integridad o confidencialidad.

- **Ciberevento:** Evento que se producen en el ciberespacio que no representa una potencial amenaza por lo que no es considerado un ciberincidente.

- **Directorio Activo (DA):** es un servicio establecido en uno o varios servidores en donde se crean objetos tales como usuarios, equipos o grupos, con el objetivo de administrar los inicios de sesión en los equipos conectados a la red, así como también la administración de políticas en toda la red.

- **Mesa de Ayuda (Helpdesk):** Es el punto de contacto entre los usuarios y el área de TIC, a través de la cual se identifica, registra, clasifica, prioriza, analiza, resuelve, escala y realiza el cierre de las solicitudes de servicio.

4. CONDICIONES GENERALES

Este manual describe los elementos necesarios para gestionar adecuadamente la seguridad de la información al interior de las compañías.

Con el fin de brindar un modelo para el establecimiento, implementación, operación, seguimiento, revisión, mantenimiento y mejora de un sistema de gestión de seguridad de la información (SGSI), se hace necesaria la inclusión de un gobierno de seguridad que esté alineado con los objetivos del negocio para realizar una protección efectiva sobre toda la información en especial los activos críticos.

Para unificar criterios y lineamientos en cuanto a la seguridad de la información y ciberseguridad, se tienen de referencia estándares como ISO27001 el cual contempla diversos aspectos que se deben tener en cuenta al implementar un modelo de seguridad o Sistema de Gestión de Seguridad de la Información (SGSI) y para la gestión de ciberseguridad, se toma el marco general de referencia del National Institute of Standards and Technology (NIST). Estos estándares incluyen no solamente los elementos tecnológicos para la protección de la información, si no que consideran también aspectos como las políticas y procedimientos que se deben establecer y cumplir para un esquema de seguridad integral que envuelva toda la organización.

DESCRIPCIÓN DEL SGSI

A continuación, se ilustra el ciclo del Sistema de Gestión de Seguridad de la información de las compañías:

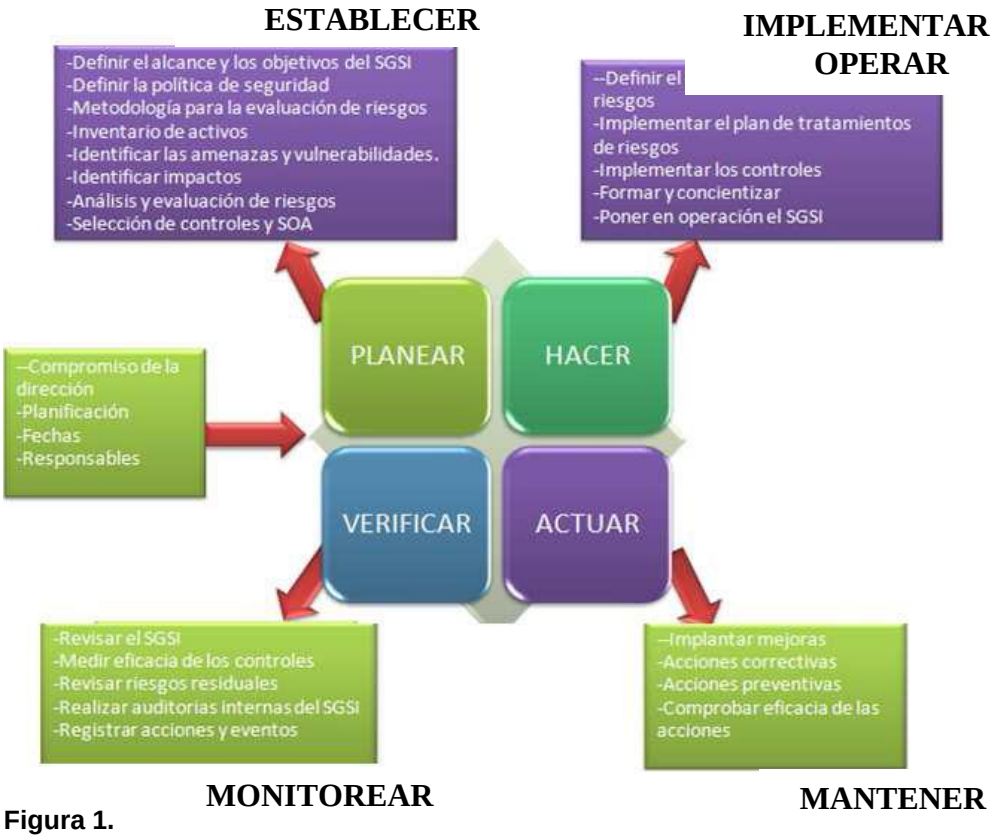

Figura 1.

Para establecer y gestionar un Sistema de Gestión de la Seguridad de la Información se utiliza el ciclo continuo PHVA, tradicional en los sistemas de gestión de la calidad.

PLANEAR: Establecer el SGSI

HACER: Implementar y operar el SGSI

VERIFICAR: Monitorear y revisar el SGSI

ACTUAR: Mantener y mejorar el SGSI

RESPONSABLES DEL SGSI[1]

La Seguridad de la Información es de aplicación obligatoria para todo el personal, cualquiera sea su tipo de vinculación, el área o el nivel de las tareas que desempeñe.

Las áreas y procesos de ODL, independiente de su nivel jerárquico, son responsables del cumplimiento de la Seguridad de la Información dentro de sus áreas de responsabilidad, así como del cumplimiento de las Políticas de Seguridad de la Información por parte de sus equipos de trabajo.

JUNTA DIRECTIVA - COMITÉ DE AUDITORÍA

Supervisar la adecuada gestión de riesgos de seguridad de la información y ciberseguridad por parte de la gerencia.

PRESIDENTE

- Aprobar las políticas y procedimientos de seguridad de la información y ciberseguridad.
- Verificar que la cultura de las Compañías y la política para la gestión del riesgo cibernético están alineadas.
- Designar un presupuesto y recursos necesarios para el cumplimiento de la política.

GERENTE TIC/TOC

- Revisar y proponer las políticas y las funciones generales en materia de seguridad de la información.
- Aprobar las principales iniciativas para incrementar la seguridad de la información, de acuerdo con las competencias y responsabilidades asignadas a cada área.
- Acordar y aprobar metodologías y procesos específicos relativos a la seguridad de la información.
- Garantizar que la seguridad sea parte del proceso de planificación de la información.
- Revisar y monitorear el cumplimiento de las políticas, directrices y procedimientos de seguridad de la información y ciberseguridad definidos por las Compañías por parte de sus colaboradores.

LÍDERES O DUEÑOS DE PROCESO

- Identificar los activos de información de su proceso y clasificarlos de acuerdo con su nivel de criticidad, tomando como base la TI-G-003 GUÍA DE CLASIFICACIÓN Y VALORACION ACTIVOS DE INFORMACIÓN definido en las compañías.

[1] A.6 Organización de la seguridad de la información. Anexo A, ISO -IEC 27001

- Identificar los riesgos de seguridad de la información en cada uno de los procesos a cargo.
- Evaluar los riesgos y proponer las medidas de tratamiento a los riesgos que requieren gestión según los resultados de la evaluación.
- Garantizar que los controles o las medidas implementadas para reducir los riesgos sean efectivas
- Proponer los mecanismos de monitoreo sobre los riesgos y controles de su proceso.
- Revisar y monitorear oportunamente el desarrollo de los planes de tratamiento, buscando que las actividades propuestas sean realizadas dentro de los tiempos propuestos y evaluar la efectividad de las mismas en relación con el riesgo que se desea reducir.
- Reportar a la mesa de ayuda los incidentes de seguridad que le sean informados por las personas de su proceso.
- Asegurar el conocimiento y cumplimiento de las políticas, procedimientos y directrices de seguridad de la información y ciberseguridad, por parte de los colaboradores a cargo.
- Asegurar el conocimiento y cumplimiento de las políticas, procedimientos y directrices de seguridad de la información y ciberseguridad, por parte de terceros contratados que cuentan con acceso a la información o a la infraestructura tecnológica de las Compañías, para lo cual debe:
    - Asegurar que en los documentos contractuales se incluyan la obligatoriedad de cumplir con las políticas, directrices y requerimientos de seguridad de la información establecidas por las Compañías.
    - Asegurar que los terceros son informados y entrenados en los aspectos de seguridad relevantes de acuerdo con la labor que van a cumplir y el nivel de acceso que tendrán a la información de las Compañías.
    - Asegurar la identidad de las personas a quienes les será dado acceso a las instalaciones y la información de las Compañías.
    - Documentar y aprobar los privilegios de acceso que se asignarán a los usuarios.
    - Retirar los privilegios de acceso asignados a los terceros, de manera inmediata cuando ya no los requieran para cumplir con sus funciones.

PROFESIONAL DE SEGURIDAD DE LA INFORMACIÓN[2]

- Apoyar y promover en los procesos de negocio la formación de la cultura de gestión de riesgos de seguridad de la información.

- Ejecutar periódicamente actividades que permitan la identificación, evaluación, mitigación, seguimiento y control de los riesgos en todos los ámbitos que involucren tecnologías de información y comunicaciones, acompañando a los procesos en la definición y ejecución de los planes de tratamiento de los riesgos con mayor grado de vulnerabilidad o criticidad.

- Velar por el cumplimiento de los requisitos de gestión de riesgos de seguridad de la información y el desarrollo de las actividades de monitoreo, para garantizar que la seguridad esté diseñada de manera apropiada y acorde a las necesidades del negocio.

- Planear y diseñar con los procesos involucrados las actividades correctivas de los hallazgos o no conformidades pertinentes a la gestión de riesgos de seguridad de la información encontrados en los ejercicios de auditorías realizados sobre el SGSI.

- Gestionar los planes de seguridad de la información y ciberseguridad.

- Liderar el proceso de recuperación de los sistemas de información frente a interrupciones imprevistas en conjunto con los dueños de los servicios.

- Definir los planes de capacitación y concientización en seguridad de la información y ciberseguridad para el personal interno o externo.

- Gestionar los incidentes reportados, hacer seguimiento y reportar a la Gerencia TIC/TOC, de acuerdo con lo establecido en el procedimiento de gestión de incidentes.

- Proponer estándares de seguridad para los diferentes componentes de la infraestructura tecnológica.

COLABORADORES, CONTRATISTAS, TERCEROS Y USUARIOS

Todos los colaboradores, contratistas y terceros con acceso a la información de las Compañías son responsables de:

- Cumplir con las políticas y directrices establecidas por las Compañías en materia de seguridad de la información y Ciberseguridad.

[2] A.6.1.1 Roles y responsabilidades. Anexo A, ISO-IEC 27001

- Demostrar debida diligencia ante la ocurrencia de un incidente de seguridad que sea de su conocimiento, donde se pueda estar involucrado él o cualquier colaborador o tercero.

- Participar en las capacitaciones y programas de concientización desarrollados por las Compañías.

- Identificar y reportar a los Líderes de Proceso, a su superior o supervisor, al Profesional de Seguridad de la Información, todos los eventos de riesgo que surjan en el desarrollo de sus actividades.

- En el caso de colaboradores de las Compañías, proponer alternativas de mejora tendientes a reducir los niveles de exposición de ODL al riesgo.

- Usar la información únicamente para el desarrollo de su trabajo.

Mesa de Ayuda

- Recibir los reportes de incidentes por parte de los usuarios y resolverlos o escalarlos de manera oportuna. Así mismo registrar en el sistema de mesa de ayuda los incidentes de seguridad. En caso de que los eventos afecten la seguridad de la información reportar al administrador de recursos informáticos y/o al responsable de seguridad de la información

NECESIDADES GRUPOS DE INTERES

El Sistema de Gestión de Seguridad de la Información, es difundido a todos los funcionarios, potenciales proveedores, contratistas y terceros que posean vínculo con ODL, y su cumplimento es una obligación de todos los funcionarios de la organización independientemente de sus cargos, jerarquías, niveles de responsabilidad, o tipos de vinculación con la empresa.

