Comunicaciones S.A.S. Soluciones que te dan Confianza	**POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN**	POLÍTICA	
		COPIA CONTROLADA	
		Código: GTC-003-PO	Versión: 0.3
		Fecha: 17 Abril 2019	Página 1 de 17

1. OBJETIVO

Determinar las políticas que regulan el sistema de gestión de seguridad de la información que permiten preservar la información y los sistemas implicados en **LINEA COMUNICACIONES S.A.S** teniendo en cuenta los requisitos legales, operativos, tecnológicos, de seguridad y de la organización alineados con el direccionamiento estratégico, gestión del riesgo y el sistema gestión de calidad con el propósito de garantizar la integridad, confidencialidad, disponibilidad, no repudio y legalidad de la información.

2. ALCANCE

Las políticas de seguridad de la información son aplicables para todos los procesos administrativos y de control que tienen que ser cumplidos por empleados, contratistas, proveedores, visitantes y demás partes interesadas que presten sus servicios o tengan alguna relación con **LINEA COMUNICACIONES S.A.S** y que hagan parte de los procesos estratégicos, misionales y apoyo del sistema de gestión.

3. POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN

La política de seguridad y privacidad de la Información es la declaración general que representa la posición de la junta directiva de **LINEA COMUNICACIONES S.A.S** con respecto a la protección de los activos de información (los colaboradores, contratistas, partes interesadas. la información, los procesos, las tecnologías de información incluido el hardware y el software), que soportan los procesos de la Compañía y apoyan la implementación del Sistema de Gestión de Seguridad de la Información, por medio de la generación y publicación de sus políticas, procedimientos e instructivos, así como de la asignación de responsabilidades generales y específicas para la gestión de la seguridad de la información.

3.1. Objetivos Específicos.

Establece la compatibilidad de la política de seguridad de la información y los objetivos de seguridad de la información, estos últimos correspondientes a:

- Minimizar el riesgo de los procesos misionales de la entidad.
- Cumplir con los principios de seguridad de la información.
- Cumplir con los principios de la función administrativa.
- Mantener la confianza de los colaboradores, contratistas y demás partes interesadas.
- Apoyar la innovación tecnológica.

- Implementar el sistema de gestión de seguridad de la información.
- Proteger los activos de información.
- Establecer las políticas, procedimientos e instructivos en materia de seguridad de la información.
- Fortalecer la cultura de seguridad de la información en los colaboradores, partes interesadas y clientes de **LINEA COMUNICACIONES S.A.S.**
- Garantizar la continuidad del negocio frente a incidentes y problemas conocidos con riesgo aceptado.
- Establecer un equipo interdisciplinario que realice la gestión de riesgo de la seguridad de la información mediante una metodología para la valoración y tratamiento del riesgo.

Nivel de cumplimiento

Todas las personas cubiertas por el alcance y aplicabilidad deberán dar cumplimiento un 100% de la política.

3.2. Políticas generales de seguridad de la información

- **LINEA COMUNICACIONES S.A.S** ha decidido definir, implementar, operar y mejorar de forma continua un Sistema de Gestión de Seguridad de la Información, soportado en lineamientos claros alineados a las necesidades del negocio, y a los requerimientos regulatorios que le aplican a su naturaleza
- El área de infraestructura y el área de calidad junto con los procesos misionales y de apoyo serán responsables del mantenimiento, revisión y mejora de los controles implementados en la Seguridad de la Información de la empresa a través de las diferentes direcciones.
- Definir los criterios básicos necesarios para la valoración, tratamiento y mitigación de los riesgos de información que serán identificados mediante la metodología de valoración de riesgos establecida en el sistema integrado de gestión.
- **LINEA COMUNICACIONES S.A.S** protegerá la información generada, procesada o resguardada por los procesos de negocio y activos de información que hacen parte de los mismos. Para ello es fundamental la aplicación de controles de acuerdo con la clasificación de la información de su propiedad o en custodia.
- Las responsabilidades frente a la seguridad de la información serán definidas, compartidas, publicadas y aceptadas por cada uno de los empleados, contratistas o partes interesadas.
- **LINEA COMUNICACIONES S.A.S** garantizará a través de una adecuada gestión de los eventos de seguridad y las debilidades asociadas con los sistemas de información una mejora efectiva de su modelo de seguridad.
- **LINEA COMUNICACIONES S.A.S** protegerá su información de las amenazas originadas por parte del personal.

