1. OBJETIVOS

- Establecer las políticas en seguridad de la información de **CONNECT SUPPORT OPERATIONAL SERVICES S.A.** quien en adelante se denominará, LA COMPAÑÍA, con el fin de regular la gestión de la seguridad de la información al interior de la organización.
- Definir mecanismos para proteger la información de negocio de la organización y cualquier información de clientes o proveedores bajo su custodia, salvaguardando su confidencialidad, integridad y disponibilidad.
- Proporcionar la adecuada cobertura de los estándares internacionales ISO 27001, ISO 27002 y PCI DSS V3.2.

2. ALCANCE

- Cada persona que desempeñe alguna labor para LA COMPAÑÍA, sin importar su condición (empleado, contratista, personal temporal, proveedor, socio de negocios, etc.) debe cumplir con las políticas de seguridad de la información definidas en este documento y en documentos de seguridad adicionales aquí referenciados.

- Estas políticas aplican a todos los activos de información de LA COMPAÑÍA, incluyendo pero no limitándose a: computadores, sistemas de red y componentes de su infraestructura, plataformas (sistemas operativos), aplicaciones (sean estas desarrolladas “in-house”, compradas o alquiladas a terceras partes), bases de datos, documentos impresos, servicios e información considerada necesaria para el negocio.

3. DEFINICIONES

Activo de información: cualquier componente (humano, tecnológico, software, documental o de infraestructura) que soporta uno o más procesos de negocios de la COMPAÑÍA y en consecuencia, debe ser protegido.
Acuerdo de Confidencialidad: Documento en el que cualquier persona que desempeñe alguna labor para LA COMPAÑÍA, sin importar su condición (empleado, contratista, personal temporal, proveedor, socio de negocios, etc.) manifiesta su voluntad de mantener la confidencialidad de la información de la organización, comprometiéndose a no divulgar, usar o explotar la información

confidencial a la que tengan acceso en virtud de la labor que desarrollan dentro de la misma.

Análisis de riesgos de seguridad de la información: proceso sistemático de identificación de fuentes, estimación de impactos y probabilidades y comparación de dichas variables contra criterios de evaluación para determinar las consecuencias potenciales de pérdida de confidencialidad, integridad y disponibilidad de la información.

Autenticación: es el procedimiento de comprobación de la identidad de un usuario o recurso tecnológico al tratar de acceder a un recurso de procesamiento o sistema de información.

Centro de cómputo: es una zona específica para el almacenamiento de múltiples computadores para un fin específico, los cuales se encuentran conectados entre sí a través de una red de datos. El centro de cómputo debe cumplir ciertos estándares con el fin de garantizar los controles de acceso físico, los materiales de paredes, pisos y techos, el suministro de alimentación eléctrica y las condiciones medioambientales adecuadas.

Cifrado: es la transformación de los datos mediante el uso de la criptografía para producir datos ininteligibles (cifrados) y asegurar su confidencialidad. El cifrado es una técnica muy útil para prevenir la fuga de información, el monitoreo no autorizado e incluso el acceso no autorizado a los repositorios de información.

Confidencialidad: es la garantía de que la información no está disponible o divulgada a personas, entidades o procesos no autorizados.

Control: es toda actividad o proceso encaminado a mitigar o evitar un riesgo. Incluye políticas, procedimientos, guías, estructuras organizacionales y buenas prácticas, que pueden ser de carácter administrativo, tecnológico, físico o legal.

Criptografía: es la disciplina que agrupa a los principios, medios y métodos para la transformación de datos con el fin de ocultar el contenido de su información, establecer su autenticidad, prevenir su modificación no detectada, prevenir su repudio, y/o prevenir su uso no autorizado.

Custodio del activo de información: es la unidad organizacional o proceso, designado por los propietarios, encargado de mantener las medidas de protección establecidas sobre los activos de información confiados.

Derechos de Autor: es un conjunto de normas y principios que regulan los derechos morales y patrimoniales que la ley concede a los autores por el solo hecho de la creación de una obra literaria, artística o científica, tanto publicada o que todavía no se haya publicado.

Disponibilidad: es la garantía de que los usuarios autorizados tienen acceso a la información y a los activos asociados cuando lo requieren.

Persona que desarrolle una actividad en la compañía: Empleado, contratista, personal temporal, proveedor, socio de negocios etc.

4. DESARROLLO

Las políticas de seguridad definidas a continuación, se encuentran alineadas con los requerimientos del estándar **ISO 27001, y PCI DSS V3.2** y aplican para todos los empleados y Outsourcing de LA COMPAÑÍA.

PRINCIPIOS DE PROTECCION

La formulación de la Política de Seguridad de la Información del SGSI dentro del cumplimiento de los siguientes principios claves de protección:

- **Eficacia**: Garantizar que toda la información utilizada es necesaria y útil para el desarrollo y difusión de los datos estadísticos generados.
- **Eficiencia**: Asegurar que el procesamiento de la información se realice mediante una óptima utilización de los recursos humanos y materiales.
- **Integridad**: Asegurar que sea procesada toda la información necesaria y suficiente para la marcha de los servicios y procesos en cada uno de los sistemas informáticos.
- **Exactitud**: Asegurar que toda la información se encuentre libre de errores y/o irregularidades de cualquier tipo.
- **Disponibilidad**: Garantizar que la información y la capacidad de su procesamiento manual y automática, sean resguardadas y recuperadas eventualmente cuando sea necesario, de manera tal que no se interrumpa significativamente la marcha de los servicios.

4.1 COMPROMISO DE LA DIRECCION GENERAL

La Dirección General de LA COMPAÑÍA, demostrara su compromiso a través de:

- La revisión y aprobación del documento de política de seguridad de la información.
- La promoción activa de una cultura de seguridad dentro de LA COMPAÑÍA.
- La divulgación del contenido de esta política a través de la estructura Compañía.
- El uso de su autoridad para asegurar que existen los recursos adecuados para implementar y mantener la política de seguridad.

Declaración de cumplimiento.

Cada persona que desempeñe alguna labor para LA COMPAÑÍA**,** sin importar su condición (empleado, contratista, personal temporal, proveedor, socio de negocios, etc.) tiene la responsabilidad de cumplir lo estipulado en este documento y las políticas y los procedimientos relacionados, bien sea que esto aplique colectivamente o individualmente.