El Sistema de Gestión de Seguridad de la Información cubre, pero no se limita a:

- Junta Directiva
- Presidencia
- Los diferentes Comités de la empresa
- Funcionarios y personal vinculado directa o indirectamente con la empresa
- Contratistas
- Terceros, proveedores
- Cualquier persona natural o jurídica que por la naturaleza de las relaciones con ODL tenga acceso, modifique o almacene información de la organización.

5. PLANIFICACIÓN DEL SGSI

Dentro de la planificación de actividades de gestión del SGSI, ODL realiza las siguientes actividades:

Clasificación y Valoración de activos de información[3]

El documento TI-G-003 GUIA DE CLASIFICACION DE ACTIVOS DE INFORMACION contiene los lineamientos para realizar la identificación los activos de información en función de valor, criticidad y susceptibilidad. Los inventarios son documentados y actualizados, tomando como base la versión actual de las TRD (Tablas de Retención) y el documento TI-F-033 Formato CMDB. El inventario de activos de información cumple las siguientes especificaciones:

- Identificación, descripción y registro del Activo de Información del proceso
- Valoración e importancia de los Activos de Información
- Definición del nivel de clasificación y Confidencialidad de la información.
- Revisión y aprobación Matriz de Clasificación y Valoración Activos de Información
- Actualización Matriz de Clasificación activos de información.

Identificación y Valoración de Riesgos

La identificación de riesgos de seguridad de la información en las compañías se desarrolla a partir de los activos de información identificados y valorados con criticidad alta; y las amenazas o peligros que afecten la información de los procesos, para posteriormente definir controles que permitan la mitigación de los riesgos identificados.

La valoración del riesgo es el proceso global de análisis y evaluación del riesgo, esta valoración describe cuantitativa o cualitativamente el riesgo y habilita a los encargados del Sistema de Gestión de Seguridad de la Información a priorizar los riesgos de acuerdo con los criterios establecidos.

Selección de controles

En las compañías ODL y Bicentenario se seleccionan los controles apropiados a fin de mitigar los riesgos a los que se encuentra expuesto los activos de información.
Esta selección se realiza de acuerdo con el análisis de riesgo, se establece un plan de trabajo para la implementación de los controles seleccionados.
Independientemente del tipo de control que se implante ya sea manual o automático se documentan los procedimientos de estos, estableciendo su instalación, uso y mantenimiento.

[3] [3] A.8.2. Clasificación de la información. Anexo A, ISO-IEC 27001

6. SOPORTE DEL SGSI

El Sistema de Gestión de Seguridad de la Información y ciberseguridad esta complementado y soportado por infraestructura tecnológica física y lógica como Firewalls, Antispam, antivirus, sistema de detección de intrusos (SDI), el SOC y otros dispositivos de seguridad perimetral que permiten minimizar la probabilidad de ingresos no autorizados a la información de las compañías. Para el acceso a los sistemas de información desde redes externas (fuera de la red corporativa); se realizará por medio de la VPN (Virtual Private Networks), y para acceder a los servicios cloud de Office 365 (entre ellas correo, SharePoint, Onedrive, Teams) deberá contar con la activación del factor de doble autenticación.

7. OPERACIÓN DEL SGSI

El Sistema de Gestión de Seguridad de la Información de las compañías se administran con base a una serie de lineamientos incluidos en este documento los cuales son claves para el aseguramiento de la información de las compañías en cuanto a: Confidencialidad, Integridad y Disponibilidad.
Adicionalmente el Profesional de Seguridad de la Información gestiona el SGSI revisando los demás procedimientos que se ejecutan con el fin de asegurar la protección de la información. Para lo anterior, realiza periódicamente una verificación de la utilización de los mismos y de ser necesario actualiza los procedimientos existentes o genera los nuevos.
Anualmente se programan pruebas de vulnerabilidad, Hardening, Ethical Hacking e Ingeniería Social, sobre la infraestructura de TIC/TOC, en donde se identifican posibles riesgos de accesos no autorizados y se definen planes de acción para su mitigación.
También anualmente se desarrollan campañas de socialización y/o capacitaciones en temas de Seguridad de la Información para los grupos de interés.

8. REVISIÓN DEL SGSI

Indicadores

Las compañías como parte de su proceso de mejora continua, monitorea mensualmente los indicadores de capacidad, disponibilidad de servicios y de gestión de incidentes (incluidos los de seguridad y ciberseguridad); lo cual permite verificar el correcto funcionamiento de infraestructura TIC y fortalecer la eficacia de los controles de TIC.

El Profesional de seguridad de la información ejecuta controles periódicos entorno a los sistemas de información críticos, aplicaciones SOX y no SOX, gestión de procesos de Cambios, configuración, incidentes y del conocimiento; que permiten prever o identificar oportunamente posibles desviaciones en el funcionamiento de los servicios prestados por la Gerencia TIC. De igual forma se gestiona el cierre oportuno de los hallazgos por auditorías internas o externas.

9. MEJORAMIENTO DEL SGSI

En esta fase se diseña y ejecuta el plan de remediación para corregir hallazgos, observaciones, oportunidades de mejora, identificadas a partir de revisiones periódicas, análisis de vulnerabilidades, auditorías internas o externas y en la operación normal del SGSI.

Así mismo, para las compañías se diseña y ejecuta el plan de mejora enfocado en resolver las no conformidades, identificadas a partir de encuestas de satisfacción, prestación y operación de los servicios TI.

10. LINEAMIENTOS ESPECÍFICOS

10.1. ACCESO A LA INFORMACIÓN [4]

10.1.1. ALCANCE

El lineamiento aplicará a todo el personal vinculado directamente en la compañías, contratistas y terceros que tengan acceso a los recursos de información de la organización.

10.1.1.1. Condiciones Obligatorias

- Todos los funcionarios, contratistas y terceros que prestan sus servicios a las compañías deben aplicar todos los controles de seguridad definidos por **las compañías** para garantizar la preservación de la Confidencialidad, Integridad y Disponibilidad de la información que está a su cargo y a la que tengan acceso por la naturaleza misma de sus actividades o que por otras situaciones esté bajo su custodia.

- Toda persona, proceso o sistema de información que realice actividades para **las compañías** debe tener acceso únicamente a la información necesaria para el desempeño de las actividades que le han sido autorizadas.

- Todo acceso a la información debe ser autorizado formalmente por el área responsable de la información. Para la autorización de acceso a la información se debe contemplar un análisis previo de la justificación de la necesidad de uso de la misma y las actividades a realizar con el acceso a la información.

- Todo acceso a la información debe considerar el nivel de clasificación definido por **las compañías** o por el responsable de la información.

- Todo acceso a la información debe cumplir con los requisitos legales, normativos, reglamentarios, procedimentales o de cualquier otra índole que haya definido el responsable de la información.

La conexión remota a la infraestructura tecnológica de las compañías debe ser establecida a través de la conexión VPN segura corporativa, la cual debe ser autorizada previamente por la Gerencia TIC y el dueño del servicio. Para la atención a solicitudes que requiera conexión remota en los equipos de usuario final, de igual forma se realiza conexión a la VPN y se activara la herramienta de gestión autorizada por la Gerencia TIC.

- El acceso a la información de **las compañías** debe estar sujeto a controles que garanticen la trazabilidad de las acciones realizadas sobre la misma, considerando la identificación de

[4] [4] A.9.1 Política de control de acceso. Anexo A, ISO-IEC 27001

la persona, proceso o sistema que realiza el acceso, acciones realizadas, instante de tiempo en que se realizan las acciones.

- En el momento que un usuario se encuentre temporalmente ausente por causas como incapacidad, licencia de maternidad, vacaciones, etc., debe ser bloqueado de los sistemas de información y será desbloqueado únicamente con aprobación de la Gerencia de la que pertenece o administrador del contrato.

- Las compañías deberán realizar un inventario y proceso de clasificación de la información con relación a la información y en especial con el fin de garantizar el acceso a la información.

- Cuando se tiene acceso a la información de **las compañías** se está obligado a la aceptación formal de la reglamentación de acceso y tratamiento de la información que definan las leyes de Colombia, Acuerdos internacionales suscritos por Colombia, normas del sector, políticas, estándares o cualquier tipo de control establecido para el tratamiento de la información.

10.1.1.2. Usos no autorizados

Los siguientes usos se consideran usos no autorizados de la información:

- Modificación de la información sin contar con la autorización formal.
- Divulgación no autorizada de información.
- Impedir el acceso a la información sin justificación real.
- Modificación o Eliminación de los controles de seguridad que protejan la información.
- Cualquier acción sobre la información considerada como ilegal o no autorizada por las leyes, regulaciones, normas o políticas a los que está sometida **las compañías**.

10.2. ASIGNACIÓN DE CLAVES [5]

10.2.1. ALCANCE

El lineamiento aplica a empleados directos, contratistas y terceros que prestan sus servicios a las compañías y que tengan acceso a los recursos de información de ODL.

10.2.2. OBJETIVO

Implementar la seguridad en los accesos de usuarios por medio de técnicas de autenticación y autorización, usando claves fuertes.

10.2.2.1. Condiciones Obligatorias

La creación y entrega de cuenta de usuario y contraseñas se realiza de forma controlada mediante, el correo electrónico informando el usuario y contraseña genéroca; dejando marcada la opción: “El usuario debe cambiar la contraseña en el siguiente inicio de sesión, cumpliendo con los parámetros de asignación de contraseña definidos por el sistema de gestión de seguridad de la información. El

[5] [5] A.9.2. Gestión de acceso de usuarios. Anexo A, ISO-IEC 27001

área de tecnología es la única autorizada para la asignación de contraseñas para acceso a servicios, sistemas de información o equipos informáticos.

Los responsables de procesos son los únicos autorizados para aprobar ante la solicitud de asignación de cuenta de usuario y contraseña para los empleados, contratistas y terceros que presten sus servicios a **las compañías**. Los responsables de procesos serán: Gerentes ó Jefes de área. .

Cualquier servicio, sistema de información o equipo informático que tenga contraseñas por defecto configuradas por el proveedor o fabricante deben ser cambiadas por nuevas contraseñas cuando se realice el proceso de configuración del servicio, sistema o equipo. Al momento de poner en producción el servicio, sistema o equipo se debe volver a cambiar la contraseña por una nueva.

La contraseña asignada a un usuario es personal e intransferible. Los usuarios no deben divulgar, prestar, exhibir, comunicar en forma escrita o verbal su contraseña. Cuando por labores de soporte o mantenimiento se requiere la contraseña de usuario, el usuario es quién debe digitarla y al final de las actividades de soporte debe cambiar por una contraseña nueva.

Los usuarios administradores de servicios, sistemas de información, equipos informáticos deben cambiar sus contraseñas una (1) vez al año.

Los administradores de servicios, sistemas de información, equipos informáticos deben utilizar contraseñas diferentes para sus cuentas de usuario y para sus cuentas como administradores.

Los usuarios finales de equipos de cómputo no pueden tener el privilegio de administradores, excepto los autorizados por la Gerencia de TIC/TOC.

Los usuarios finales no deben hacer descargas o instalaciones de software no autorizado. Se debe se realizará la solicitud a la MDA para la respectiva gestión (escaneos, aprobación e instalación).

Los funcionarios son responsables de todas las acciones que se realicen con sus usuarios. En caso de que la contraseña haya sido conocida por externos, el usuario debe informar inmediatamente al responsable del proceso o del área y al área de tecnología para bloquear cualquier acceso a servicio, sistema de información o equipo informático que utilizará la contraseña comprometida.

Adicionalmente las claves o contraseñas deben cumplir con los siguientes parámetros:

- Cada 60 días se realiza el cambio de contraseñas de acceso a servicios, sistemas de información y estaciones de trabajo.
- No utilice contraseñas que sean fáciles de deducir.
- No utilice contraseñas que haya usado en los últimos meses.
- Evite las palabras obvias. Ejemplos: Nombre, fecha de cumpleaños, nombre de la mascota, nombre de los hijos, entre otras.
- Su contraseña debe contener mínimo 12 caracteres incluyendo alfanuméricos y especiales.
- Procure usar caracteres diferentes, que no sean consecutivos o idénticos.
- Use contraseñas diferentes del usuario.
- Siempre procure memorizarla.