- **LINEA COMUNICACIONES S.A.S** protegerá las instalaciones de procesamiento y la infraestructura tecnológica que soporta sus procesos críticos.
- **LINEA COMUNICACIONES S.A.S** controlará la operación de sus procesos de negocio garantizando la seguridad de los recursos tecnológicos y las redes de datos.
- **LINEA COMUNICACIONES S.A.S** implementará control de acceso a la información, sistemas y recursos de red.
- **LINEA COMUNICACIONES S.A.S** garantizará que la seguridad sea parte integral del ciclo de vida de los sistemas de información.
- **LINEA COMUNICACIONES S.A.S** garantizará la disponibilidad de sus procesos de negocio y la continuidad de su operación basado en el impacto que pueden generar los eventos.
- **LINEA COMUNICACIONES S.A.S** garantizará el cumplimiento de las obligaciones legales, regulatorias y contractuales establecidas**.**

El incumplimiento a la política de Seguridad de la Información, traerá consigo, las consecuencias legales que apliquen a la normativa de **REGLAMENTO INTERNO DE TRABAJO LINEA COMUNICACIONES** en el capítulo XVIII e incluyendo lo establecido en las normas que competen al Gobierno nacional y territorial en cuanto a Seguridad de la Información se refiere.

3.3. Acuerdos de confidencialidad o de no divulgación [ISO/IEC 27001:2013 A.13.2.4]

La política de confidencialidad, debe contener un compromiso o acuerdo de confidencialidad, por medio del cual todo funcionario, contratista y/o partes interesadas vinculado a la **LINEA COMUNICACIONES S.A.S**, deberá aceptar y firmar un compromiso de no divulgar la información interna y externa que conozca de la compañía. La firma del acuerdo implica que la información conocida por todo funcionario, contratista y/o partes interesadas, bajo ninguna circunstancia deberá ser revelada por ningún medio electrónico, verbal, escrito u otro, ni total ni parcialmente, sin contar con previa autorización.

En el caso de los contratistas, se debe incluir una cláusula de confidencialidad en los respectivos contratos que hacen parte integral de este. Estos acuerdos deben ser aceptados por cada uno de ellos.

Para el caso de los empleados de **LINEA COMUNICACIONES S.A.S**, pero de administración del cliente, de igual meneara se les darán las políticas y estará incluido en las cláusulas del contrato, pero será su decisión del cliente dar a conocer y establecer un mecanismo para que el personal adopte las políticas de seguridad definidas por él.

La política deberá indicar desde cuando se firma el acuerdo de confidencialidad, así como la vigencia del mismo.

Las directrices de acuerdos de confidencialidad o de no divulgación se encuentran definidas en **DE-001-R V 0,1 ACUERDO DE CONFIDENCIALIDAD EMPLEADOS.**

3.4. Política sobre el uso de los servicios de red [ISO/IEC 27001:2013 A.9.1.2]

Se permite al acceso de internet, implantando lineamientos que garanticen la navegación segura y su uso adecuado de este recurso por lo cual se debe controlar, monitorear y verificar el uso de los empleados para evitar pérdidas, modificaciones o uso inapropiado.

El coordinador de infraestructura suministrará la autorización de los cambios solicitados de permisos de navegación de **LINEA COMUNICACIONES S.A.S,** previa solicitud al Gerente de Proyecto en cada una de las dependencias.

El coordinador de infraestructura establecerá herramientas para evitar descarga e instalación de software no autorizado en los equipos propios de la compañía o que estén matriculados en el dominio corporativo.

No se permite la navegación a páginas con contenidos que representen peligro a la organización o vayan en contra de la ley como: pornografía, terrorismo, hacking, racismo, violencia infantil u otras en contra de las políticas de la empresa.

Se deberán ejercer controles con el fin de evitar uso de proxys, vpn y todas aquellas herramientas que mediante mecanismos intrusivos e invasivos buscan evadir las políticas y controles de seguridad establecidos para el uso de la red tanto local como de internet.

Esta restringido el acceso a redes sociales, mensajería instantánea o servicios de streaming durante la jornada laboral como: Facebook, Twitter, Instagram, Messenger, YouTube y otros similares para fines diferentes a las actividades propias del negocio. Como parte de la campaña de bienestar de **LINEA COMUNICACIONES S.A.S** se permite el acceso controlado durante el mediodía a estas páginas de acuerdo a las políticas de seguridad en cada sede.