- Los empleados y personal temporal que no cumplan con lo establecido en estas directrices y otras declaraciones de la política de seguridad de información, serán objeto de las acciones disciplinarias definidas de acuerdo a lo establecido en el reglamento interno de trabajo capítulo XIV - ESCALA DE FALTAS Y SANCIONES DISCIPLINARÍAS, Articulo 48 literal g), soportado por el artículo 115 del código sustantivo del trabajo.
- Para los Contratistas, Proveedores y Socio de negocios que no cumplan con lo establecido en estas directrices y otras declaraciones de la política de seguridad de información, se aplicaran las sanciones correspondientes establecidas en cada contrato.

Fecha efectiva y revisiones al documento

Esta política será efectiva a partir de la fecha mencionada al inicio del documento y será revisada y actualizada anualmente o cuando existan cambios que lo ameriten previa revisión por parte del comité de seguridad de la información y el oficial de seguridad de la información, así mismo se entiende incorporada a los contratos que LA COMPAÑÍA celebre con empleados o contratistas.

Regulación

Cada persona que desarrolle una actividad en la compañía tiene la responsabilidad de cumplir lo estipulado en este documento y las políticas y los procedimientos relacionados, bien sea que esto aplique colectivamente o individualmente.

Quien no cumplan con lo establecido en estas directrices y otras declaraciones de la política de seguridad de información, serán objeto de las acciones disciplinarias definidas en LA COMPAÑÍA.

Las claves asignadas son intransferibles y personales, en caso de ser facilitadas a otras personas, se considera falta grave, causal de proceso disciplinario y sanciones.

Divulgación y aceptación de la política

Esta política una vez aprobada por la Dirección General de LA COMPAÑÍA, debe ser divulgada a todas las personas que desarrollen una actividad en la compañía, a través de los diferentes canales de comunicación disponibles y de capacitaciones periódicas, mínimo una vez por año, que permitan que los usuarios la conozcan, la entiendan y la acepten. Se debe garantizar la aceptación de esta política, mediante la firma de una carta de aceptación lo cual se realizara en los procesos de Inducción y reinducción.

4.2. POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

En LA COMPAÑÍA la información es un activo fundamental para la prestación exitosa de nuestros servicios de tercerización de procesos de negocios del sector asegurador del ciclo operativo completo; nuestro compromiso de protección de la información es parte de una estrategia orientada a la continuidad del negocio, la administración de riesgos y la consolidación de una cultura de seguridad, por tal motivo, aplicamos un modelo de gestión como la herramienta que permite: identificar y minimizar los riesgos a los cuales se expone la información, reducir los costos operativos y financieros, establecer una cultura de seguridad de la

información y garantizar el cumplimiento de los requerimientos legales, contractuales, regulatorios y de negocio vigentes.

Como parte del compromiso de mejora continua, todos los componentes del sistema de gestión de seguridad de la información serán parte del proceso periódico de revisión gerencial, o cuando se identifiquen cambios en contexto interno y/o externo de la organización, su estructura, sus objetivos o alguna condición que lo afecte, para asegurar su conveniencia, adecuación y eficacia.

LA COMPAÑÍA establecerá los mecanismos para respaldar la difusión, estudio, actualización y consolidación tanto de la presente política como de los demás componentes del Sistema de Gestión de la Seguridad de la Información y alinearlos de forma efectiva con los demás sistemas de gestión.

POLÍTICAS GENERALES PARA LA SEGURIDAD DE LA INFORMACIÓN

La Compañía ha establecido las siguientes políticas generales de Seguridad de la Información, las cuales representan la visión de LA COMPAÑÍA en cuanto a la protección de sus activos de Información:

1. Existirá un Comité de Seguridad de la Información, que será el responsable del mantenimiento, revisión y mejora del Sistema de Gestión de Seguridad de la Información de LA COMPAÑÍA.

2. Los activos de información de LA COMPAÑÍA, serán identificados y clasificados para establecer los mecanismos de protección necesarios.

3. LA COMPAÑÍA definirá e implementará controles para proteger la información contra violaciones de autenticidad, accesos no autorizados, la perdida de integridad y que garanticen la disponibilidad requerida por los clientes y usuarios de los servicios ofrecidos por LA COMPAÑÍA.

4. Cada persona que desarrolle una actividad en la compañía. serán responsables de proteger la información a la cual accedan y procesen, para evitar su pérdida, alteración, destrucción o uso indebido.

5. Se realizarán auditorías y controles periódicos sobre el modelo de gestión de Seguridad de la Información de LA COMPAÑÍA. El responsable de esta labor es el Oficial de Seguridad de la información y serán realizadas semestralmente y serán registradas en el formato FM-DR-DI-03 Programa de auditoria V2.

6. Únicamente se permitirá el uso de software autorizado que haya sido adquirido legalmente por LA COMPAÑÍA.

7. Es responsabilidad de todos los empleados y contratistas de LA COMPAÑÍA reportar los Incidentes de Seguridad, eventos sospechosos y el mal uso de los recursos que identifique de acuerdo al procedimiento PR-CS-PS-12-1 PROCEDIMIENTO DE RESPUESTA A INCIDENTES y el diligenciamiento del formato FM-CS-PS-12-1 FORMATO REPORTE DE INCIDENTES.

8. Las violaciones a las Políticas y Controles de Seguridad de la Información serán reportadas, registradas y monitoreadas de acuerdo al procedimiento PR-CS-PS-12-1 PROCEDIMIENTO DE RESPUESTA A INCIDENTES.

9. LA COMPAÑÍA contará con un Plan de Continuidad del Negocio que asegure la continuidad de las operaciones, ante la ocurrencia de eventos no previstos o desastres naturales.

Adicionalmente LA COMPAÑÍA cuenta con políticas específicas y un conjunto de estándares y procedimientos que soportan la política corporativa.

Segregación de tareas

[ISO/IEC 27001:2013 A.6.1.2]

Toda tarea en la cual los empleados tengan acceso a la infraestructura tecnológica y a los sistemas de información, debe contar con una definición clara de los roles y responsabilidades, así como del nivel de acceso y los privilegios correspondientes, con el fin de reducir y evitar el uso no autorizado o modificación sobre los activos de información de LA COMPAÑÍA.

En concordancia:

- Todos los sistemas de disponibilidad crítica o media de LA COMPAÑÍA, deben implementar las reglas de acceso de tal forma que haya segregación de tareas entre quien administre, opere, mantenga, audite y, en general, tenga la posibilidad de acceder a los sistemas de información, así como entre quien otorga el privilegio y quien lo utiliza.
- Los módulos ejecutables nunca deberán ser trasladados directamente de las librerías de pruebas a las librerías de producción sin que previamente sean compilados por el área asignada para tal efecto, que en ningún momento deberá ser el equipo encargado del desarrollo.
- El nivel de súper usuario de los sistemas debe tener un control dual, de tal forma que exista una supervisión a las actividades realizadas por el administrador del sistema.

