SITCAR S.A.

Soluciones Integrales De Tránsito Y Transporte

SEGURIDAD DE LA INFORMACIÓN.

Política para la seguridad de la información de SITCAR S.A.

TERMINOS Y CONDICIONES DE USO

Versión actual del documento: 1.0.0

El contenido de este texto es PRIVADO y la presente versión se considera un documento interno de trabajo.

NO SE AUTORIZA LA REPRODUCCIÓN O DIFUSION POR NINGÚN MEDIO O MECANISMO SIN EL DEBIDO CONTROL Y AUTORIZACIÓN DE LA OFICINA ASESORA DE SISTEMAS.

Contenido

1 INTRODUCCIÓN 6
2 ACERCA DE LA SEGURIDAD DE LA INFORMACIÓN. 7
3 CONCEPTOS BÁSICOS 8
4 POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN 11
4.1 Generalidades 11
4.2 Alcance 11
4.3 Objetivos 11
5 POLÍTICAS GENERALES 12
6 LINEAMIENTOS OPERACIONALES O ESPECÍFICOS PARA LA SEGURIDAD DE LA INFORMACIÓN 14
6.1 Organización para la seguridad de la información 14
6.1.1 Roles y responsabilidades en la seguridad de la información 15
6.2 Políticas para uso de dispositivos móviles. 18
6.3 Políticas de uso de internet 19
6.4 Políticas de dispositivos informáticos, medios y equipos 20
6.5 Políticas de usos de Activos de información 21
6.6 Políticas de seguridad para los recursos humanos. 24
6.7 Políticas de uso de estaciones cliente 25
6.8 Políticas de establecimiento, uso y protección de claves de acceso 26
6.9 Políticas de respaldo y restauración de información 27
6.10 Políticas para la realización de copias en los computadores de usuario final 28
6.11 Políticas de uso de puntos de red de datos (red de área local – LAN) 29
6.12 Políticas de administración de las comunicaciones y operaciones. 30
6.12.1 Protección contra software maliciosos y hacking 30
6.12.2 Reporte e investigación de incidentes de seguridad 30
7 PROCESO DISCIPLINARIO 31
8 CUMPLIMIENTO 34
9 REFERENCIAS 34

1 INTRODUCCIÓN

En la actualidad la información de la compañía se ha reconocido como un activo valioso, y a medida que los sistemas de información apoyan cada vez más los procesos de misión crítica se requiere contar con estrategias de alto nivel que permitan el control de administración efectiva de los datos. Nuestra compañía, los sistemas y red de información enfrentan amenazas de seguridad que incluyen, entre muchas otras: el fraude por computadora, espionaje, vandalismo, suplantación de identidad y robo. Las posibilidades de daño y pérdida de información por causa de código malicioso, mal uso o ataques de denegación de servicio se hacen cada vez más comunes.

La entidad define sus necesidades para el cumplimiento de sus requerimientos hacia un grupo interesados, por medio de controles precisos para mantener la seguridad de la información, estableciendo políticas, teniendo en cuenta el marco general del funcionamiento de la compañía.

Con la promulgación de la presente Política de Seguridad de la Información la compañía SITCAR S.A., (Soluciones Integrales de Tránsito y Transporte) formaliza su compromiso con el proceso de gestión responsable de información que tiene como objetivo garantizar la integridad, confidencialidad y disponibilidad de este importante activo, teniendo como eje el cumplimiento de los objetivos misionales.

2 ACERCA DE LA SEGURIDAD DE LA INFORMACIÓN.

La seguridad de la información, según la ISO 27001 se refiere al cumplimiento de las siguientes características:

- **Confidencialidad:** Todo activo solo pueden ser accedidos y custodias únicamente por el personal autorizado.

- **Integridad:** Los datos de los activos debe permanecer inalterado, legible y completo. Las modificaciones que se realicen deben ser registradas y asegurados su confiabilidad.

- **Disponibilidad:** Los activos de información solo pueden ser obtenidos a corto plazo por los usuarios que tengan los permisos adecuados.

- **Autenticidad:** La información de los activos verificados por un usuario que garantice que los datos sean correctos.

Para ello es necesario considerar los siguientes aspectos:

- **Posibilidad de auditoria:** Se posee evidencias digitales y/o físicas de actividades y acciones cuando se requiera un activo de información.

- **Protección a la duplicación:** Los activos de información son objeto de clasificación, y se llevan registro único y cualquier duplicidad se suprime.

- **No repudio:** Los autores, propietarios y custodios de los activos de información se pueden identificar plenamente.

- **Legalidad:** Los activos de información cumplen los parámetros legales, normativos y estatutarios de la institución.

