TELCOS INGENIERÍA S.A.

MANUAL DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN Y GESTIÓN DEL SERVICIO

08 DE SEPTIEMBRE DE 2022

TABLA DE CONTENIDO

1 INTRODUCCIÓN

El presente documento contiene las políticas aplicables a los Sistemas de Gestión de Seguridad de la Información y al Sistema de Gestión del Servicio, con las cuales se pretende orientar el establecimiento de controles y el cumplimiento de requisitos que garanticen la confidencialidad, integridad y disponibilidad de la información, así como también la calidad y mejora de los servicios de TI Internos y Externos ofreciendo valor para los clientes y los usuarios finales.

Las políticas establecidas en este manual se basan en los requisitos de las Normas Técnicas Colombianas NTC-ISO/IEC 27001 de 2013 Sistemas de Gestión de Seguridad de la Información y NTC-ISO/IEC 20000-1 de 2018 Requisitos del Sistema de Gestión del Servicio y las Guías Técnicas Colombianas NTC-ISO/IEC 27002 de 2015 Código de práctica para controles de seguridad de la información y NTC-ISO/IEC 20000-2 de 2017 Orientaciones para la aplicación del sistema de gestión del servicio.

2 OBJETIVOS

- Comunicar la visión, los lineamientos y el compromiso del Presidente y el Director Ejecutivo de la compañía, respecto a la seguridad de la información y la gestión de los servicios de TI.
- Proporcionar un marco directivo para guiar el desarrollo de procedimientos, actividades y acciones adecuados.
- Orientar la aplicación de los controles de seguridad de la Información y gestión del servicio, de acuerdo con el contexto de la compañía, las leyes aplicables y normas adoptadas por los sistemas de gestión.
- Establecer pautas de cumplimiento frente a las responsabilidades de los trabajadores para la Seguridad de la Información y la Gestión de los servicios.

3 ALCANCE

Este manual como parte de los Sistemas de Gestión de Seguridad de la Información y del Servicio, tiene alcance a todos los procesos de Telcos Ingeniería S.A. y aplica a todos los trabajadores de la compañía y a las partes interesadas externas que impacten la seguridad de la información y la Gestión del Servicio.

Otras políticas son consideradas por Telcos Ingeniería S.A, pero no se encuentran dentro de este manual.

4 RESPONSABLES

- **Presidente y Director Ejecutivo**
  - Determinar y asignar los recursos necesarios tanto físicos, técnicos, financieros y humanos para la implementación de las Políticas de Seguridad de la Información y de Gestión del Servicio.
  - Promover las políticas definidas en el presente manual, para aumentar la toma de conciencia, la motivación y la participación de los trabajadores.
  - La aprobación del presente manual de Políticas del Seguridad de la Información estará a cargo del Director Ejecutivo, Presidente o en su defecto a quien designen.

- **Director de Capital intelectual**
  - Validar el cumplimiento de requisitos legales, contractuales e internos asociados a las Políticas de Seguridad de la Información y del Servicio.

- **Director de Tecnologías de la Información y la Comunicación**
  - Dirigir la aplicación de las políticas de Seguridad de la Información y Gestión del Servicio en las actividades desarrolladas por la compañía.
  - Alinear los procedimientos del proceso de Gestión TICS y los requisitos de los servicios de TI internos a los lineamientos establecidos en el presente manual.
  - Realizar o validar los cambios en las Políticas de Seguridad de la Información y de Gestión del Servicio de acuerdo con las necesidades de la compañía o sus partes interesadas.

- Detener una actividad en la que se presente un incumplimiento a cualquiera de las Políticas de Seguridad de la Información.
- Definir los estándares para la aplicación de las directrices establecidas en el presente Manual.

- **Coordinador de Tecnología y Seguridad de la Información y Coordinador de Infraestructura Tecnológica**
  - Solicitar cambios en las Políticas de Seguridad de la Información y de Gestión del Servicio, de acuerdo con las necesidades de la compañía.
  - Llevar a cabo todas las directrices definidas en el presente Manual dentro las actividades desarrolladas, incluyendo los Servicios de TI internos.
  - Velar porque los colaboradores de la compañía y las partes interesadas externas que impacten la seguridad de la información y la Gestión de los servicios, den cumplimiento a las directrices definidas en el presente Manual.
  - Detener una actividad en la que se presente un incumplimiento a cualquiera de las Políticas de Seguridad de la Información.
  - Aplicar los controles pertinentes a tecnología que contribuyen al cumplimiento de las políticas de SI y del servicio, de acuerdo a los procedimientos establecidos.

- **Líder de Seguridad de la Información**
  - Solicitar cambios en las Políticas de Seguridad de la Información y Gestión del Servicio, de acuerdo con las necesidades y las partes interesadas de la compañía.
  - Velar porque los colaboradores y las partes interesadas externas que impacten la seguridad de la información y la Gestión de los servicios, den cumplimiento a las directrices definidas en el presente Manual.
  - Detener una actividad en la que se presente un incumplimiento a cualquiera de las Políticas de Seguridad de la Información.
  - Realizar auditorías internas para constatar el cumplimiento de las políticas definidas en el presente manual.

- **Líderes de proceso**
  - Velar porque los colaboradores y las partes interesadas externas que impacten la seguridad de la información y la Gestión de los servicios, den cumplimiento a las directrices definidas en el presente Manual.

- **Gerente Jurídico Laboral y Líder de Gestión Documental**
  - Velar porque los colaboradores de la compañía y las partes interesadas externas, que impacten la seguridad de la información física, den cumplimiento a las directrices definidas en el presente Manual.
  - Detener una actividad en la que se presente un incumplimiento a cualquiera de las Políticas de Seguridad de la Información.

- **Colaboradores y Partes Interesadas Externas**
  - Dar cumplimiento a todas las Políticas de Seguridad de la Información y de Gestión del Servicio.
  - Reportar cualquier incumplimiento de las Políticas de Seguridad de la Información y de Gestión del servicio, al área de TICS y/o al Líder de Seguridad de la Información.
  - Detener una actividad en la que se presente un incumplimiento a cualquiera de las Políticas de Seguridad de la Información y de Gestión del Servicio.