Uso aceptable de los activos

[ISO/IEC 27001:2013 A.8.1.3]

El acceso a los documentos físicos y digitales estará determinado por las normas relacionadas con el acceso y las restricciones a los documentos de LA COMPAÑÍA, a la competencia del proceso específico y a los permisos y niveles de acceso de los empleados y contratistas determinadas por los dueños de cada proceso.

Para la consulta de documentos compartidos se establecerán privilegios de acceso a los empleados y/o contratistas de acuerdo con el desarrollo de sus funciones y competencias. Dichos privilegios serán establecidos por el dueño de cada proceso, quien comunicará al grupo encargado de la administración del software el listado con los empleados y sus privilegios.

Todos los empleados y terceros que manipulen información en el desarrollo de sus funciones deberán firmar un “acuerdo de confidencialidad de la información”, donde individualmente se comprometan a no divulgar, usar o explotar la información confidencial a la que tengan acceso, respetando los niveles establecidos para la clasificación de la información; y que cualquier violación a lo establecido en este parágrafo será considerando como un “incidente de seguridad”.

Acceso a Internet

El internet es una herramienta de trabajo que permite navegar en muchos otros sitios relacionados o no con las actividades propias del negocio de LA COMPAÑÍA, por lo cual el uso adecuado de este recurso se debe controlar, verificar y monitorear, considerando, para todos los casos, los siguientes lineamientos:

a) No está permitido:

- El acceso a páginas relacionadas con pornografía, drogas, alcohol, webproxys, hacking y/o cualquier otra página que vaya en contra de la ética moral, las leyes vigentes o políticas aquí establecidas.
- El acceso y el uso de servicios interactivos o mensajería instantánea como Facebook, Kazaa, MSN Messenger, Yahoo,Net2phone y otros similares, que tengan como objetivo crear comunidades para intercambiar información, o bien para fines diferentes a las actividades propias del negocio de LA COMPAÑÍA.
- Solo personal Autorizado por la Dirección y/o Gerencia podrá hacer uso del servicio Interactivo Skype porque su función y Rol.
- El intercambio no autorizado de información de propiedad de LA COMPAÑÍA, de sus clientes y/o de sus empleados, con terceros.
- La descarga, uso, intercambio y/o instalación de juegos, música, películas, protectores y fondos de pantalla, software de libre distribución, información y/o productos que de alguna forma atenten contra la propiedad intelectual de sus autores, o que contengan archivos ejecutables y/o herramientas que atenten contra la integridad, disponibilidad y/o confidencialidad de la infraestructura tecnológica (hacking), entre otros. La descarga, uso, intercambio y/o instalación de información audiovisual (videos e imágenes) utilizando sitios públicos en Internet debe ser autorizada por el dueño del proceso respectivo a quien deleguen de forma explícita para esta función, asociando los procedimientos y controles necesarios para el monitoreo y aseguramiento del buen uso del recurso.

b) LA COMPAÑÍA debe realizar monitoreo permanente de tiempos de navegación y páginas visitadas por parte de los empleados y/o terceros. Así mismo, puede inspeccionar, registrar y evaluar las actividades realizadas durante la navegación, de acuerdo a la legislación nacional vigente.

c) Cada uno de los usuarios es responsable de dar un uso adecuado a este recurso y en ningún momento puede ser usado para realizar prácticas ilícitas o mal intencionadas que atenten contra terceros, la legislación vigente y los lineamientos de seguridad de la información, entre otros.

d) Los empleados y terceros, al igual que los empleados o subcontratistas de estos, no pueden asumir en nombre de LA COMPAÑÍA, posiciones personales en encuestas de opinión, foros u otros medios similares.

e) El uso de Internet no considerado dentro de las restricciones anteriores, es permitido siempre y cuando se realice de manera ética, razonable, responsable, no abusiva y sin afectar la productividad ni la protección de la información de LA COMPAÑÍA.

Correo electrónico

Los empleados y terceros autorizados a quienes LA COMPAÑÍA les asigne una cuenta de correo deberán seguir los siguientes lineamientos:

a) La cuenta de correo electrónico debe ser usada para el desempeño de las funciones asignadas dentro de LA COMPAÑÍA, y se debe realiza de manera ética, razonable, responsable, no abusiva y sin afectar la productividad.

b) Los mensajes y la información contenida en los buzones de correo son propiedad de LA COMPAÑÍA y cada usuario, como responsable de su buzón, debe mantener solamente los mensajes relacionados con el desarrollo de sus funciones.

c) El tamaño de los buzones de correo es determinado por IT de acuerdo con las necesidades de cada usuario y previa autorización del dueño del proceso correspondiente.

d) El tamaño de envío y recepción de mensajes, sus contenidos y demás características propios de estos deberán ser definidos e implementados.

e) No es permitido:

- Enviar cadenas de correo, mensajes con contenido religioso, político, racista, sexista, pornográfico, publicitario no corporativo o cualquier otro tipo de mensajes que atenten contra la dignidad y la productividad de las personas o el normal desempeño del servicio de correo electrónico en LA COMPAÑÍA, mensajes mal intencionados que puedan afectar los sistemas internos o de terceros, mensajes que vayan en contra de las leyes, la moral y las buenas costumbres y mensajes que inciten a realizar prácticas ilícitas o promuevan actividades ilegales.
- Utilizar la dirección de correo electrónico de LA COMPAÑÍA como punto de contacto en comunidades interactivas de contacto social, tales como facebook y/o twitter entre otras, o cualquier otro sitio que no tenga que ver con las actividades laborales.
- Solo personal Autorizado tendrá, acceso a Google + para realizar procesos laborales que autorice la Dirección y/o Gerencia.
- El envío de archivos que contengan extensiones ejecutables, bajo ninguna circunstancia.
- El envío de archivos de música y videos. En caso de requerir hacer un envío de este tipo de archivos deberá ser autorizado por el dueño del proceso respectivo y IT.

f) El envío de información corporativa debe ser realizado exclusivamente desde la cuenta de correo que LA COMPAÑÍA proporciona. De igual manera, las cuentas de correo genéricas no se deben emplear para uso personal.