- **Confiabilidad de la información:** Es fiable el contenido de los activos de información que conserven la confidencialidad, integridad, disponibilidad, autenticidad y legalidad.

3 CONCEPTOS BÁSICOS

Los siguientes conceptos corresponden al Modelo de Seguridad y Privacidad de la Información, según establecido en el decreto 1078 de 2016 a través del CONPES 3854 con el fin de reforzar las capacidades para "identificar, gestionar, tratar y mitigar los riesgos de seguridad digital" en las actividades socioeconómicas del entorno digital. La conceptualización de esta política se fundamenta en la Norma Técnica Colombiana NTC/ISO 27001:2013 Sistemas de gestión de la seguridad de la información.

- **Activo:** En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de esta (sistemas, soportes, edificios, personas…) que tenga valor para la organización. (ISO/IEC 27001).

- **Activo de Información:** Se refiere al activo que contiene información pública que el sujeto obligado genere, obtenga, adquiera, transforme o controle en su calidad de tal.

  Activo de información es todo recurso por medio del cual se almacena, procesa, transmite, divulga, comunica, intercambia, presenta y genera la información, de igual manera la información.

- **Archivo:** Conjunto de documentos, sea cual fuere su fecha, forma y soporte material, acumulados en un proceso natural por una persona o entidad pública o privada, en el transcurso de su gestión, conservados respetando aquel orden para servir como testimonio e información a la persona o institución que los produce y a los ciudadanos, o como fuentes de la historia. También se puede entender como la institución que está al servicio de la gestión administrativa, la información, la investigación y la cultura. (Ley 594 de 2000, art 3)

- **Amenazas:** Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización. (ISO/IEC 27000).

- **Análisis de Riesgo:** Proceso para comprender la naturaleza del riesgo y determinar el nivel de riesgo. (ISO/IEC 27000). Gestión de incidentes de seguridad de la información: Procesos para detectar, reportar, evaluar, responder, tratar y aprender de los incidentes de seguridad de la información. (ISO/IEC 27000).

- **Información Pública Clasificada:** Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, pertenece al

ámbito propio, particular y privado o semiprivado de una persona natural o jurídica por lo que su acceso podrá ser negado o exceptuado, siempre que se trate de las circunstancias legítimas y necesarias y los derechos particulares o privados consagrados en el artículo 18 de la Ley 1712 de 2014. (Ley 1712 de 2014, art 6).

- **Información Pública Reservada:** Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, es exceptuada de acceso a la ciudadanía por daño a intereses públicos y bajo cumplimiento de la totalidad de los requisitos consagrados en el artículo 19 de la Ley 1712 de 2014. (Ley 1712 de 2014, art 6).

- **Riesgo:** Efecto de la incertidumbre sobre los objetivos. Un efecto es una desviación respecto a lo previsto. Puede ser positivo, negativo o ambos, y puede abordar, crear o resultar en oportunidades y amenazas. Los objetivos pueden tener diferentes aspectos y categorías (por ejemplo: financieros, salud y seguridad, y metas ambientales) y se pueden aplicar a niveles diferentes (estratégico, en toda la organización, en proyectos, productos y procesos).

  A menudo el riesgo está caracterizado por la referencia a los eventos potenciales y las consecuencias o a una combinación de ellos.

  Con frecuencia, el riesgo se expresa en términos de fuentes de riesgo, eventos potenciales, sus consecuencias y sus probabilidades.

  Incertidumbre es el estado, incluso parcial, de deficiencia de información relacionada con la comprensión o el conocimiento de un evento, su consecuencia o probabilidad.

- **Riesgo de seguridad digital:** Combinación de amenazas y vulnerabilidades en el entorno digital. Puede debilitar el logro de objetivos económicos y sociales, así como afectar la soberanía nacional, la integridad territorial, el orden constitucional y los intereses nacionales. Incluye aspectos relacionados con el ambiente físico, digital y las personas.

  ISO/IEC 27000 - Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias.

- **Seguridad de la información:** Preservación de la confidencialidad, integridad, y disponibilidad de la información. (ISO/IEC 27000).

- **Sistema de Gestión de Seguridad de la Información SGSI:** Conjunto de elementos interrelacionados o interactuantes (estructura organizativa, políticas, planificación de actividades, responsabilidades, procesos, procedimientos y recursos) que utiliza una organización para establecer una política y unos objetivos de seguridad de la información y alcanzar dichos objetivos, basándose en un enfoque de gestión y de mejora continua. (ISO/IEC 27000).