No se debe intercambiar información estratégica de la empresa con terceros no autorizados y la descarga de archivos debe ser solo con propósitos laborales y de forma responsable.

El uso de este recurso no considerado dentro de las prohibiciones anteriores debe ser de forma ética, razonable, no abusiva y que no afecte la productividad ni la protección de la información de **LINEA COMUNICACIONES S.A.S**

3.5. Mensajería electrónica [ISO/IEC 27001:2013 A.13.2.3]

Definir las pautas generales para asegurar una adecuada protección de la información de **LINEA COMUNICACIONES S.A.S.** en el servicio y uso del servicio de correo electrónico por parte de los usuarios autorizados.

Todo empleado y/o tercero vinculado a la compañía a quienes se les asigne una cuenta de correo electrónico corporativa deberán acatar los siguientes lineamientos:

- Los usuarios del correo deben utilizarse la cuenta exclusivamente para la ejecución de las funciones y tareas propias de **LINEA COMUNICACIONES S.A.S** con finalidad operativa y directiva, serán responsables de malas prácticas o usos que puedan comprometer la seguridad de la información y no se podrá utilizar para uso personal, toda la información personal contenida en los buzones son propiedad de la empresa.

- Se asignará un correo corporativo según la necesidad del proyecto, iniciando con su primer nombre, seguido de un punto(.) y siguiendo con su primer apellido (nombre.apellido@lineacom.co).

- Los usuarios y claves del correo electrónico corporativo son de uso personal e intransferible, no se deben dar a conocer a terceros. Las contraseñas deben emplear un alto nivel de complejidad y de autenticación.

- Esta restringido el envío de correos con información que atente contra la integridad y dignidad de las personas, el buen nombre, imagen y reputación de la empresa, como lo son: contenidos racistas, sexistas, pornográficos, violencia infantil, publicitarios o no institucionales.

- Reportar al área de infraestructura direcciones de correos electrónicos de dudosa procedencia u origen desconocido, que contengan dominios ajenos a **LINEA COMUNICACIONES S.A.S** o contratistas y/o partes interesadas vinculados a la empresa.

- El tamaño de buzones y la firma corporativa es determinado por el área de infraestructura, teniendo en cuenta las necesidades de cada usuario.

- El envío y recepción de archivos adjuntos está permitido a excepción de archivos maliciosos, scripts o modificadores de registros. Al descargar estos adjuntos deben ser analizados por el software de antivirus vigente.

- Es responsabilidad del área de infraestructura, la creación y modificación de cuentas de correos electrónicos corporativos al momento de vinculación del personal, de igual manera la inactivación o cancelación después de finalización del contrato o desvinculación de la empresa. En este punto de acuerdo a consideración del líder del proyecto se solicitará la realización de backup del correo electrónico y/o copia del buzón.

3.6. Clasificación de la Información. [ISO/IEC 27001:2013 A.8.2]

Asegurar que la información recibe el nivel de protección apropiado de acuerdo al tipo de clasificación establecido por la ley y **LINEA COMUNICACIONES S.A.S.**

Se considera información toda modalidad de comunicación, conocimiento o datos digitales, documentados en cualquier medio, ya sea papel, impreso o magnético, por ejemplo:

- Formularios / comprobantes propios o de terceros.
- Información en los sistemas, equipos informáticos, medios magnéticos/electrónicos o medios físicos como papel.
- Otros soportes magnéticos/electrónicos removibles, móviles o fijos.
- Información o conocimiento transmitido de manera verbal o por cualquier otro medio de comunicación.

Los Líderes de área responsables de la información contenida en los Procesos y los clientes a su cargo, deben delimitar las responsabilidades de sus subordinados y determinar quién está autorizado a efectuar operaciones emergentes con dicha información tomando las medidas de seguridad pertinentes que están definidos en el formato perfil de cargo, estos privilegios están definidos en el formato de perfil d cargo.

Ningún tercero en proyectos o trabajos específicos, deberá poseer para usos no propios de su responsabilidad ningún material o información confidencial de la compañía y/o sus clientes tanto ahora como en el futuro.

Se definen las siguientes categorías para clasificar la información en la compañía:

- **Restringida:** Información extremadamente sensible al interior de la compañía y que puede ser conocida únicamente por cierto número de colaboradores.

- **Reservada:** Información sensible al interior de la compañía y es para uso exclusivo de un grupo específico de colaboradores.