g) El envío masivo de mensajes publicitarios corporativos deberá contar con la aprobación de la Dirección General, incluir un mensaje que le indique al destinatario como ser eliminado de la lista de distribución. Si una dependencia debe, por alguna circunstancia, realizar envío de correo masivo, de manera frecuente, este debe ser enviado a través de la cuenta servicioalcliente@connect-sos.com a través de cuentas de correo electrónico asignadas a un usuario particular.

h) Toda información de LA COMPAÑÍA generada con los diferentes programas computacionales (Ej. Office, Project, Access, Wordpad, etc.), que requiera ser enviada fuera de la Entidad, y que por sus características de confidencialidad e integridad deba ser protegida, debe estar en formatos no editables, utilizando las características de seguridad que brindan las herramientas proporcionadas por IT. La información puede ser enviada en el formato original bajo la responsabilidad del usuario y únicamente cuando el receptor requiera hacer modificaciones a dicha información.

i) Todos los mensajes enviados deben respetar el estándar de formato e imagen corporativa definido por LA COMPAÑÍA y deben conservar en todos los casos el mensaje legal corporativo de confidencialidad y protección de datos. Conforme al Instructivo PR-DR-SI-01 Elaboración y control de documentos V 1.0.

Recursos tecnológicos

El uso adecuado de los recursos tecnológicos asignados por LA COMPAÑÍA a sus empleados y/o terceros se reglamenta bajo los siguientes lineamientos:

a) La instalación de cualquier tipo de software o hardware en los equipos de cómputo de LA COMPAÑÍA es responsabilidad de IT y por tanto son los únicos autorizados para realizar esta labor. Así mismo, los medios de instalación de software deben ser los proporcionados por LA COMPAÑÍA a través de esta Gerencia.
b) Cada vez que se requiera de la instalación de un nuevo software específico, se debe solicitar a través de la herramienta GLPI y debe ser autorizado el Coordinador, supervisan y/o Director del proceso.

c) Los usuarios no deben realizar cambios en las estaciones de trabajo relacionados con la configuración del equipo, tales como conexiones de red, usuarios locales de la máquina, papel tapiz y protector de pantalla corporativo, entre otros. Estos cambios pueden ser realizados únicamente por el Outsourcing de TI.

d) El Outsourcing de TI debe definir y actualizar, de manera periódica, la lista de software y aplicaciones autorizadas que se encuentran permitidas para ser instaladas en las estaciones de trabajo de los usuarios. Así mismo, realizar el control, alertas y verificación de cumplimiento del licenciamiento del respectivo software y aplicaciones asociadas.

e) Únicamente los empleados y terceros autorizados por el Outsourcing de TI, previa solicitud escrita por parte del proceso que lo requiera y conforme a las políticas de seguridad, pueden conectarse a la red inalámbrica de LA COMPAÑÍA.

f) La conexión a redes inalámbricas externas para usuarios con equipos portátiles que estén fuera de la oficina y que requieran establecer una conexión a la infraestructura tecnológica de LA COMPAÑÍA, deben utilizar una conexión bajo los esquemas y herramientas de seguridad autorizados y establecidos por la Dirección.

g) Si un tercero requiere tener conexión a internet, para desempeñar una función hacia la compañía, se le asignara un modem y está sujeto a disponibilidad del recurso.

h) Sólo personal autorizado puede realizar actividades de administración remota de dispositivos, equipos o servidores de la infraestructura de procesamiento de información de LA COMPAÑÍA; las conexiones establecidas para este fin, deben utilizar los esquemas y herramientas de seguridad y administración definidos por la Dirección.

i) La sincronización de dispositivos móviles, tales como PDAs, smartphones, celulares u otros dispositivos electrónicos sobre los que se puedan realizar

intercambios de información con cualquier recurso de LA COMPAÑÍA, debe estar autorizado de forma explícita por el proceso respectivo, en conjunto con el Outsourcing de TI y podrá llevarse a cabo sólo en dispositivos provistos por LA COMPAÑÍA, para tal fin.

Gestión de soportes extraíbles
[ISO/IEC 27001:2013 A.8.3.1]

El uso de medios de almacenamiento removibles (ejemplo: CDs, DVDs, USBs, memorias flash, discos duros externos, Ipods, celulares, cintas) sobre la infraestructura para el procesamiento de la información de LA COMPAÑÍA, estará autorizado para aquellos empleados cuyo perfil del cargo y funciones lo requiera.

El Outsourcing TI es responsable de implementar los controles necesarios para asegurar que en los sistemas de información de LA COMPAÑÍA sólo los empleados autorizados pueden hacer uso de los medios de almacenamiento removibles.

Así mismo, el empleado se compromete a asegurar física y lógicamente el dispositivo a fin de no poner en riesgo la información de LA COMPAÑÍA que éste contiene.

Control de acceso físico
[ISO/IEC 27001:2013 A.9.1]

Todas las áreas destinadas al procesamiento o almacenamiento de información sensible, así como aquellas en las que se encuentren los equipos y demás infraestructura de soporte a los sistemas de información y comunicaciones, se consideran áreas de acceso restringido. En consecuencia, deben contar con medidas de control de acceso físico en el perímetro tales que puedan ser auditadas, así como con procedimientos de seguridad operacionales que permitan proteger la información, el software y el hardware de daños intencionales o accidentales.

De igual forma, los centros de cómputo, cableado y cuartos técnicos de las oficinas deben contar con mecanismos que permitan garantizar que se cumplen los requerimientos ambientales (temperatura, humedad, etc.), especificados por

los fabricantes de los equipos que albergan y que pueden responder de manera adecuada ante incidentes como incendios e inundaciones.

Control de acceso a sistemas y aplicaciones
[ISO/IEC 27001:2013 A.9.4]

El acceso a plataformas, aplicaciones, servicios y en general cualquier recurso de información de LA COMPAÑÍA debe ser asignado de acuerdo a la identificación previa de requerimientos de seguridad y del negocio que se definan por las diferentes dependencias de LA COMPAÑÍA, así como normas legales o leyes aplicables a la protección de acceso a la información presente en los sistemas de información.

Los responsables de la administración de la infraestructura tecnológica de LA COMPAÑÍA asignan los accesos a plataformas, usuarios y segmentos de red de acuerdo a procesos formales de autorización los cuales deben ser revisados de manera periódica por el proceso de Auditoria Interna de LA COMPAÑÍA.