- Específicamente para cuentas SAP se tendrá en cuenta lo siguiente:

  - ✓ Después de **20 días** de inactividad **se bloqueará la contraseña.**
  - ✓ Después de **4**5 días de inactividad **se inactivará el usuario por no uso**.
  - ✓ Después de **10 minutos** de tiempo de **inactividad SAP se cerrará la sesión.**
  - ✓ Su contraseña debe ser de mínimo **ocho (8) caracteres y** debe contener **una letra mayúscula**, una **letra minúscula**, un número y un carácter especial.
  - ✓ Cada **30 días** el sistema debe solicitar al usuario cambio **de contraseña**.
  - ✓ Al tercer intento fallido se bloqueará el usuario.

Esta expresamente prohibido divulgar por cualquier medio las contraseñas.

El uso de software para visualizar, descifrar o interceptar contraseñas de servicios, sistemas de información o equipos informáticos de **las compañías** está prohibido.

Cada usuario debe tener en cuenta las buenas prácticas de seguridad de selección y uso de sus contraseñas que defina el sistema de gestión de seguridad de la información de **las compañías**.

Los administradores de servicios, sistemas de información y equipos informáticos deben:

Cuando se detecte que una contraseña ha sido comprometida, debe seguir el i TI-I-001 - Instructivo de gestión de incidentes de seguridad de la informacion, mitigar el impacto del incidente cambiando las contraseñas de los sistemas identificados como comprometidos y evaluar la extensión del incidente para determinar el cambio de contraseñas en otros sistemas no comprometidos.

10.3. RESPALDO DE INFORMACIÓN 6

10.3.1. ALCANCE

Esta política aplica a todos los sistemas de información y dispositivos de almacenamiento electrónico de información de las compañías.

10.3.2. OBJETIVO

Definir las pautas generales para garantizar en las compañías; la ejecución, preservación, mantenimiento y verificación de copias de respaldo de la información.
El respaldo de la información busca reducir los impactos de los riesgos generados por la pérdida de información y es un mecanismo para soportar los planes de contingencia, recuperación ante desastres y atención a incidentes de seguridad de la información adoptados por las compañías.

10.3.2.1. Condiciones Obligatorias

La información de los diferentes procesos, políticas y actividades que forman parte de las funciones de **las compañías,** se respalda de acuerdo con requisitos legales, períodos de retención documental y requerimientos de uso establecidos en el **TI-M-004** Manual de gestión de información y administración de archivos de **las compañías**.

[6] A.12.3.1 Respaldo de información. Anexo A, ISO-IEC 27001

Toda informacion alojada en la infraestructura TIC debe tener una definición formalmente documentada de las necesidades de respaldo de información la cual debe incluir: identificación de la información a respaldar, periodicidad de ejecución de la copia de respaldo y período de retención de las copias de respaldo de acuerdo con la **TI-G-002** GUIA EJECUCIÓN DE BACKUP Y RESTAURACIÓN DE LA INFORMACION

Las copias de respaldo de la información deben ser preservadas por el tiempo definido en el formato de policitas de Backup.y aprobadas por los responsables del aplicativo (líder funcional los líderes funcionales y/o dueños de los procesos) a los que pertenece la información. El Sistema de Gestión de Seguridad de la Información de **las compañías** debe asistir a los líderes funcionales y/o dueños de los procesos en la definición de los períodos de retención de las copias de respaldo.

Los responsables de la gerencia TIC/TOC deben coordinar la preservación de las copias de respaldo, resguardando su acceso de acuerdo con su nivel de clasificación y la disposición final definida en las tablas de lineamientos de respaldo de información

Para llevar a cabo el respaldo de la información en computadores asignados para el cumplimiento de sus funciones en colaboradores, proveedores, contratistas o terceros, es de carácter obligatorio almacenar la información en los repositorios oficiales de trabajo colaborativo (OneDrive, Teams y SharePoint) y en Opentext almacene las versiones definitivas de los registros asociados a los procesos, los que sean objeto de audtoría, documentación contractual y en general, aquella que soporta diferentes procesos de la Organización.

Las copias de respaldo se almacenarán en sitios seguros con controles físicos y tecnológicos que permitan el cumplimiento de los estándares mínimos necesarios para: preservar las copias durante los períodos definidos, limitar su acceso a los debidamente autorizados y garantizar su disponibilidad cuando el responsable de la información los requiera.

Las copias de respaldo se deben someter a pruebas periódicamente para certificar que cumplen con los propósitos para las cuales fueron realizadas. Los resultados se deben usar para actualizar la política de respaldo de información., recursos tecnológicos necesarios, evidenciar oportunidades de mejora o riesgos en la realización de copias de respaldo y restauración de información. Los responsables de la información deben participar en las pruebas para certificar formalmente que las estrategias de respaldo y restauración se ajustan a las necesidades de sus procesos.

Cuando los requisitos legales, requisitos de retención o condiciones de los medios de respaldo de información así lo dictaminen, se debe proceder a la destrucción o disposición final de medio, garantizando que la información contenida en los mismos ya no será accesible. Cuando se requiera destrucción de medios se deben seguir las políticas aprobados por el sistema de gestión de seguridad de la información de **las compañías** para la preservación del medio ambiente.

Los responsables de procesos (líderes funcionales y/o dueños de los procesos) de **las compañías** deben informar a la Gerencia de TIC/TOC, qué datos son los necesarios para el cumplimiento de sus funciones para poder establecer el conjunto las estrategias de copias de respaldo en el Sistema de Gestión de Seguridad de la Información de **las compañías**.

Los administradores de los sistemas de información de **las compañías** deben asegurar que las actividades de respaldo de información se realicen de manera controlada y permanente, que se realicen las pruebas para certificar el correcto funcionamiento de las copias y sus restauraciones, y que se mantengan registros de las actividades relacionadas con la programación, ejecución, verificación, mantenimiento, restauración y disposición final de las copias de respaldo.

Los administradores de los sistemas de información de **las compañías** deben definir e implementar los métodos a utilizar y los medios específicos requeridos para realizar las copias de respaldo de cada sistema de información o dispositivo de almacenamiento y que permitan el cumplimiento de los requisitos de la política de respaldo de información.

10.4. ELIMINACIÓN Y DESTRUCCIÓN DE MEDIOS

10.4.1. ALCANCE

El lineamiento aplica a todos los dispositivos de almacenamiento externo e interno, fijos o removibles como discos duros discos compactos, DVD, Blue Ray, Memorias flash, cintas y medios impresos utilizados para el almacenamiento de la información de ODL.

10.4.2. OBJETIVO

Asegurar la disposición final segura de todos los elementos o dispositivos que contengan información de ODL, cuando se den de baja o sean reutilizados.

10.4.2.1. Condiciones Obligatorias

Se debe verificar la eliminación, destrucción o borrado en de forma segura de cualquier software licenciado y datos sensibles de medios de almacenamiento y equipos informáticos que se den de baja, se donen, o trasladen de área.
Se debe realizar una evaluación de riesgos para los dispositivos de almacenamiento deteriorados con el fin de determinar si se deben destruir físicamente, reciclar o donar.
Los responsables de áreas y procesos deben definir y utilizar políticas formales para la eliminación segura de los dispositivos de almacenamiento para minimizar el riesgo de fuga de información sensible a personas no autorizadas.
Las políticas de eliminación segura deben incluir el uso de herramientas tecnológicas que garanticen que la información no sea recuperable o que el esfuerzo técnico para realizar su recuperación desaliente al posible interesado en recuperar la información.
Los responsables de áreas y procesos deben llevar un registro de la eliminación de los medios de almacenamiento con información clasificada como reservada con el objetivo de tener pruebas de auditoría de las políticas de eliminación segura.
Los responsables de los equipos de cómputo que se encuentren en leasing deben garantizar el debido proceso de eliminación segura de la información antes de ser retornados a la compañía de leasing, con el fin de prevenir la fuga de información.
No se deben eliminar, retirar, cambiar o donar ningún medio de almacenamiento sin la previa autorización del responsable del proceso o del área.
No se deben usar las herramientas de borrado de los sistemas operacionales para realizar la eliminación de la información de los medios de almacenamiento, se deben usar herramientas de borrador seguro.
La eliminación o donación de medios de almacenamiento debe contar con la evaluación del responsable del área o del proceso.

10.5. TRANSFERENCIA DE INFORMACIÓN 7

10.5.1. ALCANCE

Este es un lineamiento que aplica a **las compañías** y a todos los empleados, proveedores, contratistas y terceros autorizados para intercambiar información de **las compañías**.

10.5.2. OBJETIVO

Mantener la seguridad de la información cuando se autoriza el intercambio de la misma dentro de **las compañías** y con cualquier entidad externa.

10.5.2.1. Condiciones Obligatorias

La transmisión, transferencia o comunicación de información de **las compañías** se debe realizar únicamente por las redes de comunicaciones ó herramientas de trabajo colaborativo (OneDrive, Teams y Sharepointautorizados por el Sistema de Gestión de Seguridad de la Información de **las compañías**.

El acceso a la información de **las compañías** debe estar sujeto a controles que garanticen la trazabilidad de las acciones realizadas sobre la misma, considerando la identificación de la persona, proceso o sistema que realiza el acceso, acciones realizadas, instante de tiempo en que se realizan las acciones y ubicación desde la cual se realiza el acceso a la misma.

Los controles de seguridad de la información para la transferencia de información se ejecutan para mitigar los riesgos de pérdida de confidencialidad, integridad o disponibilidad de la información.

Los accesos a información deben ser sometidos a evaluaciones de riesgos tecnológicos, administrativos y operativos antes de su aprobación.

La trasferencia de información debe cumplir con los lineamientos de control de acceso a la información.

Las actividades de trabajo remoto deben cumplir con los lineamientos de Transferencia de información.

Las actividades de transferencia de medios físicos deben cumplir con los lineamientos de transferencia de información.

Para realizar actividades de transferencia de información los proveedores, contratistas y terceros que presten sus servicios a **las compañías** deberán incluir cláusulas de confidencialidad en sus contratos o suscribir acuerdos de confidencialidad con el fin reducir los riesgos de divulgación de información con carácter confidencial o interna.

En los contratos suscritos con proveedores, contratistas o terceros que presten sus servicios a **las compañías** para actividades de transferencia de información por medios electrónicos o físicos, se

[7] A.13.2. Transferencia de información. Anexo A, ISO-IEC 27001

deben establecer y acordar los requisitos de seguridad que debe cumplir el proveedores, contratistas o tercero para poder tener acceso, procesar, almacenar, comunicar y transmitir información de **las compañías**. En los acuerdos se deben incluir las medidas necesarias para el tratamiento de los riesgos de seguridad de la información derivados de las actividades realizadas por el proveedores, contratistas o tercero. Los acuerdos deben ser formalizados antes del inicio de las actividades con el proveedores, contratistas o tercero.

La transferencia de información de carácter personal deberá observar las políticas descritos en el Art. 25 de la Ley 1581 de 2012 y el Decreto reglamentario 1377 de 2013.

10.5.2.2. Usos no autorizados

- Modificación de la información sin contar con la autorización formal para dichas modificaciones.
- Divulgación no autorizada de información.
- Impedir el acceso a la información sin justificación real.
- Modificación o eliminación de los controles de seguridad que protejan la información.
- Cualquier acción sobre la información considerada como ilegal o no autorizada por las leyes, regulaciones, normas o políticas a los que está sometida **las compañías**.

Para el cumplimiento de los lineamientos de transferencia de Información, las áreas responsables de la información deben coordinar sus esfuerzos con la Gerencia de TIC/TOC para lograr la implementación de los controles que se identifiquen como necesarios para la transferencia de información para ser incluidos y fortalecer el Sistema de Gestión de Seguridad de la Información de **las compañías.**

Todos los empleados y contratistas de las compañías que en el desarrollo de sus tareas habituales u ocasionales deban realizar actividades relacionadas con la transferencia de información dentro de las compañías o con terceros son responsables del cumplimiento y seguimiento de esta política.