5 DEFINICIONES Y/O ABREVIATURAS

- **Activo de Información:** Cualquier elemento físico, tecnológico tangible o intangible que genera; almacena o procesa información y que tiene valor para la organización.
- **Confidencialidad**: Propiedad que determina que la información no esté disponible ni sea revelada a individuos, entidades o procesos no autorizados.
- **Criptografía**: Método de protección de la información y las comunicaciones mediante el uso de algoritmos, de modo que solo aquellos a quienes está destinada la información puedan leerla y procesarla.
- **Disponibilidad**: Propiedad de que la información sea accesible y utilizable por solicitud de una entidad autorizada.
- **Evento de seguridad:** Presencia identificada de una condición de un sistema, servicio o red, que indica una posible violación de la política de seguridad de la información o la falla de los controles, o una situación desconocida previamente que puede ser pertinente a la seguridad.
- **Hardware:** es la parte física de cualquier dispositivo electrónico o informático, es usual que sea utilizado en una forma más amplia, generalmente para describir componentes físicos de una tecnología, incluyendo equipos de cómputo, periféricos, redes, cableado y cualquier otro elemento físico involucrado.
- **Integridad:** Propiedad de salvaguardar la exactitud y estado completo de los activos.
- **Incidente de Seguridad de la Información**: Un evento o serie de eventos de seguridad de la información no deseados o inesperados, que tienen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información.
- **Infraestructura Tecnológica:** se entiende por infraestructura tecnológica al conjunto de todos los elementos tecnológicos hardware y software: servidores, computadores, portátiles, impresoras, switches, routers, firewall, escáneres, cableado estructurado, CPU, software informático, sistemas de información, equipos de comunicación, internet, red LAN, entre otros.
- **Propietario de la Información:** Individuo o entidad que tiene responsabilidad aprobada de la dirección por el control de la producción, el desarrollo, el mantenimiento, el uso y la seguridad de los activos. El término “propietario” no implica que la persona tenga realmente los derechos de propiedad de los activos.
- **Registro:** Información documentada conservada que presenta resultados obtenidos y proporciona evidencia de actividades desempeñadas o resultados alcanzados, pueden ser registros internos o externos.
- **Sistema de Gestión de Seguridad de la Información – SIG:** Parte del Sistema Integrado de Gestión, cuyo fin es establecer, implementar, operar, hacer seguimiento, revisar, mantener y mejorar la seguridad de la información.
- **Software:** Se refiere al equipamiento lógico de un computador, está compuesto por todos los aplicativos y licencias que están instalados en cada uno de los equipos de cómputo de la entidad.
- **Seguridad de la información**: La seguridad de la información es el conjunto de medidas preventivas y reactivas de las organizaciones y de los sistemas tecnológicos que permiten resguardar y proteger la información buscando mantener su confidencialidad, la disponibilidad e integridad.
- **Teletrabajo:** Forma de organización laboral, que consiste en el desempeño de actividades remuneradas o prestación de servicios a terceros, utilizando como soporte las tecnologías de la información y comunicación -TIC, para el contacto entre el colaborador y la compañía, sin requerirse la presencia física del colaborador en un sitio específico de trabajo.
- **Trabajo en Casa:** Situación ocasional, temporal y excepcional en la que un colaborador desempeñará sus actividades laborales fuera de los locales habituales de trabajo del trabajador.

6 POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN Y DE GESTIÓN DEL SERVICIO

Versión 4, 08 de septiembre de 2022

TELCOS INGENIERÍA S.A. compañía líder en la prestación de servicios técnicos en construcción, instalación y mantenimiento de redes de telecomunicaciones, para los servicios de televisión, telefonía e internet a nivel nacional, define:

- La gestión del servicio como el conjunto de capacidades y procesos, para dirigir y controlar las actividades y recursos de la compañía, relacionados con la planificación, el diseño, la transición (pruebas), la prestación y la mejora de los servicios de tecnologías de la información -TI internos y externos.
- La seguridad de la información como el conjunto de medidas preventivas y reactivas de la compañía y de los sistemas tecnológicos, que permiten resguardar y proteger la información, buscando mantener su confidencialidad, disponibilidad e integridad.

Para gestionar la aplicación de los anteriores conceptos en la organización se compromete a establecer, implementar, mantener y mejorar continuamente los Sistemas de Gestión del Servicio y de Seguridad de la Información, contribuyendo al logro de los objetivos estratégicos de la compañía y en específico:

- Dar cumplimiento a los requisitos legales, contractuales, internos y de otra índole, para la prestación del servicio y la Seguridad de la Información.
- Mejorar continuamente los Sistemas de Gestión del Servicio y de Seguridad de la Información.
- Proteger la información creada, procesada, transmitida o resguardada en los diferentes procesos, asegurando el cumplimiento de los principios de Confidencialidad, Integridad y Disponibilidad de la información.
- Controlar la operación de sus procesos, garantizando la seguridad de los recursos tecnológicos, infraestructura, redes y bases de datos.
- Asegurar la calidad de los servicios de Tecnologías de la Información, en los procesos internos y en la atención del usuario final, elevando la confianza de nuestros clientes.

Aplica a todos los procesos y partes interesadas que tengan alguna relación con la Seguridad de la Información y la Gestión del Servicio, basados en los siguientes principios:

- Gobierno estratégico para la gestión del servicio y la seguridad de la información.
- Soluciones basadas en la innovación sostenible que impulsen la competitividad, la productividad y la imagen organizacional de la compañía.
- Estrategia basada en la gestión de riesgos, para garantizar la continuidad del negocio.

7 POLÍTICAS ESPECÍFICAS DE SEGURIDAD DE LA INFORMACIÓN Y DE GESTIÓN DEL SERVICIO

7.1 POLÍTICA PARA EL USO DE DISPOSITIVOS MÓVILES Y EL TRABAJO FUERA DE LAS INSTALACIONES

Versión 5, 08 de septiembre de 2022

TELCOS INGENIERÍA S.A., provee las condiciones para la ejecución de actividades laborales que se desarrollen externamente a las sedes de la compañía y se compromete a garantizar la seguridad de la información en el uso de los recursos tecnológicos móviles, que posibilitan el acceso a los activos de información de la compañía fuera de los límites físicos de las sedes de trabajo.

1. USO DE DISPOSITIVOS MÓVILES

TELCOS INGENIERÍA S.A., aplicará procedimientos de control administrativos y técnicos, y exigirá el cumplimiento de los mismos en el uso de dispositivos móviles, con el propósito de proteger los activos de información y mitigar los riesgos de daño, fuga de datos y demás acciones que afecten la seguridad, el cumplimiento de requisitos legales y contractuales, la continuidad del negocio, los datos personales de clientes y usuarios finales y la reputación de la compañía.

1.1. Dispositivos Móviles Corporativos

a) Asignación y registro

El proceso de Gestión TICS, establece las directrices de solicitud y asignación de los equipos de cómputo corporativos, registrando y manteniendo el correspondiente control de inventario.

El área de compras establece las directrices de solicitud y asignación de los teléfonos celulares corporativos de voz y/o datos y de la SIMCARD, registrando y manteniendo el correspondiente control de inventario.

b) Mantenimiento y actualizaciones

El mantenimiento de los equipos de cómputo corporativos estará restringido al área TICS. Se prohíbe el mantenimiento, reparación, cambios en el hardware, instalación de software o modificación de la configuración del equipo sin autorización del área de TICS.

El usuario debe aceptar las actualizaciones del sistema operativo, antivirus y de las aplicaciones.

c) Retiro y transporte

Los equipos que requieran ser retirados de las instalaciones de la compañía, deberán contar con autorización de acuerdo al procedimiento establecido.

El responsable del dispositivo deberá aplicar medidas para protegerlo contra el robo, pérdida y acceso no autorizado.

d) Reporte de novedades

Se debe informar el robo o pérdida de los equipos o dispositivos corporativos, hacer la denuncia ante las autoridades competentes y en el caso de los teléfonos celulares adicionalmente hacer el reporte al operador de servicio móvil.

También se deben informar los daños en los equipos o dispositivos corporativos, anexando evidencias del daño presentado y la descripción de las circunstancias en las que se presentó el hecho.