- **Interna:** Información disponible solo para los colaboradores de la compañía.

- **Publica:** Información no sensible que puede ser conocida tanto por el personal de la compañía como por terceros sin poner en riesgo la imagen institucional.

El software, documentación digital y demás tipos de información física expresa de **LINEA COMUNICACIONES S.A.S**, no deben ser compartida, puesta en venta ni transferida a ningún ente sin previa autorización expresa por la gerencia.

No se debe otorgar nombre de usuario, contraseñas ni privilegios de ningún nivel para utilizar infraestructura tecnológica como equipos de cómputo, red LAN, servicios informáticos a personas que no pertenecen a **LINEA COMUNICACIONES S.A.S** sin previa autorización del Área de Infraestructura y la gerencia general o las gerencias de proyectos.

3.7. Instalación de software en sistemas operativos. [ISO/IEC 27001:2013 A.12.5.1]

Definir las pautas generales para asegurar una adecuada utilización del software y los sistemas implicados para proteger la seguridad de la información de **LINEA COMUNICACIONES S.A.S**

El área de Infraestructura como administrador de este recurso deberá:

- Implementar herramientas para evitar la descarga e instalación de software no autorizado y/o código malicioso en los equipos en dominio y/o propiedad de **LINEA COMUNICACIONES S.A.S** para prevenir la fuga e información.

- Gestionar, aprobar y distribuir nuevo software que se vayan a adquirir de acuerdo a los requerimientos de seguridad de la información y a las políticas de adquisición.

- Establecer el procedimiento para que el software instalado y los recursos estén protegidos por derechos de autor y licenciamiento de uso.

Todo empleado y/o tercero vinculado a la compañía a quienes hagan uso de este recurso deberán acatar los siguientes lineamientos:

- Instalar y/o utilizar software no autorizados por el área de infraestructura que sean diferentes con la actividad laboral y que pueda deteriorar el desempeño de las diferentes actividades de **LINEA COMUNICACIONES S.A.S**

- Solicitar al área de infraestructura en coordinación con el área implicada la autorización para instalar software en los equipos para ejecutar tareas y funciones contemplando especificaciones técnicas, requerimientos funcionales y de seguridad de la información.

- El software proporcionado por **LINEA COMUNICACIONES S.A.S** no puede ser copiado o suministrado a terceros sin previa autorización del coordinador de Infraestructura en conjunto con la Gerencia General.

- El área de Infraestructura debe definir y actualizar, de manera periódica, la lista de software y aplicaciones autorizadas que se encuentran permitidas para ser instaladas en los puestos de trabajo de los usuarios. Así mismo, realizar el control y verificación de cumplimiento del licenciamiento del respectivo software y aplicaciones asociadas.

3.8. Procedimientos de operación documentados [ISO/IEC 27001:2013 A.12.1.1]

Todos los procedimientos que se tengan en operación deben ser documentados y puestos a disposición de los usuarios de **LINEA COMUNICACIONES S.A.S**. que los requieran para sus funciones y actividades.

En caso de instructivos, manuales y directrices propias de la compañía se debe comprobar que están completamente documentados, que las diferentes versiones se conservan adecuadamente en varios medios y se guarda copia de respaldo.

Para la copia de documentación, se requiere tener la autorización por escrito del coordinador líder del sistema de gestión de calidad con previa solicitud y/o del proveedor si éste lo exige.

Restringir el acceso a personal y/o terceros no autorizados a documentación clasificada o reservada.

3.9. Ubicación y protección de equipos [ISO/IEC 27001:2013 A.11.2.1]

Los equipos que tienen relación con la infraestructura tecnológica de **LINEA COMUNICACIONES S.A.S** que soportan la operación del negocio y brindan servicios de apoyo a la información decisiva de la empresa y sus dependencias, deben ser

ubicados y resguardados adecuadamente con óptimas condiciones de seguridad física y ambiental para prevenir deterioros, robos y accesos no autorizados. De igual forma, se deben implantar los controles necesarios para preservar los equipos distantes de lugares que contengan riesgos de amenazas tales como fuego, explosivos, agua, polvo, vibración, interferencia electromagnética y vandalismo, entre otros.

Únicamente el personal autorizado puede realizar tareas de administración en equipos de infraestructura en el cuarto de equipos, se deben utilizar herramientas y mecanismos de seguridad para monitorear las conexiones y el procesamiento de la información. De igual forma, el personal que tenga acceso al cuarto de equipos no puede fumar, beber o consumir cualquier tipo de alimento próximo a los equipos.