Los terceros que reciban información de **las compañías** se deben comprometer a proteger toda información que les sea suministrada, sin importar su nivel de clasificación para evitar su divulgación no autorizada aplicando las políticas administrativas, técnicos o legales que se acuerden con **las compañías** al momento de recibir la información.

Los proveedores, contratistas o terceros que reciban información de **las compañías** deben informar a cada uno de sus empleados o colaboradores debidamente autorizados para recibir documentos o Información, de los niveles de clasificación de la Información definidos por **las compañías** y de la existencia de acuerdos de confidencialidad con las compañías. Igualmente, el tercero debe instruir a quién reciba la información o documentos, acerca de las medidas de protección y mecanismos para manejar la información y la obligatoriedad de no utilizarla sino para los temas necesarios para el desarrollo del acuerdo suscrito entre **las compañías** y el proveedor, contratista o tercero quién será enteramente responsable por cualquier uso inadecuado de la información Suministrada por las compañías.

Cifrado de la documentación (compartimiento)

10.6. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SOFTWARE [8]

10.6.1. ALCANCE

El lineamiento que aplica para todo el personal que labore para ODL, proveedores, contratistas y terceros, con el fin de poder garantizar la adquisición y mantenimiento de los sistemas de información de manera adecuada

10.6.2. OBJETIVO

Asegurar que el software sea adquirido con los controles de seguridad requeridos en la protección de la integridad y confidencialidad de la información.

Asegurar que únicamente TIC/TOC adquiere software y/o aprueba cualquier compra relacionada.

10.6.2.1. Condiciones Obligatorias

Los requerimientos de seguridad deben ser identificados y acordados por los responsables de áreas y procesos y el usuario final antes de la adquisición de los sistemas de información.

El área de tecnología es la encargada de la adquisición de software, teniendo en cuenta las necesidades expresas por los dueños de cada proceso, o aprueba cualquier compra de software posterior al análisis de las necesidades de los dueños de procesos.

El área de tecnología debe seleccionar metodologías para adquisición de software que consideren mínimo los siguientes aspectos de seguridad y control: Control de acceso a la información, definición y autenticación de usuarios, mecanismos de detección de intrusos, definición de mecanismos de cifrado de datos, administración de la información y su confidencialidad e integridad, y administración de la seguridad física de la información.

El área de tecnología debe considerar en la adquisición de aplicaciones, los controles respectivos para la validación de datos de entrada, procesamiento, almacenamiento, hasta la salida de dichos datos, se deben considerar los controles apropiados que permitan el seguimiento de auditoría y el registro de actividades en el software. Así mismo deberá considerar la gestión adecuada de derechos de autor, propiedad intelectual, confidencialidad y normas especiales aplicables al desarrollo de software en Colombia por parte de los contratistas que desarrollen software y a nivel internacional cuando se trabaje con contratistas extranjeros.

Se debe realizar mantenimiento periódicamente a los sistemas de información con el fin de garantizar el correcto funcionamiento de los mismos.

[8] A.14.2.1. Seguridad en los procesos de desarrollo y soporte. Anexo A, ISO-IEC 27001

Se deben adoptar normas de programación de código de conformidad con los procedimientos recomendados para protegerse contra posibles vulnerabilidades conocidas, y evitar interrupciones del servicio.

El proveedor, contratista o tercero deben dar cumplimiento a los requisitos de las Compañías y de las mejores prácticas para el desarrollo de códigos seguros, deberá realizar análisis de tipo estático y dinámico de malware en el ciclo de vida del desarrollo del software, y corregir los problemas de seguridad identificados durante estos análisis de los códigos, previo a su paso al ambiente producción y se debe comprobar que se han incorporado todas las actividades clave de la seguridad en el proceso de desarrollo de sistemas, para evitar interrupciones del servicio y vulnerabilidades de seguridad.

El proveedor, contratista o tercero deben disponer de procedimientos de desarrollo seguro para sí mismo y para sus subcontratistas que incluyan la definición y comprobación de los requisitos de seguridad. Estos procedimientos deben estar documentados en detalle.

Todo desarrollo se realizará en un entorno de desarrollo y pruebas, con el fin de evitar fuga, modificación o eliminación accidental de datos y debe asegurar que la información, incluidos los datos personales, no serán utilizados en entornos que no sean de producción.

Toda adquisición y desarrollo de sistemas de información deberán incluir el suministro y/o actualización de la documentación correspondiente del sistema o módulo:

- Especificaciones funcionales
- Especificaciones de seguridad
- Manual de Instalación y configuración
- Manual de administración, operación y mantenimiento
- Manual de usuario

Deben asegurar que se entreguen los medios (programa fuente, programas objeto, licencias y manuales), de los sistemas de información para ser inventariados, contar con las garantías y licenciamientos como resultado de la adquisición o desarrollo realizado

Se debe garantizar la asignación de las licencias de los productos de software que se requieran para la prestación del servicio por parte de los proveedores, contratistas y terceros. Durante la vigencia del contrato, el proponente deberá entregar a solicitud de Las Compañías o cualquier ente de control, los respectivos soportes de titularidad de software en caso de ser requeridos.

Esta política es responsabilidad de ser ejecutada por el área de tecnología con el fin de garantizar la adquisición y mantenimiento de los sistemas de información de manera adecuada, asegurando así, la confidencialidad e integridad de la información.

10.7. GESTIÓN DE CAMBIOS9

10.7.1. ALCANCE

El lineamiento se aplica para todos los servicios, componentes operativos de información y tecnología de **las compañías**, cubre componentes como Redes de datos, servidores, computadores, dispositivos móviles, sistemas de procesamiento de información, mantenimiento y mejora de las políticas existentes de seguridad de la información y controles cuyo objetivo sea el tratamiento de información propiedad de **las compañías** o de sus clientes.

10.7.2. OBJETIVO

Garantizar que los cambios sobre la infraestructura de tecnología de información, los servicios por terceras partes, políticas, controles y comunicaciones en **las compañías** se realicen e implementen adecuadamente siguiendo políticas estándar.

10.7.3. DETALLE

Mediante esta política se establecen las directrices de alto nivel para el control de cambios permitiendo mitigar los riesgos asociados a:

- Degradación del desempeño de los componentes de procesamiento de información de las compañías
- Perdida, daño o deterioro de la información propiedad de **las compañías**
- Pérdida de productividad de las compañías generada por fallas en los componentes de procesamiento de información
- Incidentes de seguridad de la información.
- Cambios no controlados en los sistemas y los servicios de procesamiento de información.
- Gestión inapropiada de los cambios para puesta en producción de un desarrollo de software o modificaciones a componentes de tecnología de **las compañías**.

10.7.3.1. Condiciones Obligatorias

Las compañías deben dar cumplimiento a este lineamiento y del TI-P-007 PROCEDIMIENTO GESTION DE CAMBIOS TIC establecido en las comapañias para la gestión de cambios de servicios por terceras partes, infraestructura de información y tecnología y sistemas de procesamiento de información, en donde están claramente definidas las responsabilidades y actividades necesarias para la planificación, evaluación, ejecución y revisión de los cambios.
Todos los cambios a la infraestructura de Información y Tecnología deben estar plenamente justificados y aprobados.
Los cambios deben ser propuestos e implementados sin perjuicio de la calidad de los servicios prestados en la Gerencia TIC /TOC de **las compañías.**
Todos los cambios deben ser formalmente documentados.
Todos los cambios deben incluir una evaluación de riesgos, análisis de los impactos del cambio y especificar los controles de seguridad que sean necesarios adoptar (si aplica).
Todos los cambios deben ser sometidos a algún mecanismo de prueba que permita verificar si su planificación está completa antes de su ejecución.

[9] A.14.2.2 Procedimiento de control de cambio s en sistemas. Anexo A, ISO-IEC 27001

Solamente se ejecutan los cambios que han sido debidamente autorizados por **los lideres funcionales o Dueños de servicios.**
Todos los cambios deben estar formalmente registrados, clasificados y documentados de acuerdo a lo establecido en el TI-P-007 PROCEDIMIENTO GESTION DE CAMBIOS TIC.
Todos los cambios deben poderse deshacerse mediante planes de "retirada del cambio o rollback" en caso de un incorrecto funcionamiento tras su implementación.
Cuando se realicen cambios a la infraestructura de información, tecnología de comunicaciones o tecnología de la operación de las compañías, se debe verificar la necesidad de actualizar los planes de contingencia y continuidad de negocio.
Cuando se realicen cambios se debe tener en cuenta si existe la necesidad de formación adicional para el personal, documentar los costos, soporte, requerimientos tecnológicos administración y mantenimiento.
Se debe documentar los cambios hechos por **las compañías** en cuanto a mejoras del servicio actuales ofrecidos por terceros, desarrollo de todos los aplicativos nuevos, controles nuevos para resolver los incidentes de seguridad de la información, modificaciones o actualizaciones de las políticas de la organización. Teniendo en cuenta la importancia de los sistemas y procesos involucrados.
Se deben gestionar los servicios a implementar por terceros como: cambios y mejoras en las redes, uso de nuevas tecnologías, actualización de productos nuevos o nuevas versiones, nuevas herramientas y entornos de desarrollo, cambios de la ubicación física de las instalaciones de los servicios y cambio de proveedores.
Los ambientes de desarrollo, prueba y productivo, siempre que sea posible, estarán separados, y se definirán y documentarán las reglas para la transferencia de software desde el estado de desarrollo hacia el estado operativo.

Para ello, se tendrán en cuenta los siguientes controles:

- Ejecutar el software en diferentes ambientes de operaciones, equipos, o directorios.
- De ser posible, separar las actividades de desarrollo y prueba, en entornos diferentes.
- Impedir el acceso a los compiladores, editores y otros utilitarios del sistema en el ambiente operativo, cuando no sean indispensables para el funcionamiento del mismo.
- Utilizar sistemas de autenticación y autorización independientes para los diferentes ambientes, así como perfiles de acceso a los sistemas.
- Recomendar a los usuarios no compartir contraseñas en estos sistemas.
- Las interfaces de los sistemas identificarán claramente a qué instancia se está realizando la conexión.
- El proveedor, contratista o tercero que efectúe los desarrollos (consultor funcional o desarrollador) no tendrá acceso transaccional al ambiente operativo. En caso de excepción, necesidad, se establecerá la autorización por la Gerencia de TIC/TOC, conservando la documentación y registro de dichos accesos.

10.7.3.2. Usos no autorizados

No se deben realizar cambios en los ambientes operativos de acuerdo con el alcance definido (9.7.1), sin la previa autorización de **las compañías**.
No se deben aceptar cambios por parte de la prestación del servicio de terceros, sin el previo estudio, aprobación y su debida documentación.

No se debe poner en peligro la integridad de la información debido a la falta de revisión de los cambios.
No se deben realizar cambios por usuarios no autorizados.
No se pueden realizar cambios que atenten o vayan en contra de las estrategias de continuidad y seguridad definidas por **las compañías**.

Los responsables de áreas o procesos deben evaluar periódicamente los riesgos que se identifiquen sobre los cambios en la contratación de servicios de procesamientos de información con terceros. Los resultados de la evaluación de riesgos deben generar propuestas de mecanismos de control que mitiguen los impactos de los riesgos identificados.

El personal de **las compañías** debe reportar mediante los conductos aprobados la solicitud de cambios o nuevos requerimientos tecnológicos, de servicios o sistemas de información.

Los terceros responsables de la prestación de servicios a la empresa deben cumplir con las políticas de seguridad de la información adoptadas por las compañías en cuanto a cambios que pretendan realizar en la prestación del servicio.

10.8. USO DE CORREO ELECTRÓNICO

10.8.1. ALCANCE

El lineamiento aplica a todos los empleados, contratistas y terceros que presten sus servicios a **las compañías** que por el desarrollo de sus actividades utilizan el servicio de correo electrónico de **las compañías**.