2. TRABAJO FUERA DE LA INSTALACIONES

TELCOS INGENIERÍA S.A., define los siguientes tipos de trabajo fuera de las instalaciones de la compañía, con el propósito de proporcionar formas alternas de trabajo, que aplican de acuerdo a las necesidades internas o del cliente:

a) Trabajo en terreno
Es el trabajo realizado por el personal operativo del proceso de Gestión Técnica y otros cargos que apoyan actividades en terreno a nivel nacional, orientado al cumplimiento de los servicios de TI externos, de acuerdo con los requisitos contractuales con el cliente.

b) Trabajo en casa
Es el trabajo realizado por los trabajadores que como situación ocasional, temporal y excepcional, por ejemplo, condiciones de salud, desempeñarán sus funciones laborales por fuera de las sedes de la compañía, ya sea desde su lugar de residencia o cualquier otro similar.

c) Teletrabajo
Es el desempeño de actividades laborales permanentes y remuneradas o prestación de servicios, utilizando como soporte las tecnologías de la información y comunicación -TIC, para el contacto entre el trabajador y la compañía, sin requerirse la presencia física del colaborador en un sitio específico de trabajo.

d) Labores temporales
Es el trabajo ocasional que se realiza como parte de sus funciones laborales y que requiere desplazamiento o presencia en lugares diferentes a su sitio habitual de trabajo asignado, como son las comisiones, auditorias, visitas etc.

2.1. Condiciones y Restricciones

a) Uso de los dispositivos móviles para trabajo fuera de las instalaciones
Los trabajadores y/o usuarios deben aceptar y cumplir las condiciones establecidas por la compañía para el uso de los dispositivos móviles corporativos, que se usen para el desarrollo de funciones laborales fuera de las instalaciones.

Los usuarios deben aceptar las actualizaciones del sistema operativo, antivirus y de las aplicaciones, de acuerdo a los lineamientos del área de TICS.

b) Seguridad de la información
Los líderes de proceso definirán el alcance de las actividades a desarrollar, estableciendo como mínimo, el horario, los activos de información a acceder, los sistemas de información y los servicios requeridos para el desarrollo de las actividades.

Los trabajadores que realicen actividades fuera de las instalaciones de la compañía, deben aplicar todas las directrices definidas en el presente manual, controlando los riesgos relacionados con la Seguridad de la Información.

c) Conexión a redes de comunicación
Los trabajadores que ejecutan actividades en terreno y les fue asignada una SIM CARD de la compañía, deberán usar esta línea corporativa como la única red de comunicación (voz y datos), para realizar las funciones propias de su cargo.

Ningún trabajador deberá usar redes wifi públicas o desconocidas para conectar el dispositivo móvil con el que realiza actividades laborales, ya que este tipo de redes se consideran inseguras y con alta probabilidad de causar incidentes en la información que se procesa, almacena y transmite desde los dispositivos.

d) Acceso a sistemas, aplicaciones y servicios
Los canales de acceso a sistemas, aplicaciones y servicios se deben solicitar y ser gestionados de acuerdo a los procedimientos establecidos y con la autorización respectiva del área de TICS.

El área de TICS establecerá las respectivas configuraciones técnicas y de seguridad a los dispositivos y canales de acceso de acuerdo a la necesidad, el cargo, el nivel de autorización y demás factores aplicables.

El usuario no deberá ingresar a los recursos de la compañía usando dispositivos públicos, ajenos a su propiedad o a la propiedad de la organización.

e) Almacenamiento de la información
La información corporativa que no sea estrictamente necesaria para el desarrollo de las actividades laborales del usuario no debe almacenarse en el dispositivo.

La información se debe mantener almacenada en los repositorios establecidos por la compañía.

f) Tratamiento de la información confidencial
En caso de ser necesario el almacenamiento de información confidencial en los dispositivos móviles que se usen para trabajo fuera de las instalaciones de la compañía, la respectiva información debe cifrarse y permanecer cifrada mientras se encuentre almacenada en esos dispositivos, una vez terminada la labor que conllevó al almacenamiento y/o uso de la información confidencial, se deberá transferir a los medios de almacenamiento corporativos establecidos y debe ser retirada de forma segura de los dispositivos móviles de acuerdo a los procedimientos definidos.

7.2 POLÍTICA DE CLASIFICACIÓN Y ETIQUETADO DE LA INFORMACIÓN

Versión 5, 08 de septiembre de 2022

La información es uno de los activos principales en TELCOS INGENIERÍA S.A. por ello nos comprometemos a clasificar y etiquetar los activos de información, para garantizar su seguridad con criterios de Confidencialidad, Integridad y Disponibilidad. El Sistema de Gestión de Seguridad de la Información y del Servicio establecerá los procedimientos y requisitos para la clasificación y etiquetado de los activos de información de acuerdo a los requerimientos legales, contractuales, internos y de otra índole.

Los lideres de proceso serán responsables de cumplir en su proceso los procedimientos de clasificación y etiquetado de sus activos de información.

1. ACTIVOS DE INFORMACIÓN

Se definen como activos de información a los datos, metadatos, soportes documentales y otros elementos asociados donde se produce, transforma, intercambia y almacena información de distintas clases, así como el capital humano, los servicios y otros intangibles que en general se consideran críticos para el negocio y que serán objeto de control para garantizar la Confidencialidad, Integridad y Disponibilidad de la información.

Los activos de información de la compañía se identificarán, se registrarán adecuadamente en un inventario y se les asignará un propietario quien será el responsable por su uso y protección. Todos los procesos y cargos son responsables de identificar y salvaguardar los activos de información asignados y/o utilizados, apoyados en el Sistema de Gestión de Seguridad de la Información y del Servicio.

2. CATEGORÍAS DE CLASIFICACIÓN

a) Confidencial: Información que solo puede ser conocida y utilizada por los trabajadores autorizados, cuya divulgación y/o uso no autorizado se encuentra prohibido, dado que podría ocasionar pérdidas significativas para la organización.

b) Interna: Información que puede ser conocida y utilizada por todos los trabajadores de la organización y algunas partes interesadas externas debidamente autorizadas, y cuya divulgación o uso no autorizados podrían ocasionar riesgos o pérdidas leves para la organización.

c) Pública: Información que puede ser conocida y utilizada sin autorización por cualquier persona, sea trabajador de la organización o no, y cuya divulgación no genera riesgos para la compañía.

3. CRITERIOS DE CLASIFICACIÓN

El Sistema de Gestión de Seguridad de la Información y del Servicio establecerá el procedimiento para la clasificación de los activos de información, para lo cual además de lo definido en las categorías de clasificación, debe tener en cuenta:

- La protección de los datos personales, de acuerdo a lo establecido en los requisitos legales aplicables.
- Las reglas y principios generales que regulan la función archivística del Estado, como guía de trabajo para la Gestión Documental de la compañía.
- La clasificación de la información proveniente de las partes interesadas externas, la cual se tratará conforme a las políticas de la organización y de la parte interesada.

4. MÉTODOS DE ETIQUETADO

El Sistema de Gestión de Seguridad de la Información y del Servicio establecerá el procedimiento para el etiquetado de los activos de información.

5. VALORACIÓN DE LA CRITICIDAD

El Sistema de Gestión de Seguridad de la Información y del Servicio establecerá el procedimiento para la valoración de la criticidad de los activos de información, teniendo en cuenta los principios de Confidencialidad, Integridad y Disponibilidad.

6. TRATAMIENTO DE SEGURIDAD

Los activos de información son tratados de acuerdo con la categoría de clasificación y valoración de la criticidad.

Los usuarios que tienen asignados activos de información serán responsables de la protección de la información contenida en ellos.

La clasificación y etiquetado de la información es parte de los acuerdos contractuales con los proveedores de servicios, en especial en el intercambio de “información sensible”, de acuerdo con lo establecido en la normatividad aplicable.

7. MANEJO DE ACTIVOS

a) Gestión documental

La gestión documental se define como el conjunto de actividades administrativas y técnicas tendientes a la planificación, manejo, organización y control de los soportes documentales físicos producidos y recibidos por la compañía, desde su origen hasta su disposición final, con el objeto de facilitar su utilización y conservación.