3.10. Inventario de activos [ISO/IEC 27001:2013 A.8.1.1]

Se deberían identificar los activos asociados con la información y las instalaciones de procesamiento de información, y se debería elaborar y mantener un inventario de estos activos.

Se debe listar todos aquellos recursos (físicos, de información, software, documentos, servicios, personal) dentro del alcance del sistema de gestión de seguridad de la información, que tengan importancia para la organización y necesiten ser protegidos de sufrir riesgos.

Todos los equipos de cómputo y equipos de comunicación de **LINEA COMUNICACIONES S.A.S**, deben llevar un identificador único, legible de manera que los inventarios puedan hacerse de manera eficiente.

Determinar la periodicidad con la cual se va a realizar al interior de **LINEA COMUNICACIONES S.A.S** la identificación y/o actualización del inventario de activos de Información, se debe determinar el responsable de realizar la actividad, se debe determinar bajo que instrumento se va a realizar la actividad, dicho instrumento debe permitir identificar el propietario del activo de información.

Todos los activos tanto pertenecientes a la compañía y como lo de los proveedores, serán inventariados en la plataforma Mántum.

3.11. Perímetro de seguridad física [ISO/IEC 27001:2013 A.11.1.1]

Se deberían definir y usar perímetros de seguridad, y usarlos para proteger áreas que contengan información sensible o critica, e instalaciones de manejo de información.

Definir los perímetros físicos de seguridad donde se encuentra información crítica, sensible o se realice almacenamiento y/o procesamiento de información a los cuales los colaboradores, contratistas o partes interesadas, tienen acceso y a cuáles no, la política debe definir los responsables de autorizar o no ingresos a las áreas delimitadas como de acceso restringido.

El área de Infraestructura debe tener disponible el mapa actualizado de las instalaciones eléctricas y de comunicaciones de los equipos de cómputo en la red.

Las instalaciones eléctricas, físicas y de comunicaciones debe permanecer resguardados del paso de personas o maquinas y libres de cualquier interferencia eléctrica o magnética.

3.12. Gestión de acceso de usuarios [ISO/IEC 27001:2013 A.9.2]

Determinar los procedimientos formales y directrices que se deben construir para la gestión de asignación, modificación, revisión o revocación de derechos y/o privilegios a cada uno de los usuarios (ID) creados, también deben tenerse en cuenta en esta política los casos especiales como lo son usuarios (ID) con privilegios superiores utilizados para la administración de infraestructura, aplicaciones y sistemas de información de **LINEA COMUNICACIONES S.A.S.**

Todo sistema computarizado multiusuario perteneciente a la empresa debe contar con un administrador de seguridad designado para definir los privilegios de los usuarios, monitorear los registros del control de acceso.

Únicamente se permitirá el acceso a la información de **LINEA COMUNICACIONES S.A.S** al personal autorizados para el cumplimiento de las tareas relacionadas con su responsabilidad y/o funciones. Se deben identificar y autenticar a cualquier usuario que, de manera local o remota, que requiera utilizar los recursos de tecnología y operación de la compañía.

3.13. Protección contra códigos maliciosos. [ISO/IEC 27001:2013 A.12.2]

Implantar que todos los recursos informáticos deben estar respaldados por herramientas y software de seguridad como antivirus, antispam, antispyware,

antimalware y otras aplicaciones que proporcionan protección contra códigos maliciosos y prevención del mismo a la red de **LINEA COMUNICACIONES S.A.S.**

Se debe garantizar que el software antivirus cuenta con licencias de uso activas, respaldando su autenticidad y su constate actualización previniendo que códigos maliciosos ataquen vulnerabilidades del sistema.

Los usuarios que manipulen activos de información tecnológicos bajo ninguna circunstancia podrán operar la configuración del software antivirus de sus computadores. Únicamente se podrá utilizar hardware y software que esté aprobado por el área de infraestructura.

Se deberá comunicar al área de infraestructura en caso de que los equipos presenten infecciones por virus, elementos sospechosos o perdidas de información.

3.14. Copias de respaldo. [ISO/IEC 27001:2013 A.12.3]

Suministrar medios de respaldo adecuados para garantizar que toda la información vital y el software, se pueda rescatar después de una falla, asegurando que la información y la infraestructura del software esencial de **LINEA COMUNICACIONES S.A.S** sean respaldados en caso de un error y/o desastre.