10.8.2. OBJETIVO

Definir las pautas generales para asegurar una adecuada protección de la información de **las compañías** cuando se usa el servicio de correo electrónico por parte de los usuarios autorizados

10.8.2.1. Condiciones Obligatorias

El servicio de correo electrónico institucional debe ser utilizado exclusivamente para las tareas propias de la función desarrollada por **las compañías,** los usos diferentes a los necesarios para el cumplimiento de las funciones encargadas al funcionario, contratista o tercero y son de entera responsabilidad del usuario al que se le asigna la cuenta de acceso al servicio. Por lo anterior no se permitirá un uso con fines personales del correo institucional.
El acceso al servicio de correo electrónico debe ser autorizado por el gerente de área al que pertenece el funcionario, contratista o tercero que presta sus servicios a **las compañías** y por la Gerencia TIC
Para creación de la cuenta de correo electrónico se seguirán las lineamientos definidos en el documento TI-I-001 Instructivo Gestión de Usuarios Directorio Activo.El uso de las cuentas de correo electrónico debe cumplir con los estándares de creación y utilización de cuentas de usuario de **las compañías.**
El servicio de correo electrónico oficial de **las compañías** es el que es suministrado y gestionado por el Sistema de Gestión de Seguridad de la Información, el cual cumple los requerimientos técnicos y de seguridad necesarios para garantizar la confidencialidad, integridad y disponibilidad de las

comunicaciones oficiales por correo electrónico. Los usuarios reconocen y aceptan que los incidentes de seguridad de la información generados por el uso de servicios de correo electrónico no autorizados serán de su entera responsabilidad.

La clave de acceso al servicio de correo electrónico no debe ser divulgada a ninguna persona, exhibirse en público y para su gestión se debe seguir los controles de protección de contraseñas definidos por el Sistema de Gestión de Seguridad de la Información de **las compañías**.

Las compañías pueden supervisar el uso del servicio de correo electrónico para verificar que se está usando para el cumplimiento de las funciones misionales de las compañías.

Los correos electrónicos externos deben contener una nota de confidencialidad ubicada al final del texto, después de la firma del mismo, este mecanismo es una medida preventiva de divulgación no autorizada de contenidos de correo electrónico. La nota de confidencialidad debe seguir el estándar definido por el Sistema de Gestión de Seguridad de la Información de **las compañías.**

Al finalizar su relación laboral todo funcionario, contratista o tercero que preste sus servicios a **las compañías**, debe realizar la devolución de la información de correo electrónico al responsable del proceso para el cual laboraba. El área Talento Humano o el administrador del contrato notificará el bloqueo/eliminación de accesos en los sistemas de la Compañía mediante un correo al Helpdesk..

10.8.2.2. Usos no autorizados

Los usos no autorizados constituyen un incidente de seguridad de la información y se tratan de acuerdo con las políticas adoptados por **las compañías**:

- Envío de correos masivos sin autorización oficial, del área autorizada para el envío de correos masivos es Comunicaciones.
- Envío, reenvío o intercambio de mensajes no deseados o considerados SPAM.
- Envío o intercambio de mensajes con contenido que atente contra la integridad de las personas o instituciones, tales como contenidos ofensivos, obscenos, pornográficos, terroristas, discriminación sobre la base de raza, género, nacionalidad de origen, edad, estado marital, orientación sexual, religión o discapacidad, amenazas, cualquier contenido que represente riesgo para la seguridad de la información de las compañías o esté prohibido por la leyes, regulaciones o normas a las cuales está sujeta las compañías.
- Creación, almacenamiento o intercambio de mensajes que violen las leyes de material protegido por la ley de derechos de autor, normas sobre seguridad de la información y protección de datos personales.
- Crear, enviar, alterar, borrar mensajes suplantando la identidad de un usuario.
- Abrir, usar o revisar indebidamente la cuenta de correo electrónico de otro usuario, sin contar con la autorización formal del titular de la cuenta.
- Uso, envío, reenvío o intercambio de mensajes con uso de plataformas de intercambio de archivos como P2P.

10.9. USO DE SERVICIOS DE ACCESO A INTERNET10

10.9.1. ALCANCE

Es un lineamiento de **las compañías** que aplica a toda la empresa y a todos los usuarios autorizados para acceder al servicio de Internet en las compañías.

10.9.2. OBJETIVO

Definir las pautas generales para asegurar una adecuada protección de la información de **las compañías** en el uso del servicio de Internet por parte de los usuarios autorizados.

10.9.2.1. Condiciones Obligatorias

El servicio de acceso a Internet debe utilizarse exclusivamente para las tareas propias de la función desarrollada en **las compañías**, los usos diferentes a los necesarios para el cumplimiento de las funciones son de entera responsabilidad del usuario al que se le asigna la cuenta de acceso al servicio.
El acceso al servicio podrá ser asignado a las personas que tengan algún tipo de vinculación con **las compañías**, ya sea como empleado, contratista o tercero. El acceso al servicio es solicitado por el responsable del área o proceso de las compañías.
El navegador autorizado para el uso del servicio de Internet en **las compañías** es el designado por el Sistema de Gestión de Seguridad de la Información de **las compañías**, el cual cumple con todos los requerimientos técnicos y de seguridad de la información.
Los servicios a los que un determinado usuario pueda acceder desde Internet dependerán del rol que desempeña el usuario en **las compañías**, este permiso se asigna a través de las funcionalidades contenido Perfiles APP Control y Webfilter configuradas desde el firewall
Todo usuario es responsable de informar sobre los contenidos o acceso a servicios que no le estén autorizados o no correspondan a sus funciones dentro de **las compañías**.
Todo usuario es responsable tanto del contenido de las comunicaciones como de cualquier otra información que se envíe desde la red de **las compañías** o descargue desde Internet empleando la cuenta de acceso a Internet que se le ha suministrado.
Las compañías pueden supervisar el acceso del servicio de Internet para certificar que se está usando para el cumplimiento de las funciones institucionales.
Cuando un empleado o contratista al que le haya sido autorizado el uso de una cuenta servicio de Internet o de acceso a la red local de las compañías finalice su vinculación, deberá seguir las políticas definidos por para entregar su cuenta de usuario y accesos a servicios informáticos provistos.

10.9.2.2. Usos no autorizados

Los siguientes usos se consideran usos no autorizados del servicio de acceso a Internet. Los usos no autorizados constituyen un incidente de seguridad de la información:

- Envío o descarga de información sometida a derechos de autor cuando no se tienen esos derechos.

[10] A.9.1.2. Acceso a redes y a servicios en red. Anexo A, ISO-IEC 27001

- Envío, descarga o visualización de información con contenidos que no forman parte de las actividades propias asignadas al usuario
- Envío o descarga de información cuyo volumen ponga en riesgo la disponibilidad del servicio, los usuarios del servicio deben informarse de las políticas para descarga de información con los responsables de áreas o procesos.
- Cualquier otro propósito considerado inmoral o ilegal de acuerdo con las leyes, regulaciones o normas a las que está sometida las compañías.
- No es aceptable el uso del servicio de acceso a Internet para actividades comerciales.
- Está prohibido el uso del servicio de acceso a Internet para realizar o propiciar propaganda de productos o propaganda política.
- Queda estrictamente prohibido el uso, autorizado o no, de un nombre de usuario distinto al designado por el responsable de área o proceso o administrador de sistema de información.
- No está autorizado el acceso a sitios Web relacionados con actividades de juego, apuestas, o actividades ilegales en general.
- No está autorizado el acceso a material pornográfico o a sitios Web de contenido para adultos relacionados con desnudismo, erotismo o pornografía, salvo en los casos que estén expresa y formalmente autorizados con apego a funciones explícitamente definidas para el empleado, caso particular de investigaciones en procesos judiciales, en dichos casos se debe gestionar los mecanismos de acceso seguro en canales protegidos configurados por los responsables de administración de tecnología durante el tiempo requerido para el cumplimiento de la asignación.
- El acceso a sitios de música, juegos, vídeos está limitado para el uso con propósitos laborales.
- No está autorizado el acceso a sitios Web de carácter discriminatorio, racista, o material potencialmente ofensivo incluyendo, bromas de mal gusto, prejuicios, menosprecio, o acoso explícito.
- No está autorizado el acceso a sitios de “hacking” o sitios reconocidos como inseguros, los cuales puedan poner en riesgo la integridad y confidencialidad de la información de las compañías.
- Participación en cualquier actividad ilegal o criminal mediante las redes de comunicaciones de las compañías.
- Instalación y uso de programas de transferencia de información vía Internet para el intercambio de archivos.

Las excepciones a dicha política serán aprobadas por el jefe de área, profesional de seguridad de la información y por el responsable de Telecomunicaciones.

Los empleados responsables de los procesos de las compañías son los autorizados para solicitar la creación, modificación o cancelación de las cuentas de acceso al servicio de Internet.
Todos los empleados y contratistas que, en el desarrollo de sus tareas habituales u ocasionales, utilicen cualquier servicio de tecnología de la información y comunicaciones (TIC) que provea **las compañías** son responsables del cumplimiento y seguimiento de ésta política.

Los responsables de la administración de tecnología deben de implementar los controles necesarios para evitar la circulación de información o contenidos desde Internet hacia la red de **las compañías** que puedan constituirse en riesgos para la seguridad de la Información.
Los responsables de la administración de tecnología deben garantizar que cualquier conexión de red de comunicaciones se encuentre protegida mediante controles de seguridad que garanticen la confidencialidad, integridad y disponibilidad de la información.

10.10. ANTIVIRUS

10.10.1. ALCANCE

Es un lineamiento que aplica a todos los equipos informáticos (computadores, tabletas, equipos portátiles, teléfonos inteligentes, entre otros) que sean utilizados para conexión con los servicios o sistemas de información de las compañías, ya sea de empleados directos, empleados en misión, contratistas, proveedores o terceros.

10.10.2. OBJETIVO

Definir las pautas generales para asegurar una adecuada protección de la información de **las compañías** contra software malicioso.

10.10.2.1. Condiciones Obligatorias

Es obligatorio usar un software de protección contra código malicioso (antivirus) en todos los computadores, dispositivos móviles y cualquier tipo de equipo de cómputo empleado para acceder a los servicios y sistemas de información de **las compañías**.
Es obligatorio que el software contra código malicioso (antivirus) siempre se encuentre actualizado con la versión más reciente de base de datos de virus.
El software de antivirus siempre debe estar activo en los computadores, dispositivos móviles equipos de cómputo desde los cuales se accede a los servicios de las compañías
Es obligatorio aplicar los controles de seguridad que defina el Sistema de Gestión de Seguridad de la Información de **las compañías** para evitar incidentes de seguridad de la información generados por la presencia de código malicioso en los equipos de cómputo, redes de comunicaciones, dispositivos de almacenamiento fijos o removibles de los computadores o dispositivos informáticos.
Los usuarios finales de los computadores no deben detener, desinstalar o alterar el funcionamiento del software de antivirus. Las modificaciones sobre el software de antivirus solo deben ser realizadas por personal formalmente autorizado por el Sistema de Gestión de Seguridad de la Información de **las compañías**.
Es obligatorio realizar verificaciones periódicas automáticas a los computadores de **las compañías**, de acuerdo con el estándar que defina el Sistema de Gestión de Seguridad de la Información de **las compañías**.
Todo contratista, proveedor o tercero que se conecte a la red de las compañías debe tener instalado en su equipo un antivirus vigente para poder autorizar su conexión.

10.10.2.2. Usos no autorizados

Esta formalmente prohibida la utilización de software de código malicioso dentro de la infraestructura tecnológica de **las compañías**. El Personal que cuenta con autorización para atención de incidentes de seguridad de la información debe tramitar autorización específica para la utilización de software de código malicioso con propósitos de tratamiento de incidentes de seguridad en equipos de **las compañías** y siempre en ambientes aislados no productivos.
El Sistema de Gestión de Seguridad de la Información de **las compañías** es responsable del aseguramiento en la administración del servicio de antivirus corporativo.