Esta actividad estará liderada por el área de Gestión Documental, quien establecerá los respectivos procedimientos y requisitos para controlar el ciclo de vida de los soportes documentales desde su creación hasta su disposición final.

b) Gestión TICS

Conjunto de actividades administrativas y técnicas tendientes a la planificación, manejo, organización y control de los activos tecnológicos de información y redes, asociados a la creación, almacenamiento, gestión y tratamiento de información.

El proceso de Gestión TICS establece los respectivos procedimientos y requisitos para controlar y gestionar los activos tecnológicos propios, apoya y asesora a los demás procesos de la compañía que usen sistemas, servicios y aplicaciones de terceros, ya sean contratados, públicos, *open source,* entre otros y se encarga de gestionar las condiciones técnicas y de acceso a las plataformas, aplicaciones y servicios que el cliente provee para el desarrollo del objeto contractual.

8. DISPOSICIÓN FINAL

Las áreas de Gestión Documental y TICS, establece los procedimientos de disposición final de los activos propios, de acuerdo a los requisitos legales, ambientales, contractuales con el cliente e internos.

7.3 POLÍTICA DE ESCRITORIO LIMPIO Y PANTALLA LIMPIA

Versión 4, 08 de septiembre de 2022

TELCOS INGENIERÍA S.A., garantiza que los trabajadores y partes interesadas externas, que tengan acceso a las instalaciones físicas de la empresa, sistemas de información y/o equipos de cómputo, cumplan las directrices en materia de seguridad de la información, para todos los activos de información a los que tengan acceso.

El Sistema de Gestión de Seguridad de la Información y del Servicio establece los procedimientos y requisitos para la protección de la información gestionada en los puestos y computadores de trabajo.

1. ESCRITORIO LIMPIO

La información gestionada en papel u otros medios físicos presenta riesgos no tecnológicos, como la exposición visual, el peligro de robo o extravío, el daño físico, entre otros, debido principalmente al acceso de terceras personas a las zonas de trabajo, por lo tanto, se deben aplicar los siguientes lineamientos para mitigar los riesgos asociados.

- Se debe guardar la documentación de trabajo en sitios seguros, al ausentarse del puesto de trabajo y al terminar la jornada laboral.
- En ningún momento se debe dejar información confidencial a la vista de personas que pudieran hacer un uso indebido de la misma.
- Los proveedores y demás partes interesadas externas que tengan acceso a las instalaciones físicas de la compañía, sistemas de información y equipos de cómputo, deben cumplir todas las políticas de seguridad de la información y además garantizar que en sus escritorios o áreas de trabajo no se pone en riesgo la confidencialidad, integridad o disponibilidad de la información.
- Los dispositivos de almacenamiento autorizados se deben guardar en sitios seguros, después de la jornada laboral o cuando no estén siendo utilizados.
- No apuntar credenciales de acceso a sistemas de información, como usuarios y contraseñas, en lugares visibles o con acceso al público en general.
- Los soportes documentales en papel u otros medios que ya no se usen, se deben disponer adecuadamente.

2. PANTALLA LIMPIA

Los equipos de cómputo asignados o usados para la gestión de información e ingreso a los recursos tecnológicos, también se enfrentan a riesgos como accesos no autorizados al equipo y desde este a los sistemas y aplicaciones de la compañía, infecciones por malware, robo y fuga de datos electrónicos, ataques de ingeniería social, etc., por lo tanto, se deben aplicar los siguientes lineamientos para mitigar los riesgos asociados, en especial cuando el equipo esta desatendido:

- No se permite tener accesos directos en el escritorio del computador.
- El usuario debe bloquear sesión cuando se ausente de su puesto de trabajo o deje el equipo desatendido, para proteger el acceso a la documentación digital, aplicaciones y servicios de la compañía.
- El área de TICS programará un bloqueo automático de sesión en los equipos y aplicativos al no detectarse actividad del usuario en un tiempo determinado.
- Los usuarios deben apagar su equipo de cómputo una vez terminada la jornada laboral.
- Una vez termine la labor o actividad en las aplicaciones, herramientas de software o sistemas de información, se debe cerrar la sesión de usuario, evitando posibles suplantaciones y accesos no autorizados.

3. OTRAS ÁREAS DE TRABAJO LIMPIAS

Además de los puestos de trabajo, se debe tener en cuenta la protección de la información en áreas comunes donde se ubican los equipos de impresión, salas de reunión, etc., incluyendo comunicaciones verbales o telefónicas, para ello se deben cumplir las siguientes directrices:

- Se debe retirar de las impresoras, escáneres y fax, toda documentación física, evitando de esta manera la exposición de la información a personal no autorizado, en el caso de la información confidencial debe ser retirada inmediatamente se utiliza el activo.
- No revelar información a usuarios desconocidos, que pueden intentar obtener contraseñas de usuario, información de cuentas bancarias o cualquier otra información confidencial de la compañía, engañando a trabajadores o a partes interesadas externas, a través de conversaciones, llamadas telefónicas, correos electrónicos, redes sociales o mensajes tipo SMS o Whatsapp.
- Durante los tiempos de inactividad en reuniones virtuales se debe cerrar el micrófono o desconectarse de la reunión, para prevenir divulgación accidental de información confidencial.

7.4 POLÍTICA DE COPIAS DE RESPALDO DE INFORMACIÓN

Versión 5, 08 de septiembre de 2022

TELCOS INGENIERÍA S.A garantiza que la información que la organización y/o el responsable de la misma determine que debe ser protegida, es respaldada mediante copias de seguridad, y que las mismas son sometidas a pruebas de restauración que verifican su grado de integridad.

El Sistema de Gestión de Seguridad de la información y del Servicio establece un plan de restauración de copias de seguridad, que son probadas a intervalos regulares, con el fin de asegurar que son confiables en caso de emergencia y retenidas por un tiempo determinado.

Es responsabilidad de los usuarios almacenar la información laboral, únicamente en los sitios asignados por el área de TICS, para garantizar su copia de respaldo. Adicionalmente deben atender las instrucciones del área de TICS, para la correcta ejecución de las copias de respaldo en los tiempos estipulados.

El área de TICS garantizará la generación y almacenamiento de las copias de respaldo de la información en un sitio alterno.

Para asegurar los principios de Confidencialidad, Integridad y Disponibilidad de la información, el área de TICS NO se hace responsable de respaldar información que no sea de la compañía, por lo anterior todo trabajador o parte interesada externa debe abstenerse de almacenar información personal en los equipos de la empresa.

TELCOS INGENIERÍA S.A. no se hace responsable de salvaguardar información laboral almacenada en medios no autorizados, ni aplicaciones no corporativas.

7.5 POLÍTICA DE TRANSFERENCIA DE INFORMACIÓN

Versión 6, 08 de septiembre de 2022

TELCOS INGENIERÍA S.A., permite el uso de diversos medios de transferencia de información, dado que es imprescindible para el funcionamiento de la compañía; y se compromete a garantizar la seguridad de la información en la transferencia de información y a controlar el uso de los medios de transferencia para reducir el riesgo de incidentes con implicaciones legales, contractuales y reputacionales, para ello establece las siguientes directrices:

1. INTERCAMBIO DE INFORMACIÓN

Todos los colaboradores de la compañía son responsables de aplicar los controles para proteger la información transmitida a partes interesadas, mediante el correcto uso de los diferentes medios de intercambio autorizados.