El área de infraestructura será el responsable de definir la frecuencia de respaldo, requerimientos de seguridad y de realizar los respaldos periódicos para la información con cierto nivel de clasificación.

Las copias de respaldo se conservarán solo con el objetivo de recomponer el sistema después de la infección de un virus informático, defectos en los discos de almacenamiento, fallas de los servidores o computadores, materialización de amenazas, catástrofes y por requerimiento legal.

Se verificará la correcta ejecución de los procesos de backups de los servidores de **LINEA COMUNICACIONES S.A.S** con una periodicidad diaria para garantizar que la información este respaldada en caso de fallas. se evidenciarán con registros los backups realizados. Del mismo modo, se deberá definir la periodicidad para ejecutar los backups de los equipos de los usuarios de la empresa.

Ningún tipo de información corporativa puede ser almacenada en forma exclusiva en los discos duros de las estaciones de trabajo, por lo tanto, es obligación de los usuarios finales realizar las copias en las carpetas destinadas para este fin.

Desarrollar un plan de emergencia para las aplicaciones que manipulen información crítica, se debe asegurar que el plan es adecuado, frecuentemente actualizado y frecuentemente probado y revisado.

El área de infraestructura debe preservar un inventario actualizado de las copias de respaldo de la información y los aplicativos de **LINEA COMUNICACIONES S.A.S**

Todas las copias de información sensible deben ser almacenadas de forma apropiada y con control de acceso.

Los medios que vayan a ser suprimidos deben padecer un proceso de borrado seguro y seguidamente serán eliminados o destruidos de forma apropiada.

3.15. Requisitos del negocio para control de acceso [ISO/IEC 27001:2013 A.9.1]

Limitar el acceso a información y a instalaciones de procesamiento de información a personal no autorizado. Todo empleado y/o tercero vinculado a la compañía deberán acatar los siguientes lineamientos:

- Los sistemas de información de la compañía deben contar con privilegios o niveles de seguridad de acceso suficientes para garantizar la seguridad de la información corporativa.

- El acceso a plataformas, aplicaciones, servicios y en general cualquier recurso de información de **LINEA COMUNICACIONES S.A.S** o de los clientes que este administre, debe ser asignado de acuerdo a la identificación previa de requerimientos de seguridad y del negocio que se definan por las diferentes dependencias.

- Los usuarios que han sido autorizados para ver la información confidencial con un cierto nivel de sensibilidad (perfiles críticos), pueden acceder sólo a la información de ese nivel o de grados inferiores.

- No debe otorgarse privilegios para utilizar los equipos de cómputo o los sistemas de comunicación de la empresa a las personas que no sean empleados como contratistas o consultores, a menos que se obtenga previa autorización del área de Infraestructura y/o gerencia general.

- El área de infraestructura administrara el ciclo de vida de los usuarios, desde su ingreso, creación de cuentas, roles, privilegios, permisos hasta su retiro o desvinculación de la organización considerando los requerimientos reportadas por cada una de las áreas de la empresa con el propósito de que el funcionario

tenga acceso apropiado a los sistemas de información y recursos tecnológicos, validando su autenticación y autorización.

Las directrices de control de acceso se encuentran definidas **GTC-000-P V 0,1 PROCEDIMIENTO PARA CONTROL DE ACCESO EN EL ÁREA TI.**

3.16. Sistema de gestión de contraseñas de usuario. [ISO/IEC 27001:2013 A.9.4.3]

Definir las directrices mínimas en cuanto a calidad que deben tener las contraseñas para ser empeladas como procedimiento de legitimación en los accesos de la red, aplicaciones y/o sistemas de información.

Todos los colaboradores, contratista y/o tercero vinculado a la **LINEA COMUNICACIONES S.A.S** deben acatar los siguientes criterios:

- Ningún usuario debe acceder a los servicios o aplicaciones de red, utilizando las credenciales de otros usuarios.
- Se suministrará a los usuarios las claves o contraseñas respectivas para los accesos a los diferentes servicios de red con previa autorización teniendo en cuenta privilegios de acceso de usuarios con base en los roles y perfiles.

- Las claves o contraseñas son personales e intransferibles y no deben prestarse, ni compartirse. La compañía debe establecer que por cada funcionario, contratista o tercero debe tenerse un usuario y una contraseña para el acceso.