10.11. USO DE DISPOSITIVOS MÓVILES11

10.11.1. ALCANCE

Estos lineamientos se aplican para cualquier equipo o dispositivo móvil de propiedad de **las compañías** y que por necesidad de los servicios que presta, requiere acceso a la información, los sistemas de información o los servicios de tecnología de información de **las compañías**.

En cuanto a los dispositivos móviles de propiedad personal, y que tengan acceso a la información o los sistemas de información de las compañías, es responsabilidad de los usuarios mitigar las amenazas y acatar las recomendaciones de seguridad que se describen en la TI-G-008 GUÍA DE BUENAS PRACTICAS DE CIBERSEGURIDAD PARA EL USO DE DISPOSITIVOS MÓVILES PERSONALES.

10.11.2. OBJETIVO

Garantizar la seguridad de la información cuando se utilizan dispositivos móviles en las Instalaciones de **las compañías** o cuando se usan para tener acceso a sistemas de información o servicios de procesamiento de información, aunque no se encuentren dentro de instalaciones de **las compañías**.

10.11.2.1. Condiciones obligatorias

Los dispositivos móviles destinados a ser utilizados fuera de las instalaciones de **las compañías** que deban tener acceso o que contengan información clasificada con carácter confidencial (**TI G 003 Guía de clasificación de Activos de Información V2**) seguir las recomendaciones y buenas prácticas para el acceso de sistemas de información mediante el uso de dispositivos móviles externos se establecen en la TI-G-008 Guía de buenas prácticas de ciberseguridad para el uso de dispositivos móviles personales

La conexión de dispositivos móviles a las redes de comunicaciones de **las compañías** desde redes de terceros debe utilizar canales seguros de comunicación que impidan el acceso no autorizado a información con carácter interno o confidencial. Los canales de acceso seguro son configurados por los administradores de sistemas de información.

En caso de pérdida o hurto de dispositivos móviles de **las compañías** o dispositivos móviles personales con acceso a la información de las compañías, el responsable del dispositivo debe notificar a la mayor brevedad posible a los responsables de áreas y procesos y a la autoridad

[11] A.6.2.1 Política para dispositivos móviles. Anexo A, ISO-IEC 27001

competente para que se tomen las acciones necesarias para impedir el uso no autorizado de la información en el dispositivo.

Usos no autorizados

La modificación de los controles de seguridad implantados en los dispositivos móviles no está autorizada si ello implica un riesgo para la seguridad de la información de **las compañías**

Solamente el personal técnico debidamente autorizado puede realizar instalación, desinstalación o borrado de software en los dispositivos móviles de **las compañías**.

Todos los empleados y contratistas de **las compañías** son responsables de reportar a la mayor brevedad posible la pérdida o hurto de los dispositivos móviles bajo su responsabilidad mediante la mesa de ayuda.

El área de tecnología es la responsable de coordinar y gestionar la instalación de controles de seguridad en los dispositivos móviles de propiedad de **las compañías.**

10.12. USO ACEPTABLE DE LOS ACTIVOS DE INFORMACIÓN12

10.12.1. ALCANCE

Es un lineamiento qué aplica para todos los empleados, contratistas y terceros que presten sus servicios a **las compañías** responsables de usar o administrar activos de información de **las compañías**.

10.12.2. OBJETIVO

Definir las pautas generales para asegurar un adecuado uso y administración de los activos informáticos de **las compañías** por parte del personal a cargo de su administración.

10.12.2.1. Condiciones Obligatorias

Las actividades de administración y operación de los activos de información de **las compañías** deben estar orientadas a garantizar la prestación de los servicios necesarios para el cumplimiento de la misión de las compañías, los usos diferentes deben ser formalmente autorizados.

Las compañías mantienen y mejora continuamente el inventario de los activos de información que son de vital importancia para el desarrollo de sus funciones misionales.

Todos los empleados de **las compañías** deben reportar sin demoras injustificadas a los responsables de sus áreas o los responsables de los procesos en los cuales cumple sus funciones cualquier evento que pueda afectar la integridad, disponibilidad o confidencialidad de cualquier activo de información de las compañías.

Todos los empleados de **las compañías** deben aplicar la política de gestión de riesgos para identificar y tratar los riesgos que puedan afectar a sus activos de información. Cada responsable de proceso o área debe coordinar la aplicación de la política institucional de gestión de riesgos sobre los activos a su cargo.

[12] A.8.1 Responsabilidad por los activos. Anexo A, ISO-IEC 27001

Los cambios sobre la información de las compañías deben estar autorizados por el dueño del servicio o el proceso al que pertenece la información.
Todos los empleados de **las compañías** deben desarrollar las acciones requeridas, para garantizar la seguridad de la información.
Todos los empleados de **las compañías** deben aplicar los controles de seguridad de la Información definidos el sistema de gestión de seguridad de la información de **las compañías** para reducir los riesgos que afectan a la seguridad de la información.

10.12.2.2. Usos no autorizados

Esta formalmente prohibido realizar cambios a los activos informáticos de **las compañías** sin contar con la autorización formal del responsable de las áreas o proceso en el que este el activo informático.
Esta formalmente prohibida la divulgación de información de las compañías a personal o terceros que no estén autorizados.
Esta formalmente prohibido Impedir el acceso a la información a los debidamente autorizados sin justificación real.
Esta formalmente prohibido utilizar los activos de información de las compañías para fines diferentes al cumplimiento de las funciones asignadas y el cumplimiento de la misión institucional.
El área de tecnología de **las compañías** debe generar y mantener un registro detallado de todos los eventos que sucedan sobre los diferentes activos de información.
El área de tecnología de **las compañías** debe coordinar sus esfuerzos para realizar el mejoramiento de los servicios informáticos de las compañías, así como de controlar cualquier cambio que afecte los niveles acordados para la prestación de los servicios.
La Gerencia TIC y los responsables de áreas y procesos de **las compañías** deben coordinar la realización del inventario de activos de información.

El área de tecnología y los administradores de equipos informáticos:

- Mantener y aplicar las políticas de operación de los equipos o servicios informáticos definidos por el sistema de gestión de seguridad de la Información de **las compañías**.
- Aplicar y mantener los acuerdos de confidencialidad sobre la información a su cargo.
- Mantenimiento y aplicación de las responsabilidades para la administración y operación de los activos de información identificados a su cargo.
- Mantener actualizado el registro de riesgos que afecte a los activos bajo su responsabilidad.
- Reportar lo cambios que sucedan sobre los activos a su cargo ante los responsables de áreas o procesos de **las compañías**.
- Aplicar las políticas que defina el sistema de gestión de seguridad de la información de **las compañías** para el acceso de terceros a los componentes a su cargo en situaciones como mantenimiento o garantía.
- Mantenimiento de registros del desempeño de los equipos o servicios a su cargo.
- Mantenimiento de registros que muestren las actividades realizadas por los administradores o los operadores de los equipos o servicios a su cargo.
- Mantenimiento de los registros de las fallas sobre los equipos o servicios a su cargo.
- Mantener registros de los usuarios a los cuales se les ha otorgado acceso a cada activo, servicio o componente.

- Realizar una revisión periódica de los privilegios de acceso otorgados a los usuarios de los servicios o componentes a su cargo.
- Coordinar la aplicación de las políticas definidos el sistema de gestión de seguridad de la Información de **las compañías** para la asignación de cuentas de usuario y contraseñas de acceso a servicios y componentes.
- En coordinación con los responsables de los procesos y áreas de **las compañías** aplicar las medidas de mitigación que se definan en el sistema de gestión de seguridad de la Información de **las compañías** para contrarrestar las vulnerabilidades que se identifiquen sobre los componentes o servicios de tecnología.
- Mantener y aplicar de las políticas de respaldo de la información.
- Mantener, Mejorar y probar periódicamente las políticas de contingencia, recuperación ante desastres y continuidad en la prestación de servicios de tecnología.
- Implementar, mantener y mejorar de los controles de protección física lógica o procedimental que defina el sistema de gestión de seguridad de la Información de **las compañías** para la protección de los activos de información, componentes o servicios a su cargo.
- Los activos de información se ubican en países / ubicaciones autorizados, incluidas las instalaciones de recuperación ante desastres.
- Los activos de información deben protegerse con mecanismos de prevención de pérdida de información, antivirus, sistemas de detección de intrusos en la red, cifrado de disco duro.
- Todos los controles relacionados con los servicios en la nube deben ser tratados y acordados con las Compañías.

10.13. ESCRITORIO Y PANTALLA LIMPIOS [13]

10.13.1. ALCANCE

Es un lineamiento que aplica a cualquier tipo de información que repose en escritorios, áreas de trabajo, computadores, equipos portátiles, documentos en papel, medios de almacenamiento y en general cualquier tipo de información que utilicen los empleados, contratistas o terceros vinculados a **las compañías**.

10.13.2. OBJETIVO

Definir las pautas generales para reducir el riesgo de acceso no autorizado, pérdida o daño de la información disponible de los puestos de trabajo durante y fuera del horario trabajo normal de los empleados, contratistas y terceros que prestan sus servicios a **las compañías.**

10.13.3. DETALLE

Todos los empleados, contratistas y terceros que presten sus servicios a **las compañías** deben aplicar los controles recomendados por el sistema de gestión de seguridad de la información o el

[13] A.11.2. Equipos. Anexo A, ISO-IEC 27001

responsable de la información para impedir el acceso no autorizado de terceros a la información de la organización.

Los lugares de trabajo de empleados, contratistas y terceros que prestan sus servicios a **las compañías** y cuyas funciones no obliguen a la atención directa de público se deben localizar preferiblemente en ubicaciones físicas que no queden expuestas al público para minimizar los riesgos asociados a acceso no autorizado a la información o a los equipos informáticos.

En los puntos de atención al público se debe evitar el acceso a información no indispensable para la prestación de los servicios

Durante las ausencias temporales o definitivas el personal de **las compañías** se debe bloquear la pantalla de los computadores a su cargo con el protector de pantalla designado por el sistema de gestión de seguridad de la información, para impedir el acceso de terceros no autorizados a la información almacenada en el computador.

Durante ausencias temporales o definitivas el personal de **las compañías** debe guardar en un lugar seguro los documentos físicos o medios de almacenamiento para impedir su pérdida, daño o acceso por parte de personal no autorizado.

Los documentos impresos y los archivos electrónicos clasificados con carácter confidencial siempre deben permanecer custodiados o protegidos en áreas seguras para evitar su divulgación no autorizada. Ver TI-G-003 GUÍA DE CLASIFICACIÓN Y VALORACION ACTIVOS DE INFORMACIÓN

Cuando esté autorizada la impresión o reproducción de documentos clasificados con carácter confidencial, se deben retirar inmediatamente de los dispositivos empleados para su impresión o reproducción.

Todos los computadores y cuando sea factible en equipos de impresión o reproducción deben tener configurada una cuenta con privilegios de administrador que permita realizar labores de instalación, configuración, soporte y mantenimiento, el uso de dicha cuenta es de responsabilidad exclusiva del personal que presta los servicios de soporte tecnológico en cada dependencia de **las compañías.**

Para el acceso a cualquier computador de **las compañías** se debe hacer uso de una cuenta y una contraseña que serán únicos, exclusivos, personales e intransferibles para cada usuario de **las compañías**

Todos los computadores de **las compañías** deben tener configurado y operativo un protector de pantalla que se active cuando el equipo no esté en uso y bloquee el acceso con contraseña al equipo cuando no esté en uso por parte del funcionario, contratista o tercero que presten sus servicios a **las compañías.**

10.14. SEGURIDAD DE LA INFORMACIÓN PARA RELACIONES CON PROVEEDORES, CONTRATISTAS Y TERCEROS14

10.14.1. ALCANCE

El presente lineamiento de seguridad es aplicable a los proveedores, contratistas y terceros, que tengan alguna relación con **las compañías**, bien sea de tipo legal, contractual o de cualquier otra índole no laboral y que, en razón de ésta, tengan acceso a información, sistemas de información, centros de cómputo, redes de telecomunicaciones o tecnologías de información y comunicaciones de propiedad de **las compañías**.