El Sistema de Gestión de Seguridad de la Información y del Servicio establece los controles administrativos y técnicos necesarios para mitigar los riesgos asociados a la transferencia de información.

Los propietarios, responsables o custodios de la información, son los encargados de aplicar los controles que garantizan el cumplimento de los criterios de Confidencialidad, Integridad y Disponibilidad, según corresponda a cada medio de transferencia de información.

2. MÉTODOS DE TRANSFERENCIA DE INFORMACIÓN

TELCOS INGENIERÍA S.A., ha dispuesto los siguientes métodos de transferencia de información, los cuales se deberán usar adecuadamente siguiendo los lineamientos y buenas prácticas expuestos a continuación:

a) **Uso de mensajería instantánea:** El uso de la plataforma WhatsApp está permitido bajo autorización individual por parte del Líder del proceso. El acceso a dicha plataforma se hace solo a través de la aplicación o página oficial.
b) **Plataformas web de terceros**: Las plataformas de terceros se validan por el área de TICS, para que cuenten con protocolos de transferencia de información seguros (Https, VPN). Cuando la transferencia es a través de plataformas web de terceros, el usuario solo la debe usar si la página es segura.
c) **Protección de información verbal:** Los trabajadores de Telcos Ingeniería no deben tener conversaciones que puedan revelar información confidencial de la compañía en lugares públicos, o mediante canales de comunicación no seguros, como oficinas abiertas y salas de reunión.
d) **Uso de dispositivos USB y medios extraíbles:** Los puertos USB se encuentran bloqueados contra escritura y lectura, y únicamente se habilitarán con la autorización respectiva de acuerdo a los procedimientos establecidos. Los medios extraíbles y los dispositivos USB autorizados deben tener un tipo de encriptación, o la información contenida debe ir cifrada, con el fin de protegerla contra accesos no autorizados o fugas de información en su transporte.

3. USO DEL CORREO ELECTRÓNICO

El uso de las cuentas y el contenido de los mensajes de correo electrónico deberá cumplir con las políticas y procedimientos definidos el Sistema de Gestión de Seguridad de la Información y del Servicio y con las siguientes directrices:

- **Antimalware y antispam:** Implementar controles antimalware y filtros antispam, para que los correos maliciosos sean identificados y no lleguen al usuario final.

- **Direcciones de correo electrónico en páginas web:** No se deben publicar las direcciones de correo corporativas en páginas web, incluyendo redes sociales, en formato texto, de requerirse utilice imágenes.

- **Uso apropiado del correo corporativo:** No se debe usar el correo corporativo para fines diferentes al objeto del contrato laboral.
- **Contraseña segura:** Todas las cuentas de correo deben utilizar contraseñas de acceso de acuerdo a las directrices del Sistema de Seguridad de la Información y del Servicio.
- **Correos sospechosos:** Los trabajadores al identificar correos fraudulentos o sospechosos, deben abstenerse de abrirlos y reportarlo inmediatamente al área de TICS.
- **No responder al spam (correo basura):** Cuando reciba correo no deseado no responda ni reenvíe dicho mensaje.
- **Utilizar la copia oculta (BCC o CCO):** Los trabajadores que tengan autorización para el envío de correos masivos deben agregar los destinatarios en Copia Oculta (BCC o CCO).

4. PROTECCIÓN CONTRA CÓDIGOS MALICIOSOS

La aparición constante de nuevos **virus** y otros tipos de **código malicioso** son una de las principales **amenazas** a las que se enfrenta la información de la compañía, por lo tanto, se definen los siguientes lineamientos con el objetivo de prevenir, detectar, controlar y eliminar la ejecución de cualquier software malicioso en los sistemas de cómputo.

El sistema de gestión de seguridad de la información y del servicio determina las soluciones más convenientes para la compañía, considerando el tipo de aplicación, la clasificación de la información a proteger y la infraestructura existente.

a) Configuración de las herramientas de detección de código malicioso

Las herramientas de detección de códigos maliciosos implementadas en la compañía deben:

- Realizar análisis automáticos y periódicos.
- Realizar comprobaciones automáticas de los ficheros adjuntos al correo y de las descargas web.
- Bloquear el acceso a aplicaciones o sitios web que distribuyan código malicioso.
- Permitir el acceso a aplicaciones o sitios web basándonos en metodología de listas blancas
- Las actualizaciones de la base de datos de firmas de detección de códigos maliciosos deben ser en lo posible automáticas.

b) Buenas prácticas para el control de código malicioso

Con el fin de reforzar las medidas técnicas establecidas para el control de código malicioso, los usuarios deben aplicar las siguientes directrices:

- Se prohíbe alterar la configuración de seguridad establecida para los sistemas y equipos de tratamiento de información.
- Debe utilizarse únicamente el software permitido por la organización.
- Seguir las instrucciones difundidas por el Sistema de Gestión de Seguridad de la Información y del Servicio relacionadas a la prevención de amenazas por código malicioso.

5. PÁGINAS WEB

TELCOS INGENIERÍA S.A., hace presencia en internet mediante la publicación de aplicativos, lo cual permite ofrecer servicios, facilitar la operación, posibilitar la comunicación entre los usuarios de la compañía y como consecuencia se aumenta la exposición a ataques por código malicioso, con el propósito de prevenir este riesgo se establecen las siguientes directrices:

- Utilizar metodologías de desarrollo seguro.
- Aplicación de los controles adecuados para el acceso al panel de administración del sitio web.
- Realizar copias de seguridad periódicas de todos los elementos que conforman el servicio web.
- Mantener las aplicaciones web actualizadas.
- Generar y guardar registros de la actividad del servidor.
- Disponer de un certificado digital que garantice la seguridad del sitio web.

7.6 POLÍTICA DE DESARROLLO SEGURO

Versión 5, 08 de septiembre de 2022

TELCOS INGENIERÍA S.A. garantiza que el desarrollo de software y sistemas dentro de la organización cumplen con los requerimientos de seguridad establecidos, con las buenas prácticas para el desarrollo seguro de aplicativos, así como con las metodologías para la realización de pruebas de aceptación y seguridad al software desarrollado.

Para garantizar que en el proceso de desarrollo de software se proteja la seguridad de la información, el área de TICS establece las siguientes directrices que deben ser cumplidas por los desarrolladores de software:

- Los equipos usados para el desarrollo de software cumplen con todos los controles de acceso a redes y aplicaciones.
- Los equipos usados para desarrollo están conectados a un entorno de red diferente al de producción. Así mismo los ambientes de pruebas y producción deben estar separados.
- El desarrollador se abstiene de usar contraseñas o claves en texto plano dentro del código.
- Los datos de prueba no deben contener información confidencial.
- Las credenciales de acceso a sistemas de información usadas durante el desarrollo, no son usadas en producción.
- Toda modificación o cambio en el software desarrollado, deberá ser analizado y probado en ambientes de pruebas y autorizado por el personal correspondiente en TELCOS INGENIERÍA S.A., con el fin de identificar, analizar y evaluar los posibles riesgos de seguridad de la información que puedan presentarse por dichos cambios.
- Garantizar que no se divulgue información confidencial en respuestas de error, incluyendo detalles del sistema, identificadores de sesión o información de las cuentas de usuarios en entorno de producción. Para dicho entorno implementar mensajes de error genéricos.