- Las contraseñas para garantizar nivel alto de complejidad y fuerte autenticación deben: Tener mínimo ocho (8) caracteres alfanuméricos, caracteres en minúscula y al menos un carácter en mayúscula y otro carácter no alfabético (Ejemplo: ¡,$,%,&), no deben ser palabras comunes, ni tener información personal, evitar asociarla con fechas especiales, por ejemplo: fechas de cumpleaños, nombres o números telefónicos.

- Se debe asegurar que el ingreso a la plataforma de tecnología se realice con la vinculación directamente de los permisos de los usuarios de directorio activo.

- Cambiar obligatoriamente la primera vez que se ingresa a los sistemas y se deben cambiar periódicamente las contraseñas y claves de acceso para los diferentes servicios y aplicaciones de red.

- Evitar utilizar claves y contraseñas personales en el campo corporativo.

- No registrar claves y contraseñas en papel, archivos digitales o manuales, almacenarlas en el navegador de uso frecuente, por lo contrario; se podrán almacenar de forma segura con métodos de almacenamiento autorizados.

3.17. Política de escritorio limpio y pantalla limpia [ISO/IEC 27001:2013 A 11.2.9]

Atribuir las pautas generales para minimizar el riesgo de acceso no autorizado, pérdidas o daños durante y fuera de la jornada de trabajo normal de los usuarios.

Los empleados, contratistas y/o partes interesadas que tienen algún vínculo con **LINEA COMUNICACIONES S.A.S** deben conservar la información restringida o confidencial contenida en su escritorio que debe estar libre de información, propia de la compañía, que pueda ser obtenida, copiada o manipulada por ter ceros o por personal que no tenga autorización para su uso o conocimiento.

Se debe mantener bajo llave dispositivos con información confidencial tales como: documentos impresos, USBs, CDs, discos duros o medios removibles en general. Al imprimir documentos con información reservada se deben ser retirados inmediatamente de la impresora.

Los usuarios deben bloquear la sesión de sus computadores en los momentos que no se esté utilizando el equipo, cuando estén desentendidos, cuando por cualquier motivo deba dejar su puesto de trabajo o en horas no laborables. Los usuarios deben cerrar las aplicaciones y servicios de red cuando no se estén utilizando.

3.18. Separación de redes. [ISO/IEC 27001:2013 A.13.1.3]

Los grupos de servicios de información, usuarios y sistemas de información se deberían separar en las redes.

Las servicios y aplicaciones de red que soportan los sistemas de información deberán estar divididos en segmentos de red físicos y lógicos e independientes de los segmentos de red de usuarios, conexiones de terceros y accesos a internet.

El área de Infraestructura es el área encargada de indicar los perímetros de seguridad necesarios para resguardar dichos segmentos, conforme con el nivel de criticidad del flujo de la información transmitida.

La información involucrada en las transacciones de servicios de aplicación deberá ser protegida para prevenir la transmisión incompleta, mal enrutamiento, alteración de mensaje no autorizado, la divulgación no autorizada, la duplicación de mensajes no autorizados o la reproducción.

3.19. Identificación de requerimientos de seguridad. [ISO/IEC 27001:2013 A.14.1]

Asegurar que la seguridad de la información sea una parte integral de los sistemas de información durante todo el ciclo de vida. Esto incluye también los requisitos para sistemas de información que prestan servicios en redes públicas.

Los requisitos asociados con la seguridad de la información serán comprendidos, identificados, aprobados y documentados en los requerimientos para la obtención de nuevos sistemas de información como también mejoras, actualización y/o cambios a los sistemas ya existentes, tarea que efectuara el área de infraestructura y las áreas propietarias del sistema en cuestión.

Los responsables por el aprovisionamiento de soluciones deben crear y preservar las metodologías que manejen el ciclo completo de adquisición, elaboración, conservación y disposición seguro de soluciones de sistemas de información.

Todas las soluciones de información o de infraestructura debe preservar durante su ciclo de vida una gestión de riesgo que comuniquen permanentemente el nivel de exposición que signifique para la **LINEA COMUNICACIONES S.A.S.**

Los requerimientos de seguridad de la información reconocidos, obligaciones provenientes de las leyes de propiedad intelectual y derechos de autor deben ser implantados en los acuerdos contractuales que se ejecuten entre **LINEA COMUNICACIONES S.A.S.** y cualquier proveedor de productos y/o servicios vinculado a la infraestructura de procesamiento de información.