10.14.2. OBJETIVO

Mantener la seguridad de la información y los servicios de procesamiento de información a los cuales tienen acceso los proveedores, contratistas o terceros que prestan sus servicios a **las compañías**.

10.14.2.1. Condiciones obligatorias

Los proveedores, contratistas o terceros que presten sus servicios a **las compañías** que contemplen la gestión, almacenamiento, custodia, transformación o transmisión de información de **las compañías** deben conocer, aceptar y cumplir la política de seguridad de la información y lineamientos definidos por el sistema de gestión de seguridad de la Información; donde el administrador del contrato deberá realizar la evaluación de riesgos de ciberseguridad en el Formato TI-F-030 Clasificación Proveedores – Ciberseguridad, para determinar la criticidad de los servicios prestados por terceros frente a los riesgos de Ciberseguridad (alta, media o baja), de acuerdo con las actividades a realizar y el acceso a sistemas de información. Acorde al nivel de criticidad se aplicarán los siguientes controles establecidos:

Los Proveedores, contratistas **y terceros darán cumplimiento a los siguientes Controles de nivel bajo:**

Con el propósito de garantizar el buen desarrollo del presente vínculo comercial, EL PROVEEDOR, contratista o terceo realizará a todos los aspirantes el proceso de selección y el respectivo estudio de seguridad.

Para el acceso a cualquier tipo de información o sistema de información, los proveedores, contratista y terceros que presten sus servicios a las compañías darán cumplimiento a la cláusula CONFIDENCIALIDAD Y PROPIEDAD INTELECTUAL del contrato establecido, con el fin de reducir los riesgos de divulgación de información con carácter confidencial o interna.

Garantizar que se acoge a los procedimientos de manejo de usuarios y contraseñas y cumplan con la Política de Seguridad de la Información y Ciberseguridad y el Manual del Sistema de Gestión de Seguridad de la Información de las Compañías, para los sistemas propios del PROVEEDOR, contratista o tercero que sean partes del servicio como los sistemas de Las Compañías a los que acceda el PROVEEDOR.

[14] A.15. Relaciones con los proveedores. Anexo A, ISO-IEC 27001

Se debe evitar el incumplimiento de las obligaciones legales, estatutarias, de reglamentación o contractuales relacionadas con la Seguridad de la Información y ciberseguridad de cualquier requisito de seguridad expedido por los entes de vigilancia y control que rigen para Las Compañías.

Las Compañías podrán llevar a cabo auditorías, a través de colaboradores de la compañía o firmas especializadas, con el fin de verificar que los servicios se ejecuten bajo las condiciones de seguridad de la información y ciberseguridad definidas en las diferentes cláusulas del contrato. Los proveedores, contratista y terceros se comprometen a corregir las situaciones identificadas en las auditorías, que pongan en riesgo la seguridad de la información. De igual manera, las compañías se reservan el derecho de verificar la veracidad de la información suministrada por los proveedores y terceros, para tal fin, podrá solicitar la documentación adicional que considere necesaria y visitar las instalaciones de los proveedores, contratista y terceros cuando lo considere necesario.

Se debe implementar la protección contra malware más actualizada a todos los activos informáticos utilizados para proporcionar el servicio, a fin de evitar la interrupción del servicio o incidente de seguridad de la información y ciberseguridad, acorde con los requerimientos de las Compañías para este fin.

Se debe utilizar los controles requeridos para establecer medidas de protección contra la transferencia de código malicioso a sistemas de las Compañías, clientes de las Compañías y terceros a través de sistemas de las Compañías o del Proveedor.

Los Proveedores, contratistas y terceros prestadores de un servicio de criticidad Media **darán cumplimiento a los controles de nivel bajo y a los siguientes Controles de nivel Medio:**

Se debe contar con políticas de seguridad de la información y ciberseguridad acordes con estándares internacionales, así como con procedimientos, estándares, procesos de gestión y supervisión de los requisitos normativos, jurídicos y de riesgos relacionados con la ciberseguridad, del entorno y operativos del proveedor.

Se deberá garantizar que incorpora prácticas líderes de seguridad de la información en sus procesos tales como:

- Una clara definición de los roles y responsabilidades en Seguridad de la Información para todos los funcionarios y/o contratistas de su organización.

- Desarrollar material de formación adecuado, que incluya capacitación y concienciación sobre ciberseguridad, y asegurarse de que todos los empleados correspondientes reciban una formación adecuada para desempeñar sus funciones y responsabilidades.

- Controles establecidos para evitar la fuga de información de las Compañías

Se deberá limitar el acceso a puertos lógicos (USB), internet, envío o recepción de correo electrónico, mensajería instantánea u otro servicio de intercambio de información en los equipos de cómputo utilizados en sus instalaciones, exclusivamente a los sitios web, aplicativos o sistemas de información requeridos para prestar el servicio a Las Compañías y así mitigar fuga de información, tanto para funcionarios como para contratistas. Para el intercambio de información se realizará mediante las herramientas de trabajo colaborativo (onedrive, teams y sharepoint)

Se deberá garantizar que incorpora en la prestación del servicio herramientas de seguridad sin estar limitadas a Perimetral, Red, EndPoint, entre otras, que mitiguen los riesgos de seguridad, como mínimo los siguientes controles:

- Antivirus
- Control de Navegación
- Control de Correo
- Control de medios extraíbles

Se deberá garantizar que los recursos lógicos y bases de datos utilizados para la prestación del servicio a Las Compañías se encuentren separados (virtual y/o físicamente) de otros clientes.

Se debe contar con programas de mantenimiento preventivo para la infraestructura tecnológica crítica para el servicio contratado por Las Compañías. De igual forma deberán contar con programas de mantenimiento preventivos en la infraestructura prestadora de servicios, con mecanismos de control de temperatura y humedad en los sitios que lo requiera el servicio contratado por Las Compañías.

Se debe asegurar las operaciones correctas y seguras de las instalaciones de procesamiento de información.

Se debe garantizar el respaldo de la información generada o entregada por Las Compañías y la ejecución de pruebas periódicas de restauración, para mitigar riesgos de perdida. Al finalizar la relación contractual, deberá entregar toda la información en la estructura requerida y certificar la eliminación segura de la información de Las Compañías de su infraestructura tecnológica y nube para la prestación del servicio.

Se debe asegurar la protección y segregación de la información en las redes, y sus instalaciones de procesamiento de información de soporte.

Se debe mantener controles que garanticen la confidencialidad e integridad de la información dentro y fuera de la organización.

Se debe asegurar que la Seguridad de la Información sea una parte integral de los sistemas de información durante todo su ciclo de vida.

Se deberá cumplir con estándares de desarrollo como OWASP, OAUTH 2.0, entre otros para la prestación del servicio.

Se deberá asegurar la gestión de incidentes de seguridad de la información, los cuales deberán ser notificados a las Compañías.

Se deberá realizar periódicamente evaluaciones de riesgo relacionado con la seguridad de la información y la ciberseguridad, como mínimo una vez al año, e implementar los controles que se requieran para mitigar los riesgos identificados. Si se identifica un riesgo material que pueda afectar negativamente a la reputación o el servicio prestado a las Compañías, el proveedor debe notificárselo a las Compañías de forma inmediata.

Sin perjuicio de otros derechos, las Compañías pueden realizar una evaluación del riesgo de cualquier incumplimiento notificado por el Proveedor a las Compañías, y determinar un plazo para que el Proveedor adopte las medidas necesarias.

Se debe asegurar que la información, incluidos los datos personales, no serán utilizados en entornos que no sean de producción.

Se debe disponer de procedimientos de desarrollo seguro para sí mismo y para sus subcontratistas que incluyan la definición y comprobación de los requisitos de seguridad. Estos procedimientos deben estar documentados en detalle.

Debe asegurarse de separar las funciones para el desarrollo de sistemas. Esto incluye asegurarse de que los desarrolladores de sistemas no tengan acceso al entorno productivo.

Los Proveedores, contratistas y terceros prestadores de un servicio de criticidad Alta **darán cumplimiento a los controles de nivel bajo, Medio y a los siguientes Controles de nivel Alto:**

Se debe garantizar que realiza una clasificación de sus activos de información y aplica medidas de protección, para mitigar riesgos de fuga y/o perdida de información.

Se debe contar con controles de acceso lógico y físico robustos a todas las dependencias, donde se procesa, almacena, resguarde o transmite información de Las Compañías.

Se debe garantizar la ejecución de pruebas de vulnerabilidad y/o Ethical Hacking para las aplicaciones o sistemas de información que sean parte del servicio ofertado, para comprobar su seguridad, se deben ejecutar como mínimo una vez al año. La primera prueba se debe realizar antes de iniciar el servicio y los resultados, incluyendo las remediaciones, deben ser entregados a Las Compañías como mínimo una semana antes del inicio del servicio. Si se identifican vulnerabilidades de tipo CRITICO, se deben corregir antes del inicio de operación. Durante la vigencia del contrato las vulnerabilidades CRITICAS identificadas se deben remediar de forma inmediata, las MEDIAS Y BAJAS en acuerdo con Las Compañías.

Se debe contar con procedimientos definidos para la planeación de capacidad de los sistemas de información.

Se debe tener una clara definición de la arquitectura de seguridad en sus redes inalámbricas (WiFi) que mitigue la generación de brechas de seguridad en el resto de la red.

Se debe aplicar procedimiento de monitoreo de logs.

Se debe disponer de planes de contingencia y continuidad debidamente documentados con constancia de la ejecución de las pruebas periódicas.

Se debe realizar periódicamente auditorías detalladas del estado de seguridad de la información de los entornos informáticos relevantes, incluyendo los sistemas del proveedor, las aplicaciones, las instalaciones informáticas, las redes y la actividad de desarrollo de sistemas que soportan los servicios prestados a las Compañías. Estas auditorías deben ser realizadas por un ente

independiente. Si se identifica una vulnerabilidad material que pueda afectar negativamente a la reputación o al servicio suministrado a las Compañías, el proveedor, contratista o tercero debe notificárselo a las Compañías de forma inmediata.

Se debe aplicar procedimiento de monitoreo de logs

Se debe revisar los registros de eventos para detectar posibles incidentes de ciberseguridad o actividades fraudulentas y analizar los eventos detectados para comprender los objetivos y métodos del ataque. Una vez identificados los incidentes materiales y/o las infracciones de los derechos de acceso, se reportarán inmediatamente y se asegurará de seguir el Proceso de gestión de incidentes

Se debe notificar y acordar con las Compañías el alcance de las pruebas, en particular las fechas y horas de inicio y fin para evitar la interrupción o afectación de actividades clave de las Compañías, así como tener en cuenta los eventos generados por los sistemas de seguridad de las Compañías.

Todas las vulnerabilidades de seguridad y ciberseguridad para las cuales el Proveedor, contratista o terceo haya decidido aceptar el riesgo, deben comunicarse y acordarse con las Compañías."

10.14.2.2. Usos no autorizados

Los proveedores, contratista y terceros que presten sus servicios a **las compañías** no están autorizados para utilizar los recursos de información y tecnología de **las compañías** para propósitos diferentes a los necesarios para el cumplimiento del objeto contractual suscrito.

No está autorizada la utilización de equipos informáticos dentro de las redes de comunicaciones de **las compañías** que no cumplan con los controles de seguridad especificados por el sistema de gestión de seguridad de la información de **las compañías**.

No está autorizada la ejecución de cambios sobre la infraestructura de información y comunicaciones de **las compañías** sin contar con la autorización formal y expresa del responsable del área o proceso que utilizan el recurso informático.

No está autorizada la modificación o desactivación de los controles de seguridad instalados en los componentes de información y tecnología de **las compañías** sin contar con autorización del responsable del área o proceso que utilizan el recurso informático.

10.15. TRATAMIENTO DE DATOS PERSONALES

10.15.1. ALCANCE

El lineamiento de protección de datos personales es aplicable a los datos personales registrados en las bases de datos de **las compañías** y se rige por los lineamientos establecidos en la Ley 1581 de 2012 y decreto reglamentario 1377 de 2013.