7.7 POLÍTICA DE CONTROL DE ACCESO

Versión 5, 08 de septiembre de 2022

TELCOS INGENIERÍA S.A., provee las condiciones para el desarrollo de las funciones laborales, entre las que se incluye la disponibilidad de instalaciones, equipos, redes de comunicaciones, sistemas, aplicaciones y servicios de tecnologías de información propios y de terceros, y se compromete a garantizar la seguridad de la información en el acceso y uso de esos recursos que posibilitan la gestión de la información de la compañía, para ello establece las siguientes directrices:

1. RESTRICCIONES DE ACCESO

Todos los accesos, tanto físicos como informáticos, están restringidos y controlados mediante mecanismos adecuados que garantizan la seguridad de instalaciones y activos de información.

Se debe aplicar el principio del mínimo privilegio, en el acceso de las partes interesadas a los activos de información aprobados.

Los responsables de la seguridad física y seguridad de la información establecen procedimientos para la asignación, modificación, actualización y retiro de los accesos respectivos de acuerdo a las necesidades, el cargo, las funciones, entre otros, con la respectiva autorización según sea el caso.

Las áreas de seguridad física y de TICs implementan, monitorean y mejoran continuamente los procedimientos, métodos y controles de acceso.

2. MÉTODOS DE CONTROL DE ACCESO

a) Controles de acceso físico

Los Directores Técnicos a nivel nacional y el proceso de Gestión Jurídica en la ciudad de Bogotá, llevan a cabo controles de acceso y salida en las instalaciones, para personal, activos y vehículos.

b) Controles de acceso informático

El proceso de Gestión TICS identifica y establece los controles de acceso para cada recurso informático, asegurando que cuenten con las características necesarias para proteger la confidencialidad, disponibilidad e integridad de la información.

3. MÉTODOS DE IDENTIFICACIÓN

TELCOS INGENIERÍA establece que los métodos de identificación se basan en la utilización de uno, o varios, de los siguientes factores:

- Nombre de usuario
- Documento de identificación
- Reconocimiento biométrico.

4. MÉTODOS DE AUTENTICACIÓN SECRETA

TELCOS INGENIERÍA establece que los requisitos de autenticación de usuarios se basan en la utilización de uno, o varios, de los siguientes factores:

- Contraseñas.
- Reconocimiento biométrico.
- Tokens.

5. REQUISITOS MÍNIMOS PARA LA CREACIÓN DE CONTRASEÑAS

Los sistemas autenticados por contraseña deben cumplir como mínimo con los siguientes requisitos:

- Debe solicitar al usuario el cambio de contraseña en un intervalo de máximo tres meses.
- Debe verificar la calidad de la contraseña, al no permitir el nombre de usuario o el nombre propio como parte de la misma.
- Crear contraseñas con un alto nivel de complejidad que incluyan:
  - Combinar mayúsculas con minúsculas
  - Incluir números
  - Incluir caracteres especiales como: ()=/&%$!”#+*- entre otros.
  - La contraseña debe tener una longitud mínima de 8 caracteres.

Los usuarios serán responsables de custodiar las contraseñas y demás métodos de autenticación que les hayan sido asignados, aplicando los siguientes lineamientos:

- Las credenciales de usuario y contraseña son de uso personal e intransferible, no deben ser compartidas, ni divulgadas a otros trabajadores o personas externas.
- Las contraseñas deben ser memorizadas, no se deben escribir.
- No usar la función de almacenamiento y llenado automático de contraseñas de los navegadores.

6. CONTROL DE ACCESO A REDES DE COMUNICACIONES

- El proceso de Gestión TICS brindará acceso a las redes corporativas, solamente con autorización de los líderes de proceso de la compañía.
- El acceso a la redes inalámbricas o servicio WIFI es concedido de forma individual, con la aprobación de líderes de proceso y las credenciales de acceso no se deben compartir.
- La conexión de dispositivos no corporativos a la red, sin la previa autorización del Líder de proceso está prohibida.
- La configuración de red asignada por el área de TICS no se debe modificar por el usuario.
- El traslado de equipos de escritorio conectados a la red alambrada debe ser coordinado con el área de TICS, para garantizar su correcto funcionamiento.

7.8 POLÍTICA DE ALMACENAMIENTO Y PROTECCIÓN DE REGISTROS

Versión 1, 08 de septiembre de 2022

Todos los empleados y demás Partes Interesadas de TELCOS INGENIERÍA deben almacenar los registros en los sitios aprobados por el Sistema de Gestión de Seguridad de la Información y del Servicio, los cuales cuentan con los requisitos para garantizar la confidencialidad, integridad y disponibilidad de la información:

1. SITIOS DE ALMACENAMIENTO

- **Almacenamiento local de los equipos:** TELCOS INGENIERÍA prohíbe el almacenamiento local de registros de forma permanente, ya sea en los discos duros de los equipos de cómputo o en los espacios de almacenamiento de los teléfonos inteligentes.
- **Almacenamiento en dispositivos móviles o extraíbles**: Se autoriza el almacenamiento transitorio más no permanente en dispositivos móviles o extraíbles, los cuales deben contar con autorización de acuerdo al procedimiento establecido, en todas las circunstancias la información y/o el dispositivo deben tener un tipo de encriptación, o la información contenida debe ir cifrada, con el fin de protegerla contra accesos no autorizados o fugas de información en su transporte.
- **Nubes públicas:** TELCOS Ingeniería prohíbe el almacenamiento de cualquier tipo de información corporativa en nubes de almacenamiento públicas como Dropbox, Drive, etc. **Excepción:** Se exceptúa de esta prohibición los usuarios con cuenta corporativa de la suite Office 365, quienes están autorizados a almacenar información o registros no confidenciales en OneDrive.
- **Nube privada corporativa ALFRESCO:** TELCOS INGENIERÍA ha establecido el sistema corporativo de nube, para el almacenamiento formal de registros finales de los procesos de la empresa que lo requieran.
- **Carpetas compartidas:** TELCOS INGENIERÍA ha establecido el sistema de carpetas compartidas, en las cuales los procesos de la empresa pueden guardar todo tipo de documentos que hacen parte de su gestión y que pueden o no ser compartidos con otros colaboradores.

2. PROTECCIÓN DE REGISTROS

Los sitios de almacenamiento aprobados por el Sistema de Gestión de Seguridad de la Información y del Servicio cuentan con controles de acceso adecuados para garantizar la confidencialidad de la información y son protegidos siguiendo los lineamientos de la Política de Copias de Respaldo de la Información.

7.9 POLÍTICA DE ÁREAS SEGURAS

Versión 5, 08 de septiembre de 2022

TELCOS INGENIERÍA S.A. garantiza que todo colaborador y parte interesada, que necesite utilizar las instalaciones físicas, realice su ingreso y salida cumpliendo con las medidas de seguridad física y digital establecidas por la organización.

1. ÁREAS SEGURAS

Se define el Centro de Datos y al área de Gestión Documental como áreas seguras y su acceso está restringido por un lector biométrico.

2. CONTROLES DE LAS ÁREAS SEGURAS

- El personal autorizado para ingresar al Centro de Datos es definido por el Presidente, Director Ejecutivo y/o el Coordinador de Tecnología y Seguridad de la Información.
- El personal autorizado para ingresar al área de Gestión Documental es definido por el Presidente, Director Ejecutivo, Apoderado General y/o el Líder de Gestión Documental.
- El personal autorizado registra el ingreso al área segura correspondiente, en el lector biométrico ubicado a su entrada. En caso de que este lector biométrico no pueda ser utilizado por daño, no disponibilidad o restricción asociada al cumplimiento de normas sanitarias, se determinará otro sistema de acceso previamente aprobado por el Presidente y/o la Dirección Ejecutiva y en su defecto se diligenciará el formato de control de ingreso y salida áreas seguras.
- Todo personal ajeno, interno o externo, que requiera ejecutar labores dentro del área segura deberá solicitar autorización y diligenciar el formato de control de ingreso y salida áreas seguras.
- Absténgase de dejar descuidados y/o desatendidos los equipos de cómputo o elementos que estén bajo su custodia. Tanto en las instalaciones de la compañía como en las del usuario final.