La autorización para el acceso a los sistemas de información debe ser definida y aprobada por el proceso propietario de la información, o quien ésta defina, y se debe otorgar de acuerdo con el nivel de clasificación de la información identificada, según la cual se deben determinar los controles y privilegios de acceso que se pueden otorgar a los empleados y terceros e implementada por la el Outsourcing de TI. No se deben utilizar las contraseñas predeterminadas por los proveedores y otros parámetros que el proveedor predetermine.
Cualquier usuario interno o externo que requiera acceso remoto a la red y a la infraestructura de procesamiento de información de LA COMPAÑÍA, sea por Internet, acceso telefónico, VPN o por otro medio, siempre debe estar autenticado y sus conexiones deberán utilizar cifrado de datos.

Gestión de contraseñas de usuario
[ISO/IEC 27001:2013 A.9.4.3]

Todos los recursos de información críticos de LA COMPAÑÍA tienen asignados los privilegios de acceso de usuarios con base en los roles y perfiles que cada empleado requiera para el desarrollo de sus funciones, definidos y aprobados por los procesos de negocio y administrados por el Outsourcing de TI.

Todo empleado o tercero que requiera tener acceso a los sistemas de información de LA COMPAÑÍA debe estar debidamente autorizado y debe acceder a dichos sistemas haciendo uso como mínimo de un usuario (ID) y contraseña (password) y se debe cambiar periódicamente cada 60 dias, para aplicativos con una clave fija debe ser única para el empleado o tercero . El usuario debe ser responsable por el buen uso de las credenciales de acceso asignadas.

Controles Criptográficos

[ISO/IEC 27001:2013 A.10.1]

LA COMPAÑÍA asegura el uso adecuado y efectivo de la criptografía para proteger la confidencialidad, autenticidad y/o integridad de la información.

Se deben utilizar controles criptográficos en los siguientes casos:

- Para la protección de claves de acceso a sistemas, datos y servicios.
- Para la transmisión de información clasificada, fuera del ámbito de la Organización.
- Para el resguardo de información, cuando así surja de la evaluación de riesgos realizada por el Propietario de la Información y el Responsable de Seguridad Informática.
- La política sobre uso, protección y duración de las claves criptográficas se realiza a través del directorio activo durante todo su ciclo de vida.
- Se adecua un canal denominado SFTP que permite compartir información de forma segura.

Protección y ubicación de los equipos

[ISO/IEC 27001:2013 A.11.2]

Los equipos que hacen parte de la infraestructura tecnológica de LA COMPAÑÍA tales como, servidores, equipos de comunicaciones y seguridad electrónica, centros de cableado, UPS, subestaciones eléctricas, aires acondicionados, plantas telefónicas, así como estaciones de trabajo y dispositivos de almacenamiento y/o comunicación móvil que contengan y/o brinden servicios de soporte a la información crítica de las dependencias, deben ser ubicados y protegidos adecuadamente para prevenir la pérdida, daño, robo o acceso no autorizado de los mismos. De igual manera, se debe adoptar los controles necesarios para mantener los equipos alejados de sitios que puedan tener riesgo de amenazas potenciales como fuego, explosivos, agua, polvo, vibración, interferencia electromagnética y vandalismo, entre otros.

Los empleados y terceros, incluyendo sus empleados o subcontratistas, que tengan acceso a los equipos que componen la infraestructura tecnológica de LA COMPAÑÍA no pueden fumar, beber o consumir algún tipo de alimento cerca de los equipos.

LA COMPAÑÍA mediante mecanismos adecuados monitoreará las condiciones ambientales de las zonas donde se encuentren los equipos (Centros de Cómputo).

Escritorio y pantalla limpia
[ISO/IEC 27001:2013 A.11.2.9]

Con el fin de evitar pérdidas, daños o accesos no autorizados a la información, todos los empleados de LA COMPAÑÍA deben mantener la información restringida o confidencial bajo llave cuando sus puestos de trabajo se encuentren desatendidos o en horas no laborales. Esto incluye: documentos impresos, CDs, dispositivos de almacenamiento USB y medios removibles en general. Adicionalmente, se requiere que la información sensible que se envía a las impresoras sea recogida de manera inmediata.

Todos los usuarios son responsables de bloquear la sesión de su estación de trabajo en el momento en que se retiren del puesto de trabajo, la cual se podrá desbloquear sólo con la contraseña del usuario. Cuando finalicen sus actividades, se deben cerrar todas las aplicaciones y dejar los equipos apagados.

Todas las estaciones de trabajo deberán usar el papel tapiz y el protector de pantalla corporativo, el cual se activará automáticamente después de cinco (5) minutos de inactividad y se podrá desbloquear únicamente con la contraseña del usuario.

Gestión de Cambios

[ISO/IEC 27001:2013 A.12.1.2]

LA COMPAÑÍA a través del área responsable establecerá, coordinará y controlará los cambios realizados en los activos de información tecnológicos y los recursos informáticos, asegurando que los cambios efectuados sobre la plataforma tecnológica, tanto el software operativo como los sistemas de información, serán debidamente autorizados por las áreas correspondientes. El Outsourcing de TI debe garantizar que todo cambio realizado a un componente de la plataforma tecnológica, el cual conlleve modificación de accesos, modificación o mantenimiento de software, actualización de versiones o modificación de parámetros, certifica y mantiene los niveles de seguridad existentes.

Se debe garantizar que todo cambio realizado sobre la plataforma tecnológica de LA COMPAÑÍA, quedará formalmente documentado desde su solicitud hasta su implantación cumpliendo con el procedimiento correspondiente. Los dueños o responsables de los activos de información tecnológicos y recursos informáticos deben solicitar formalmente los requerimientos de nuevas funcionalidades, servicios o modificaciones sobre sus sistemas de información. Los Administradores de los activos de información tecnológicos y recursos informáticos deben garantizar que las modificaciones o adiciones en las funcionalidades de los sistemas de información están soportadas por las solicitudes realizadas por los usuarios, siguiendo el procedimiento vigente para dicha acción.

Protección contra código malicioso

[ISO/IEC 27001:2013 A.12.2]

LA COMPAÑÍA establece que todos los recursos informáticos deben estar protegidos mediante herramientas y software de seguridad como antivirus, antispam, antispyware y otras aplicaciones que brindan protección contra código malicioso y prevención del ingreso del mismo a la red de LA COMPAÑÍA, en donde se cuente con los controles adecuados para detectar, prevenir y recuperar posibles fallos causados por código móvil y malicioso. Será responsabilidad del

Outsourcing de TI autorizar el uso de las herramientas y asegurar que estas y el software de seguridad no sean deshabilitados bajo ninguna circunstancia, así como de su actualización permanente.