10.15.2. OBJETIVO

En cumplimiento a lo dispuesto en la Ley 1581 de 2012, reglamentada parcialmente por el Decreto 1377 de 2013 sobre protección de datos personales, **las compañías** establecen la política de tratamiento de datos personales con el propósito de que todas las personas puedan conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en las bases de datos o archivos a cargo de las compañías.

10.15.3. DETALLE

Las compañías en cumplimiento de sus funciones encargadas por la Constitución Política y la ley, de hacer efectivos los derechos, obligaciones, garantías y libertades para lograr la convivencia social, deber realizar la administración y tratamiento de bases de datos con la información de los ciudadanos que realizan cualquier tipo de trámite o política ante **las compañías**, Los datos personales que recolectan y almacenan **las compañías** en sus bases de datos se utilizarán única y exclusivamente para el desarrollo de sus funciones misionales y en tal virtud no requiere la autorización previa del titular para acceder a su información de conformidad con lo dispuesto en el literal a) del artículo 10 de la Ley 1581 de 2012.
Dicha ley está reglamentada en su política interna **GL-M-001 Manual de Política de Protección de datos personales**

1. GESTIÓN DE CAPACITACIÓN Y CONCIENTIZACIÓN

Teniendo en cuenta que el ser humano continúa siendo el elemento que más genera vulnerabilidades en la gestión de seguridad de la información y ciberseguridad, es preponderante lograr un cambio en la mentalidad de nuestros colaboradores, lo cual lograremos a través de la capacitación para:

- Que logren comprender sus responsabilidades con respecto a la seguridad de la información de nuestras compañías.
- Conozcan las políticas, directrices y procedimientos establecidos por las Compañías.
- Conozcan las amenazas a las que nos vemos expuestos como Compañías y personalmente, así como los tipos de ataques que están siendo utilizados por los ciberdelincuentes.

Adicionalmente, es igual o más importante crear en ellos la conciencia sobre la importancia e impacto que tiene la seguridad de la información y ciberseguridad para nuestras Compañías, con el fin de lograr cambiar sus comportamientos y hábitos para que se alineen con los comportamientos que esperamos, y así lograr mantener asegurada nuestra información de las múltiples amenazas que actualmente hay en nuestro entorno.

Para lograr estos objetivos debemos:

1. Identificar los diferentes tipos de audiencias, de acuerdo con el nivel de riesgo que pueden generar para la seguridad de la información.
2. Establecer las necesidades de conocimiento y sensibilización de cada audiencia.

3. Definir los mensajes y contenido a transmitir a cada audiencia.
4. Definir los canales a utilizar para capacitar y sensibilizar a cada audiencia.
5. Estructurar el plan de capacitación y sensibilización.
6. Definir los indicadores para medir la efectividad del plan de capacitación y sensibilización.
7. Anualmente se realizará un simulacro de ciber incidentes (war game) gestionando un incidente en un escenario hipotético de acuerdo con lo establecido en el manual de crisis. Como resultado del simulacro se genera un informe con los resultados obtenidos en la actividad junto con las observaciones /oportunidades de mejora relacionadas con ajustes a procedimientos /guías, datos de contacto, refuerzos específicos, capacitaciones, entre otras, sobre las cuales se hace la respectiva gestión para su solución y/o fortalecimiento para los próximos simulacros

2. CIBERSEGURIDAD

9.16.1 ALCANCE

Los siguientes lineamientos son aplicables a los administradores de plataformas tecnológicas internos y externos, que tengan acceso a información, sistemas de información, centros de cómputo, redes de telecomunicaciones o tecnologías de información y comunicaciones de propiedad de **las compañías** o de sus clientes.

9.16.2 OBJETIVO

Describir los lineamientos de ciberseguridad, para la protección de la información que circula, a través de las redes de las compañías e internet (ciberespacio)

9.16.3 DETALLE

Conforme a la norma ISO 27032:2012 en relación a la Ciberseguridad y con el fin de proteger la información, las aplicaciones, las redes, el internet y la infraestructura en las compañías; mitigar los riesgos del ciberespacio como lo son la exposición de información en las redes y las transacciones comerciales; las amenazas de tipo hacking, Spyware, phishing y ataques de ingeniería social entre otros; a continuación, se detallan los dominios definidos y lineamientos de ciberseguridad, para la protección de las aplicación, servidores, usuario final e ingeniería social, en las compañías:

9.16.3.1 Ciberseguridad a nivel de aplicación.

Periódicamente se deben emitir comunicados asociados a las buenas prácticas para el intercambio de información en línea.

Asegurar que existan mecanismos de seguridad en los aplicativos webs, administrados por las compañías, que contemplen: inicio seguro, autenticación de los servicios WEB, uso correcto de los

subdominios, uso de protocolo seguro HTTPS, secuencias de ordenes en sitios cruzados o Cross-site Scripting. ,

Realizar revisiones y pruebas de códigos de seguridad en aquellas aplicaciones que contengan o comprometan información confidencial y reservada de las Compañía.

Definir los procedimientos de respaldo de los datos, así como los procedimientos de recuperación utilizando elementos que garanticen su integridad y recuperación.

Los desarrollos se realizarán en un entorno de desarrollo y pruebas, con el fin de evitar interrupción en los servicios, fuga, modificación o eliminación accidental de datos. Para las pruebas no se deben usar datos de producción.

9.16.3.2 Ciberseguridad a nivel de servidores.

Realizar revisiones de seguridad identificando la configuración actual de los servidores con base a las guías de aseguramiento, donde se defina claramente la asignación de accesos, credenciales y usuarios; elevación de privilegios, actualización y parches de sistemas operativos, redes, comunicaciones y recursos compartidos, protección (antivirus y firewall) y logs de auditoria.

Asegurar que los sistemas operativos y aplicaciones estén actualizados realizando con frecuencia el despliegue y aplicación de actualizaciones de seguridad.

Realizar evaluaciones y pruebas de seguridad gestionando las vulnerabilidades identificadas mediante los planes de remediación.

Realizar seguimiento de desempeño (capacidad y disponibilidad) de los servidores a través de las herramientas definidas por el proveedor, contratista o tercero del servicio para tal fin.

Ejecutar controles anti software malicioso (como spyware o malware) en los servidores.

Cambiar todas las contraseñas que vienen por defecto del fabricante en los sistemas operativos, los cuales son de conocimiento público, antes del inicio del procesamiento y cambiarlas posteriormente de forma periódica

Los servidores deben estar ubicados en zonas físicamente restringidas, a donde tendrán acceso sólo aquellas personas autorizadas que estrictamente lo requieran para cumplir con sus funciones.

Fortalecer la seguridad de los servidores utilizados para procesar, almacenar o transmitir información de las compañías, incluyendo entre otros, la eliminación de todos los privilegios y servicios que no son esenciales para la ejecución de las operaciones para las que están instalados dichos servidores.

Implementar mecanismos de análisis de la seguridad de los servidores para evaluar e informar periódicamente el estado de cada servidor y verificar que las configuraciones, parámetros y opciones están conformes con las líneas base definidas para ese dispositivo y detectar cambios no autorizados

Mantener activos los logs de auditoría del servidor (Application, Security y System) y almacenarlos por un período mínimo de un (1) año; y revisar por lo menos una vez al año todos los controles de seguridad del servidor acá definidos, para asegurarse que siguen operando

9.16.3.3 Ciberseguridad a nivel de usuarios finales.

Concientizar a los usuarios finales periódicamente mediante la emisión de comunicados, charlas y capacitaciones acerca de las exposiciones, riesgos, buenas prácticas y cuidados en el ciberespacio.

Promover el reporte mediante el Botón de Phishing o a la mesa de ayuda en caso de sospechar o constatar estar afectado.

Para los usuarios de dominio de las compañías, asegurar el uso de sistemas operativos compatibles con los parches de seguridad actualizados.

Asegurar la instalación y aplicación de actualizaciones de parches de los paches de seguridad y del Antivirus, en los usuarios que cuentan con sus equipos corporativos de dominio de las compañías.

Implementar controles de seguridad que eviten el acceso a sitios web maliciosos y/o no autorizados (por ejemplo, listas negras) y monitorear el uso de software permitido para el desarrollo de las actividades laborales.

Configurar políticas de directivas contra correo no deseado, filtro de contenido y Phishing, detección de spam y entrada de correo malware.

9.16.3.4 Ciberseguridad contra ataques de Ingeniería Social.

Este dominio provee el marco de controles para gestionar y minimizar los riesgos con relación a los ataques de ingeniería social:

Publicar y actualizar la política de seguridad y ciberseguridad donde se establecen y adoptan principios por parte de todas las personas con acceso a la información e infraestructura tecnológica de las compañías.

Implementar controles técnicos aplicables como la activación del doble factor de autenticación, uso de tokens de seguridad transaccional.

Monitorear el acceso no autorizado de acuerdo con los niveles de seguridad en la clasificación de los activos de información, para la protección contra exposición accidental, al ciberespacio.

3. SEGUIMIENTO Y CONTROL (MONITOREO)

Este documento debe ser revisado y actualizado al menos cada dos años o cuando se presenten eventos que así lo demanden.

Los responsables de procesos realizan seguimiento y control al cumplimiento de estas políticas.

4. REFERENCIAS

Familia normas ISO 27000:

Estándar	Asunto
ISO/IEC 27000:2009	Vocabulario y Enfoque del SGSI
ISO/IEC 27001:2013	Requerimientos para el SGSI
ISO/IEC 27002:2005	Código de Práctica para la Gestión de SI
ISO/IEC 27003	Guía de Implementación para el SGSI
ISO/IEC 27004	Métricas en la Gestión de SI
ISO/IEC 27005:2008	Gestión del Riesgo en SI
ISO/IEC 27006:2007	Requerimientos para Entidades de Auditoría y Certificación en SGSI
ISO/IEC 27007	Guía de Auditoría para el SGSI
ISO 27031	Guía de continuidad de negocio en cuanto a Tecnologías de la información y comunicaciones.
ISO 27032:2012	Relativa a la ciberseguridad.
ISO 27033	La constituyen 7 partes: 1) Gestión de seguridad de redes 2) Arquitectura de seguridad de redes 3) Escenarios de redes de referencia 4) Aseguramiento de las comunicaciones entre redes mediante gateways 5) Acceso remoto 6) Aseguramiento de comunicaciones en redes mediante VPNs 7) Diseño e implementación de seguridad en redes.
ISO 27034	Guía de seguridad en aplicaciones.
NIST – 800	(National Institute of Standards and Technology) Guías de interés de las series 800 dedicados a seguridad en tecnología de información.
ISACA	Information Systems Audit and Control Association
Ley 1581 del 2012	Por la cual se dictan disipaciones generales para la protección de datos personales

5. TABLA DE VERSIONES Y CAMBIOS

Versión	Fecha	Cambios
1	12/12/2014	Se crea el documento
2	30/05/2018	Se modifica para incluir manejo de claves en SAP, numeral 9.2 Política de asignación de claves y acorde con los cambios en la organización en la Estructura Organizacional.
3	20/09/2019	Se modifica la POLÍTICA DE ASIGNACIÓN DE CLAVES, donde se incluye intentos fallidos específicamente para SAP. Se modifica la POLÍTICA DE ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SOFTWARE, para incluir requerimiento de documentación correspondiente del sistema o módulo.
4	07/10/2021	Se incluye capítulo de Ciberseguridad y actualización en general del documento.

Elaboró	Revisó	Aprobó
DocuSigned by: Angelica Gil C7988A3A10134E1...	DocuSigned by: FF50ED636E8946E...	DocuSigned by: Ana Maria Betancur E8CDF5D2B2874B7...
Angelica Gil Leyton Profesional Seguridad de la Información	**Lourdes Yulieth Ucrós Ospino** Gerente TIC/TOC	**Ana Maria Betancur** Director de Soporte a la Operación
07/10/2021	**07/10/2021**	**07/10/2021**