3. TÉRMINO DE LABORES EN LAS ÁREAS SEGURAS

Al dejar su área de trabajo o al final del día:

- Apague su estación de trabajo.
- Cierre su oficina o áreas bajo su custodia con llave, si trabaja en una oficina cerrada llévese la llave.
- Asegure los cajones que contengan información o recursos informáticos asignados a su cargo.
- No deje elementos que contengan información confidencial sobre los puestos de trabajo, tales como tokens o elementos de acceso físico, dispositivos móviles, carpetas o documentos.

4. PROHIBICIONES Y RESTRICCIONES EN LAS ÁREAS SEGURAS

Absténgase de realizar acciones riesgosas o inadecuadas, tanto para su seguridad física como para la del elemento y la información contenida en él. Entre estas acciones riesgosas se encuentran, pero no se limitan a:

- Trasladar o mover los equipos en condiciones no seguras, exponiéndolos a daño o hurto.
- Continuar utilizando el equipo de cómputo, portátil, dispositivo móvil, tableta o cualquier otro elemento electrónico, cuando se detecte o sospeche que el mismo se encuentre infectado por un virus.
- Golpear, manipular o utilizar de forma inadecuada los equipos informáticos y de servicio tecnológico. En caso de algún problema físico con los elementos tecnológicos solicitar al área de TICs su ayuda.

- Realizar conexiones eléctricas no adecuadas o usar redes o dispositivos con protección eléctrica para uso de aparatos como brilladoras, secadoras, ventiladores, calentadores entre otros, consulte previamente al personal del área de TICs.

5. PROHIBICIONES Y RESTRICCIONES EN LA VIVIENDA DEL USUARIO FINAL

Durante la prestación de servicios de TI externos el personal que tenga acceso a la vivienda del usuario final, se debe abstener de realizar las siguientes actividades:

- Manipular directamente los computadores portátiles, de escritorio y celulares del usuario sin previa autorización. En todos los casos el usuario debe prender el equipo e introducir la contraseña de inicio.
- No solicitar el retiro de elementos de valor, cuando los identifique a la vista en el lugar donde se ejecutará el servicio.
- Quedarse sin acompañamiento de un mayor de edad al interior de la vivienda. En caso de que este se retire informarle que no puede continuar la labor sin su supervisión.

7.10 POLÍTICA DE USO DE CONTROLES CRIPTOGRÁFICOS

Versión 5, 08 de septiembre de 2022

TELCOS INGENIERÍA S.A., entendiendo que la información sensible y confidencial por su trascendencia para nuestro negocio debe estar especialmente protegida tanto en tránsito como cuando está almacenada, se compromete al uso adecuado y eficaz de las técnicas criptográficas para asegurar la confidencialidad e integridad.

1. INFORMACIÓN QUE DEBE SER CIFRADA

La clasificación de la información será la base para determinar qué información debe ser cifrada, garantizando su confidencialidad e integridad, algunos ejemplos son:

- Información sensible, de carácter personal o confidencial.
- Registros con credenciales de autenticación.
- Información almacenada en dispositivos móviles.
- Información transferida a través de redes de comunicaciones externas.
- Información confidencial enviada a través de correo electrónico a partes interesadas externas.
- Información transferida en memorias USB o discos duros.

2. TÉCNICAS CRIPTOGRÁFICAS

a) Uso de firma electrónica

Se usarán firmas electrónicas en procesos financieros y cualquier otro aprobado por la compañía que requiera garantizar la autenticidad de la información. El destinatario de la información determina las características técnicas de la firma electrónica.

b) Certificados web

Para garantizar la seguridad de la información en nuestro sitio web, se usarán certificados web (SSL/TLS).

c) Cifrado de datos sensibles en la transferencia de información

La transferencia de datos confidenciales o sensibles a entidades o personas externas se debe hacer cifrando los datos antes de transferirlos.

d) Cifrado en desarrollo de aplicaciones

En los sistemas de control de acceso de las aplicaciones, se debe almacenar la contraseña de forma cifrada.

e) Acceso desde el exterior con VPN

Se establecen y habilitan canales VPN cifrados que garanticen la confidencialidad e integridad de las comunicaciones.

3. ASIGNACIÓN DE CONTROLES CRIPTOGRÁFICOS

TELCOS INGENIERÍA, provee herramientas y protocolos de cifrado para almacenar y trasmitir información, de acuerdo a las necesidades internas o de las partes interesadas externas.

Las claves criptográficas suministradas por el cliente o por terceros y asignadas a un cargo o colaborador en específico para el cumplimiento de funciones propias, lo hace responsable por su custodia y conservación bajo los principios de disponibilidad, integridad y confidencialidad.

4. USO DE PROTOCOLOS SEGUROS EN REDES INALÁMBRICAS

Las redes WLAN (*wifi*) de la compañía se configuran con el estándar WPA2.

7.11 POLÍTICA PARA LAS RELACIONES CON LOS PROVEEDORES

Versión 3, 04 de diciembre de 2020

Los proveedores de TELCOS INGENIERÍA S.A., que tengan cualquier tipo de acceso a los activos de información son responsables de protegerlos, conservarlos y utilizarlos solo para los fines autorizados. Los activos de información de la compañía incluyen elementos tangibles, como equipos, información digital e impresa, sistemas informáticos y de comunicación, así como también elementos intangibles, como el buen nombre y la reputación de la compañía.

Los proveedores que tengan acceso a la información de TELCOS INGENIERÍA S.A, incluyendo aquellos que dentro de la cadena de suministro también tengan acceso a los activos de información, se deben ajustar a las siguientes reglas, para evitar su divulgación o mal uso:

- Las contraseñas o claves de acceso de equipos de telecomunicaciones deben ser confidenciales y no serán divulgadas a terceros.
- Los proveedores que tengan acceso a los activos de información deberán dar estricto cumplimiento a lo establecido frente a confidencialidad, disponibilidad e integridad de la información, en las Políticas de Seguridad de la Información de TELCOS INGENIERÍA S.A.
- Los proveedores que tenga acceso a los activos de información deben aceptar el acuerdo de confidencialidad proporcionado por TELCOS INGENIERÍA S.A. o contar con un acuerdo de confidencialidad compatible con los mínimos exigidos por TELCOS INGENIERÍA S.A.
- Los proveedores que tengan acceso a los activos de información de la compañía mantendrán la debida reserva y protegerán, en todo momento, los documentos de trabajo y la información restringida que esté a su cuidado.
- Todos los proveedores que tenga acceso a los activos de información de TELCOS INGENIERÍA S.A deben contar con una política de tratamiento de datos personales y privacidad que cumpla con la legislación vigente.
- En caso de evidenciar algún riesgo, problema o incidente que comprometa la Seguridad de la Información se debe informar inmediatamente al personal de TELCOS INGENIERÍA S.A o al personal encargado de la seguridad de la información.

El área de Compras monitorea periódicamente, el cumplimiento de las obligaciones del proveedor, incluyendo el acuerdo y/o cláusula de confidencialidad.