Así mismo, LA COMPAÑÍA define los siguientes lineamientos:

a) No está permitido:

- La desinstalación y/o desactivación de software y herramientas de seguridad avaladas previamente por LA COMPAÑÍA.
- Escribir, generar, compilar, copiar, propagar, ejecutar o intentar introducir cualquier código de programación diseñado para auto replicarse, dañar o afectar el desempeño de cualquier dispositivo o infraestructura tecnológica.
- Utilizar medios de almacenamiento físico o virtual que no sean de carácter corporativo.
- El uso de código móvil. Éste sólo podrá ser utilizado si opera de acuerdo con las políticas y normas de seguridad definidas y debidamente autorizadas la Dirección.

Copias de respaldo

[ISO/IEC 27001:2013 A.12.3]

LA COMPAÑÍA debe asegurar que la información con cierto nivel de clasificación, definida en conjunto por la Gerencia TI y los procesos responsables de la misma, contenida en la plataforma tecnológica de la Institución, como servidores, dispositivos de red para almacenamiento de información, estaciones de trabajo, archivos de configuración de dispositivos de red y seguridad, entre otros, sea periódicamente resguardada mediante mecanismos y controles adecuados que garanticen su identificación, protección, integridad y disponibilidad. Adicionalmente, se deberá establecer un plan de restauración de copias de seguridad que serán probados a intervalos regulares con el fin de asegurar que son confiables en caso de emergencia y retenidas por un periodo de tiempo determinado.

La Dirección establecerá procedimientos explícitos de resguardo y recuperación de la información que incluyan especificaciones acerca del traslado, frecuencia,

identificación y definirá conjuntamente con cada uno de los procesos los períodos de retención de la misma. Adicionalmente, debe disponer de los recursos necesarios para permitir la identificación relacionada de los medios de almacenamiento, la información contenida en ellos y la ubicación física de los mismos para permitir un rápido y eficiente acceso a los medios que contienen la información resguardada.

Los medios magnéticos que contienen la información crítica deben ser almacenados en otra Disco diferente a las instalaciones donde se encuentra dispuesta. El sitio externo donde se resguardan dichas copias, debe tener los controles de seguridad adecuados, cumplir con máximas medidas de protección y seguridad física apropiados.

Registros de actividad y supervisión
[ISO/IEC 27001:2013 A.12.4]

LA COMPAÑÍA establecerá los lineamientos para registrar eventos y generar evidencia, con el fin de identificar situaciones o incidentes de seguridad sobre los sistemas informáticos de LA COMPAÑÍA.

Se producirán revisiones regulares y cuidadosas a los registros de eventos que se graban de las actividades del usuario, excepciones, fallas y eventos de seguridad de la información y se protegerán contra la manipulación y el acceso no autorizado.

Las actividades del administrador del sistema y de la red serán registradas y estos registros serán protegidos y regularmente revisados.
Los relojes de todos los sistemas informáticos relevantes serán sincronizados a una fuente de tiempo de referencia única.

Esta supervisión se debe realizar periódicamente para garantizar el buen manejo de los registros a cargo de Oficial de Seguridad.

Gestión de vulnerabilidades técnicas
[ISO/IEC 27001:2013 A.12.6.1]

La información sobre las vulnerabilidades técnicas de los sistemas de información que se utilizan, se obtendrán en el momento oportuno, la exposición de la entidad a tales vulnerabilidades será evaluada y se tomaran las medidas pertinentes para hacer frente a los riesgos asociados.

La Auditoria de vulnerabilidades se debe realizar semestralmente. Para garantizar la seguridad de la información

Los reportes de auditoria al identificar las vulnerabilidades, se debe realizar las respectivas correcciones, el responsable de este proceso es el área TI.
Al realizar las correcciones se enviara notificación al Auditor para realizar nuevamente las pruebas de Vulnerabilidades.

Controles de red
[ISO/IEC 27001:2013 A.13.1.1]

Las redes deberán ser administradas y controladas para proteger la información en los sistemas y aplicaciones de acuerdo a los procedimientos establecidos en LA COMPAÑÍA.

Mecanismos de seguridad asociados a servicios en red
[ISO/IEC 27001:2013 A.13.1.2]

Los mecanismos de seguridad, niveles de servicio y los requisitos de gestión de todos los servicios de la red deben ser identificados e incluidos en los acuerdos de servicios de red.

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

La plataforma tecnológica de LA COMPAÑÍA que soporta los sistemas de Información debe estar separada en segmentos de red físicos y lógicos e independientes de los segmentos de red de usuarios, de conexiones con redes con terceros y del servicio de acceso a Internet. La división de estos segmentos debe ser realizada por medio de dispositivos perimetrales e internos de

enrutamiento y de seguridad si así se requiere. El Outsourcing de TI es el encargado de establecer el perímetro de seguridad necesario para proteger dichos segmentos, de acuerdo con el nivel de criticidad del flujo de la información transmitida.

LA COMPAÑÍA establece mecanismos de identificación automática de equipos en la red, como medio de autenticación de conexiones, desde segmentos de red específicos hacia las plataformas donde operan los sistemas de información de LA COMPAÑÍA.

Es responsabilidad de los administradores de recursos tecnológicos garantizar que los puertos físicos y lógicos de diagnóstico y configuración de plataformas que soporten sistemas de información deban estar siempre restringidos y monitoreados con el fin de prevenir accesos no autorizados.

Intercambio de información
[ISO/IEC 27001:2013 A.13.2]

LA COMPAÑÍA firmará acuerdos de confidencialidad con los empleados, clientes y terceros que por diferentes razones requieran conocer o intercambiar información restringida o confidencial de la Institución. En estos acuerdos quedarán especificadas las responsabilidades para el intercambio de la información para cada una de las partes y se deberán firmar antes de permitir el acceso o uso de dicha información.

Todo empleadode LA COMPAÑÍA es responsable por proteger la confidencialidad e integridad de la información y debe tener especial cuidado en el uso de los diferentes medios para el intercambio de información que puedan generar una divulgación o modificación no autorizada.

Los propietarios de la información que se requiere intercambiar son responsables de definir los niveles y perfiles de autorización para acceso, modificación y eliminación de la misma y los custodios de esta información son responsables de implementar los controles que garanticen el cumplimiento de los criterios de confidencialidad, integridad, disponibilidad y requeridos.

Acuerdos de confidencialidad y secreto
[ISO/IEC 27001:2013 A.13.2.4]

Todos los empleados de LA COMPAÑÍA y/o terceros deben aceptar los acuerdos de confidencialidad definidos por LA COMPAÑÍA, los cuales reflejan los compromisos de protección y buen uso de la información de acuerdo con los criterios establecidos en ella.