4. TÉRMINOS Y DEFINICIONES

- **Activo:** Cualquier información o sistema asociado con el tratamiento de la misma que tenga valor para la compañía.
- **Amenaza:** Causa potencial de un incidente no deseado, el cual puede causar el daño a un sistema o la organización.
- **Autenticación:** Proceso que tiene como finalidad validar la identificación de una persona o sistema.
- **Confidencialidad:** se garantiza que la información sea accesible sólo a aquellas personas autorizadas a tener acceso a la misma.
- **Control**: son todas aquellas políticas, procedimientos, prácticas y las estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido.
- **Disponibilidad:** se garantiza que los usuarios autorizados tengan acceso a la información y a los recursos relacionados con la misma, toda vez que lo

requieran.

- **ERP:** Enterprise Resource Planning; Sistema de información utilizado por la empresa para almacenar los datos de gestión contable, gestión humana y demás.
- **Gestión del Riesgo:** actividades coordinadas para dirigir y controlar una organización en relación con el riesgo.
- **Información:** todo aquel conjunto de datos organizados en poder de una entidad que posean valor para la misma, independientemente de la forma en que se guarde o transmita (escrita, en imágenes, oral, impresa en papel, almacenada electrónicamente, proyectada, enviada por correo, fax o e-mail, transmitida en conversaciones, etc.), de su origen (de la propia organización o de fuentes externas) o de la fecha de elaboración.
- **Integridad:** se salvaguarda la exactitud y totalidad de la información y los métodos de procesamiento.
- **ISO**: Organización Internacional de Normalización, con sede en Ginebra (Suiza). Es una agrupación de organizaciones nacionales de normalización cuyo objetivo es establecer, promocionar y gestionar estándares.
- **Kastor:** Software enfocado para la gestión de actividades.
- **Legalidad:** referido al cumplimiento de las leyes, normas, reglamentaciones o disposiciones a las que está sujeto el Organismo.
- **Mántum:** Plataforma para gestión y sistematización de los activos y procesos de la Compañía.
- **No repudio:** Una autentificación que con un alto aseguramiento pueda ser reafirmado como genuino.
- **Privilegios:** Permisos de acceso a aplicativos y/o redes.
- **Riesgo:** Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información.
- **Tratamiento del Riesgo**: proceso de selección e implementación de medidas para modificar el riesgo.
- **Virus:** Programas informáticos de carácter malicioso, que buscan alterar el normal funcionamiento de una red de sistemas o computador personal.
- **VPN:** Una red privada virtual (RPV), en inglés: Virtual Private Network (VPN) es una tecnología de red de computadoras que permite una extensión segura de la red de área local (LAN) sobre una red pública o no controlada como Internet.
- **Vulnerabilidad:** Debilidad en la seguridad de la información de una organización que potencialmente permite que una amenaza afecte a un activo.

5. MARCO LEGAL

Las directrices del marco legal se encuentran definidas en **MATRIZ REQUISITOS LEGALES.**

6. REQUISITOS TÉCNICOS

- Norma técnica colombiana NTC-ISO/IEC 27001:2013 Sistemas de gestión de la seguridad de la información.
- Norma técnica colombiana NTC-ISO/IEC 27002:2013 Técnicas de seguridad. Código de practica para la gestión de la seguridad de la información.
- Guía No. 2. Elaboración de la política general de seguridad y privacidad de la información. MINTIC.
- Guía No. 8. Controles de seguridad y privacidad de la información. MINTIC.
- Modelo de seguridad y privacidad de la informacion. MINTIC.

7. DOCUMENTOS ASOCIADOS

- **DE-001-R V 0,1 ACUERDO DE CONFIDENCIALIDAD EMPLEADOS.**
- **REGLAMENTO INTERNO DEL TRABAJO.**
- **MATRIZ REQUISITOS LEGALES.**
- **GTC-002-P V 0,1 PROCEDIMIENTO ACCESO Y DENEGACIÓN DE USUARIOS.**

8. RESPONSABLE DEL DOCUMENTO

Área de Infraestructura TI.

Control de cambios

Versión	Fecha	Descripción Del cambio
0.1	22-12-2017	Borrador
0.2	01-03-2018	Versión Inicial
0.3	00-04-2019	Se cambia codificación para el área de TIC y se incluyen elementos según los requisitos exigidos