Las áreas de Compras y de TICS administran los cambios en el suministro de servicios por parte de los proveedores, manteniendo los niveles de cumplimiento del servicio y la seguridad de la información.

Todas las acciones de mejora, observaciones e inquietudes por parte TELCOS INGENIERÍA S.A. con respecto al uso y seguridad de la información y al manejo de activos de información, deben ser acogidas y aceptadas de manera conjunta con el proveedor, minimizando riesgos que comprometan la información.

7.12 POLÍTICA DE GESTIÓN DEL CAMBIO

Versión 1, 16 de julio de 2019

TELCOS INGENIERÍA S.A garantiza que la gestión del cambio, se realice adecuadamente en los servicios de tecnología de la información internos y externos, definiendo las siguientes categorías: cambios mayores, cambios programados, cambios de emergencia y cambios estándar:

1. **Cambios Mayores:** Cambios que requieren de aprobación por parte del Presidente y/o Director Ejecutivo, como por ejemplo servicios nuevos, retirados, sus modificaciones, un nuevo cliente, un nuevo proceso, una nueva área, traslados de bodega, una nueva actividad de negocio, cambios en el contrato con el cliente o cambios tecnológicos que superen los $500.000. Dichos cambios requieren generar una Solicitud de Cambio (RFC).

2. **Cambios Programados:** En los servicios de TI internos son cambios liderados por el área de TICS que no implican una inversión superior a $500.000, pueden ser cambios en los elementos de configuración (a excepción de la información documentada), en la infraestructura de TIC, en los sistemas de información soportados, en los servidores, o en los elementos de la red interna. Para los servicios TI externos puede ser el cambio de versión de un elemento de configuración (a excepción de la información documentada), la adopción de una nueva actividad dentro de un área o el aumento de capacidades. Dichos cambios requieren generar una Solicitud de Cambio (RFC).

3. **Cambios de Emergencia:** Corresponden a cualquier interrupción de los servicios de alto impacto, ya sea por el número de usuarios que se está afectando o porque se han visto involucrados sistemas o activos críticos para la organización. Estos cambios deben encontrar una respuesta inmediata. La solución al problema requiere una Solicitud de Cambio (RFC), la cual debe realizarse posteriormente.

4. **Cambios Estándar**: Es un cambio pre-autorizado de bajo riesgo, para los servicios TI internos es relativamente común, por ejemplo, el restablecimiento de contraseñas o reasignación de equipos. En los servicios de TI externo, es un cambio en una sola actividad de un proceso, que no afecta la operación de los servicios y que no implica la adquisición de recursos que requieren autorización, por ejemplo, cambios en la información documentada de origen interno o externo, uso de recursos de back up, cambios en el turno de personal, cambios en la fecha de ejecución de un servicio o su no prestación por motivos del cliente. Los cambios en las políticas del SIG son considerados como un cambio estándar, pero requieren autorización formal por parte de la Presidencia o su apoderado.

Las anteriores Políticas del Sistema de Gestión de Seguridad de la Información son aprobadas para su socialización y cumplimiento.

MAURICIO BOTERO TOBÓN
APODERADO GENERAL

8 CONTROL DE REVISIONES

VERSIÓN N°	ELABORÓ	REVISÓ	APROBÓ	FECHA DE APROBACIÓN	MODIFICACIÓN REALIZADA
3	Jose Antonio Mojica Amaya	Claudia Galeano Paula Pesca	Mauricio Botero Tobón	08 de septiembre de 2022	• Se modificó el título del documento de Manual de Políticas de Seguridad de la Información a Manual de Políticas de Seguridad de la Información y de Gestión del Servicio. • Se redefinieron los ítems 1. INTRODUCCIÓN y 2. OBJETIVOS. • En el ítem 4. RESPONSABLES se incluyeron los cargos: Director de Capital Intelectual, Director de Tecnologías de la información y la Comunicación y Gerente Jurídico Laboral. A los demás cargos se les incluyó su alcance a la Gestión del Servicio. • Se redefinió el ítem 6. POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN, cambiando su título por POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN Y GESTIÓN DEL SERVICIO e incluyendo los conceptos generales de la Gestión del Servicio. • En el ítem 7. POLÍTICAS ESPECÍFICAS DE SEGURIDAD DE LA INFORMACIÓN se llevaron a cabo los siguientes cambios: - Modificación del nombre del ítem a POLÍTICAS ESPECÍFICAS DE SEGURIDAD DE LA INFORMACIÓN Y DE GESTIÓN DEL SERVICIO. - Se modificó la POLÍTICA PARA DISPOSITIVOS MÓVILES, TELETRABAJO Y TRABAJO EN CASA, cambiando su título por POLÍTICA PARA EL USO DE DISPOSITIVOS MÓVILES Y EL TRABAJO FUERA DE LAS INSTALACIONES y su contenido en general. - Se redefinieron las Políticas de: CLASIFICACIÓN Y ETIQUETADO DE LA INFORMACIÓN, ESCRITORIO LIMPIO Y

	Líder de Seguridad de la Información	Director de Capital Intelectual Coordinador de Calidad	Apoderado General		PANTALLA LIMPIA, POLÍTICA DE TRANSFERENCIA DE INFORMACION, POLÍTICA DE CONTROL DE ACCESO - En la POLÍTICA DE COPIAS DE RESPALDO DE INFORMACIÓN se reemplazó el área de TICS por el SGSI y del servicio y se amplió su alcance a las partes interesadas externas. - En la POLÍTICA DE DESARROLLO SEGURO se aclara la aplicabilidad de la misma a los desarrolladores de software. - Se crea la POLÍTICA DE ALMACENAMIENTO Y PROTECCIÓN DE REGISTROS. - En la POLÍTICA DE ÁREAS SEGURAS, se establecen los subtítulos: Áreas Seguras, Controles de las áreas seguras, Término de labores en las áreas seguras, Prohibiciones y restricciones en las áreas seguras y Prohibiciones y restricciones en la vivienda del usuario final. - Se redefinió la POLÍTICA DE CONTROLES CRIPTOGRAFICOS, cambiando su titulo por POLÍTICA DE USO DE CONTROLES CRIPTOGRAFICOS, y modificando su contenido. - Se incluye en el documento la POLÍTICA DE GESTIÓN DEL CAMBIO.
2	Luz Adriana Poveda	Claudia Galeano Paula Pesca	Luis Soler Mauricio Botero Tobón	04 de diciembre de 2020	• Se amplía el alcance del Manual a las partes interesadas externas que impacten la seguridad de la información. • Se realiza actualización de cargos. • Se incluye el numeral 4 RESPONSABLES. • Se incluyen los conceptos de Teletrabajo y Trabajo en Casa. • Se actualizan todas las Políticas de SI: General de SI, para dispositivos

	Líder de Seguridad de la Información	Director de Capital Intelectual Coordinador de Calidad	Coordinador de Tecnología y Seguridad de la Información Apoderado General		móviles y teletrabajo, de clasificación y etiquetado de la información, de escritorio limpio y pantalla limpia, de copias de respaldo de información, de transferencia de información, de desarrollo seguro, de control de acceso, de áreas seguras, de controles criptográficos, y para las relaciones con los proveedores.
1	Omar Andrés Fonseca Herrera	Claudia Galeano R. Directora Capital Intelectual	Mauricio Botero Tobón	08 de julio de 2019	• Creación del documento. • Actualización y compilación de todas las políticas de seguridad de la información en un solo documento.
	Líder de Seguridad de la Información	Luis Soler Coordinador de Tecnología y Seguridad de la Información	Apoderado General		