Para el caso de contratistas, los respectivos contratos deben incluir una cláusula de confidencialidad, de igual manera cuando se permita el acceso a la información y/o a los recursos de LA COMPAÑÍA, personas o entidades externas.

Estos acuerdos deben aceptarse por cada uno de ellos como parte del proceso de contratación, razón por la cual dicha cláusula y/o acuerdo de confidencialidad hace parte integral de cada uno de los contratos.

Análisis y especificación de los requisitos de seguridad
[ISO/IEC 27001:2013 A.14.1.1]

La inclusión de un nuevo producto de hardware, software, aplicativo, desarrollo interno o externo, los cambios y/o actualizaciones a los sistemas existentes en LA COMPAÑÍA, deben estar acompañados de la identificación, análisis, documentación y aprobación de los requerimientos de seguridad de la información, labor que debe ser responsabilidad de la Gerencia TI y los procesos propietarios del sistema en cuestión.

Los requerimientos de seguridad de la información identificados, obligaciones derivadas de las leyes de propiedad intelectual y derechos de autor deben ser establecidos en los acuerdos contractuales que se realicen entre LA COMPAÑÍA y cualquier proveedor de productos y/o servicios asociados a la infraestructura de procesamiento de información. Es responsabilidad del Outsourcing de TI garantizar el cumplimiento de los requerimientos de seguridad de la Información conforme han sido aprobados por la Dirección General estableciendo estos aspectos con las obligaciones contractuales específicas.

Seguridad en los procesos de desarrollo y soporte
[ISO/IEC 27001:2013 A.14.2]

LA COMPAÑÍA garantiza que la seguridad informática diseñada e implementada se cumpla durante el ciclo de vida de desarrollo de sistemas de información, para lo cual se establecerán y aplicarán reglas para el desarrollo de software.

Los cambios en los sistemas dentro del ciclo de desarrollo deberán cumplir los procedimientos formales de control de cambios establecidos. Cuando se cambian las plataformas de operación, las aplicaciones críticas deberán ser revisadas y probadas para asegurar que no hay impacto negativo en las operaciones de LA COMPAÑÍA o de la seguridad.

Las modificaciones a paquetes de software serán definidas y limitadas a cambios necesarios y todos los cambios estrictamente serán controlados, donde se apliquen los principios para ingeniería de sistemas segura, se documentará, y aplicara en la implementación de cualquier sistema de información.

El proceso IT debe definir y establecer formalmente la documentación requerida en las diferentes etapas de ciclo de vida de los sistemas y contar con un grupo de personas el cual debe autorizar la creación, adaptación o adquisición de software.

Los contratos de consultoría y en general todo tipo de contratos de servicios deben contener provisiones a este respecto. De igual manera, dada la proliferación del “outsourcing”, es especialmente importante clarificar los derechos generados por proveedores en desarrollo de este tipo de contratos.

Tratamiento de seguridad dentro de los acuerdos con proveedores
[ISO/IEC 27001:2013 A.15.1.2]

LA COMPAÑÍA identifica los posibles riesgos que pueden generar el acceso, procesamiento, comunicación o gestión de la información y la infraestructura para su procesamiento por parte de los terceros, con el fin de establecer los mecanismos de control necesarios para que la seguridad se mantenga.
Los controles que se establezcan como necesarios a partir del análisis de riesgos, deben ser comunicados y aceptados por el tercero mediante la firma de acuerdos, previamente a la entrega de los accesos requeridos.

Cumplimiento de los requisitos legales y contractuales
[ISO/IEC 27001:2013 A.18.1]

Evitar el incumplimiento de las obligaciones legales, estatutarias, reglamentarias o contractuales relacionadas con la seguridad de la información y de los requisitos de seguridad.

Las situaciones o acciones que violen la presente Política deben ser detectadas, registradas, analizadas, resueltas y reportadas de manera inmediata a través de los canales señalados para el efecto.

Se entenderán incluidas a la Política las regulaciones nacionales e internacionales que de tiempo en tiempo se expidieren y que se relacionen con la misma.

Cuando de la aplicación de tales normas se presentare un conflicto, se entenderá que aplica la más restrictiva, es decir, aquella que exija el mayor grado de seguridad.

Así mismo y con el fin de mantener un nivel de seguridad adecuado con LA COMPAÑÍA, esta Política se debe apoyar en las mejores prácticas de seguridad de la información y aquellas que el mercado y LA COMPAÑÍA reconozcan como tal.

La Política junto con el Proceso IT debe ser auditada anualmente para verificar su nivel, actualidad, aplicación, completitud y cumplimiento.

La información de auditoría generada por el uso de los controles de seguridad de los recursos de tecnología, debe ser evaluada por el responsable para:

- Detectar Violaciones a la Política.
- Reportar incidentes de seguridad.
- Constatar que los datos registrados incluyen evidencias suficientes para el seguimiento y resolución de incidentes de seguridad.

Periódicamente se debe evaluar el cumplimiento de los requerimientos de seguridad por parte de los Usuarios. El incumplimiento de los requerimientos de seguridad, se debe registrar como un incidente a la Política de Seguridad de la

información que debe ser resuelto de acuerdo con los procedimientos de manejo de incidentes de LA COMPAÑÍA.

Deben establecerse procedimientos apropiados para asegurar el cumplimiento con las restricciones de carácter legal en el uso de material que puede estar sujeto a derechos de propiedad intelectual tales como derechos de autor y derechos de diseño.

Todos los requisitos pertinentes, legislativos estatutarios, reglamentarios y contractuales, y el planteamiento de LA COMPAÑÍA para cumplir con estos requisitos deberán estar explícitamente identificados, documentados y protegidos al día para cada sistema de información.

Se aplicarán procedimientos apropiados para garantizar el cumplimiento de requisitos legales, reglamentarios y contractuales, relacionados con los derechos de propiedad intelectual y uso de productos de software propietario.
Se debe establecer en los contratos de trabajo de empleados y en los contratos de desarrollo realizados por proveedores y contratistas, cláusulas respecto a la propiedad intelectual de LA COMPAÑÍA, al material y productos generados en el desarrollo del negocio.

Los registros deben estar protegidos contra pérdida, destrucción, falsificación, acceso no autorizado y divulgación no autorizada, de conformidad con los requisitos de legalidad, reglamentarias, contractuales y comerciales.
Se garantizará la privacidad y la protección de la información de identificación personal a lo dispuesto en la legislación y la reglamentación pertinente en su caso.

Los controles criptográficos serán utilizados en cumplimiento a todos los acuerdos pertinentes, la legislación y los reglamentos.

Revisiones de la Seguridad de la Información
[ISO/IEC 27001:2013 A.18.2]

LA COMPAÑÍA garantiza que la seguridad informática sea implementada y aplicada de acuerdo con las políticas y procedimientos establecidos.

El enfoque de LA COMPAÑÍA para la gestión de seguridad de la información y su aplicación (es decir, los objetivos de control, controles, políticas, procesos y

procedimientos para la seguridad de la información) se revisará de forma independiente a intervalos planificados o cuando se produzcan cambios significativos.

Los procesos deberán comprobar periódicamente el cumplimiento de los procedimientos de procesamiento de la información dentro de su área de responsabilidad con las políticas de seguridad, las normas y otros requisitos de seguridad.
Los sistemas de información deben ser revisados regularmente para cerciorarse que se da cumplimiento a las políticas y normas de seguridad de la información de LA COMPAÑÍA.

Las situaciones o acciones que violen la presente Política deben ser detectadas, registradas, analizadas, resueltas e informadas al comité de Seguridad de la Información y a las áreas responsables por su tratamiento de manera inmediata.

4.3 Política de dispositivos móviles

1) Los dispositivos móviles autorizados para contener, administrar o manejar información privada y/o confidencial de la compañía son aquellos que hacen parte del inventario de la compañía y que son controlados por la gerencia de LA COMPAÑÍA y el Outsourcing de IT.

2) Los equipos de escritorio, portátiles o dispositivos tecnológicos que almacenen información confidencial deben estar protegidos con mecanismos de seguridad para evitar que ante la pérdida del equipo una persona no autorizada pueda acceder a la información almacenada en estos.

Los celulares Deben contar con clave y bloqueo automático.

3) Todas las estaciones de trabajo, dispositivos extraíbles y demás recursos tecnológicos son asignados a un responsable, por lo cual es su compromiso hacer uso adecuado y eficiente de dichos recursos.

4) Los equipos deben marcarse para su identificación y control de inventario. Los registros de inventario deben mantenerse actualizados.

5) No será permitido la instalación de cualquier software sin la debida autorización de LA COMPAÑÍA.

6) Existe un listado de dispositivos móviles corporativos autorizados para ser retirados de la compañía.

7) Adicional a esto los usuarios deben:

   a) Evitar usar los dispositivos móviles corporativos en lugares que no les ofrezcan las garantías de seguridad física necesarias para evitar pérdida o robo de estos.

   b) No modificar las configuraciones de seguridad, software o hardware de los dispositivos móviles corporativos bajo su responsabilidad.

   c) Evitar la instalación de programas desde fuentes desconocidas; se deben instalar aplicaciones únicamente desde los repositorios oficiales de los dispositivos móviles corporativos.

   d) No hacer uso de redes inalámbricas de uso público, así como deben desactivar las redes inalámbricas como WiFi, Bluetooth, o infrarrojos en los dispositivos móviles corporativos asignados.

   e) No conectar los dispositivos móviles corporativos asignados por puerto USB a cualquier computador público, de hoteles o cafés internet, entre otros.

f) No almacenar videos, fotografías o información personal en los dispositivos móviles corporativos asignados.

8) Para el ingreso a la oficina de un dispositivo móvil no propiedad de LA COMPAÑÍA se debe:

a) Registrar en la recepción indicando fecha/hora de ingreso/salida y motivo por el cual se trae el dispositivo, según formato de control establecido. No aplica para celulares.

b) Los equipos nuevos debe ser revisado por el área de infraestructura para validar tipo de dispositivo y niveles de seguridad para autorizar la conexión a la red de LA COMPAÑÍA.
Los equipos personales no tienen autorización para conectarse a la red de la compañía ni conexión inalámbrica deberán contar con su propia herramienta de conexión.

c) No está autorizada la conexión a los recursos tecnológicos de la compañía los dispositivos móviles de los empleados.

d) Es prohibido el Ingreso se de dispositivos móviles a áreas restringidas de la compañía. Los dispositivos deberán dejarse en el casilleros de los funcionarios y par los terceros se encuentra ubicado un casillero en el hall de acceso a las áreas restringidas

4.4 Política de teletrabajo

LA COMPAÑÍA autoriza el trabajo fuera de las sedes o instalaciones físicas a los cargos:

AREA	CARGO
Dirección	Gerencia
Canal Presencial	Gestores Comerciales
Canal Presencial	Especialistas de Producto
Canal Presencial	Supervisores de Ventas

Cumpliendo los siguientes parámetros:

1) El horario autorizado para el teletrabajo es 7*24

2) Solo se autoriza el teletrabajo desde equipos de cómputo asignados por LA COMPAÑÍA o aquellos autorizados por seguridad de la información.

3) La conexión al escritorio virtual únicamente se debe realizar desde la VPN que asigne LA COMPAÑÍA

4) No está autorizado el uso de sistemas de almacenamiento en la nube

5) Las licencias de los equipos de cómputo asignados para el teletrabajo son propiedad de LA COMPAÑÍA, por tanto no se autoriza la instalación de otras licencias.

6) No se autoriza salida o intercambio de información física para efectos de teletrabajo.

7) La conexión se debe realizar desde sitios seguros, preferiblemente desde redes domésticas.

8) Al retirar el equipo de la compañía debe velar por su cuidado no exponiéndolo ni abandonándolo en lugares públicos o privados, y en viajes debe siempre tenerlo consigo llevándolo como equipaje de mano y nunca almacenándolo en la bodega de carga.

9) Todo uso indebido de la información y del entorno físico es responsabilidad del empleado.

CUADRO DE CONTROL				
	CARGO	*NOMBRE*	*FECHA*	*FIRMA*
ELABORADO POR:	CONSULTOR SI IDENTIAN S.A.S.	LUIS CARLOS AMAYA	11/04/2016	
REVISADO POR	COORDINADOR SISTEMA INTEGRAL DE GESTION	ANDREA MORENO	16/06/2017	
APROBADO POR	GERENTE	LUZ AIDA VEGA		

CONTROL DE CAMBIOS			
VERSIÓN	*REVISIÓN*	*FECHA*	*DESCRIPCIÓN DEL CAMBIO*
3.0	Yuri Andrea Moreno.	30/03/2017	En declaración de Cumplimiento se registra el código Disciplinario. Se completa la Política Dispositivos Móviles. Se actualiza la Política recursos Tecnológicos.