- **Transformación Digital para Todos (TDxT):** Es la estrategia del Ministerio de las TIC que busca acompañar a las entidades públicas del orden nacional y territorial para impulsar su nivel de madurez digital a través de la adopción de soluciones tipo y en consecuencia, su capacidad de entregar los servicios del Estado de manera efectiva a los ciudadanos.

4 POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

4.1 Generalidades

La información es un recurso, como el resto de los activos es un valor importante para la compañía, y por consiguiente debe ser debidamente protegida.

La compañía está comprometida con el seguimiento, mejora continua y aplicación de nuevas políticas de seguridad de la información, garantizando la protección de la alta serie de amenazas que se presenta en el mundo digital. Con esta política se contribuye en mitigar los riesgos o daños y se asegura el eficiente cumplimiento de las funciones sustantivas de la compañía disponiendo de un correcto sistema de la información.

4.2 Alcance

Esta política es para la aplicación en conjunto con dependencias que componen la compañía, a sus recursos, a la totalidad de los procesos internos o externos vinculados a SITCAR S.A., a través de contratos o acuerdos con terceros y a todo el persona, cualquier sea su situación contractual, la dependencia a la cual se encuentre adscrito y el nivel de las tareas que desempeñe.

4.3 Objetivos

- Proteger, preservar y administrar la información de SITCAR S.A., junto con las tecnologías, frente a amenazas internas o externas, deliberadas o accidentales, con el fin de asegurar el cumplimiento de los características de confidencialidad, integridad, disponibilidad, legalidad,confiabilidad y no repudio de la información.

- Definir las directrices de SITCAR S.A., para la correcta valoración, análisis y evaluación de los riesgos de seguridad asociados a la información y su impacto, identificando y evaluando diferentes opciones para su tratamiento con el fin de garantizar la continuidad e integridad de los sistemas de información.

- Proteger la confidencialidad de los activos de información relacionada con los clientes y con los planes de desarrollo.

5 POLÍTICAS GENERALES

A continuación, se establecen las políticas generales de seguridad de información que soportan el Sistema de Gestión de Seguridad de la Información de SITCAR S.A:

- SITCAR S.A., ha decidido definir, implementar, operar y mejorar de forma continua un Sistema de Gestión de Seguridad de la Información, soportado en lineamientos claros a las necesidades de la entidad, y a los requerimientos regulatorios que le aplican a su naturaleza. •

- Las responsabilidades frente a la seguridad de la información serán definidas, compartidas y aceptadas por cada uno de los funcionarios, contratistas o terceros.

- SITCAR S.A., protegerá la información accedida, procesada, transportada, almacenada, presentada, comunicada y divulgada por los procesos, con el fin de minimizar los impactos negativos y de tipo financiero, legal, operativo o reputaciones como consecuencia de incidentes de seguridad de la información para lo cual se implementarán controles como mecanismos de tratamiento del correspondiente riesgo.

- SITCAR S.A., protegerá su información de las amenazas originadas por parte del personal.

- SITCAR S.A., Adaptación implementa controles para la protección de las instalaciones de procesamiento y la infraestructura tecnológica que soporta sus procesos.

- SITCAR S.A., implementa los controles para cumplir con los niveles requeridos por esta, para la seguridad de los recursos tecnológicos y la red de datos.

- SITCAR S.A., implementa controles de acceso a la información, sistemas y recursos de red.

- SITCAR S.A., la mejora continua de la seguridad y privacidad de la información a través de una adecuada gestión de los eventos de seguridad y las debilidades asociadas.

- SITCAR S.A., garantizará el cumplimiento de las obligaciones legales, regulatorias y contractuales establecidas.

El incumplimiento a la política de Seguridad y Privacidad de la Información traerá consigo, las consecuencias legales que apliquen a la normativa de la compañía, incluyendo lo establecido en las normas que competen al Gobierno nacional y territorial en cuanto a Seguridad y Privacidad de la Información se refiere.

La presente política debe ser revisada y actualizada anualmente o cuando el Líder de Seguridad de la Información lo determine, teniendo como criterios los cambios relevantes en el contexto interno y externo, cuando la identificación de nuevos riesgos de seguridad de la información lo requiera o cuando el marco legal que regula las políticas nacionales en materia de Seguridad de la Información, Seguridad Digital o Gobierno Digital lo demanden.

Las peticiones de información por parte de entes externos de control deben ser aprobadas por la Vicerrectoría Administrativa y Financiera de ambas partes, y dirigida por dichos entes a los responsables de su custodia.

Toda la información de la compañía debe ser manejada de acuerdo a la legislación.

6 LINEAMIENTOS OPERACIONALES O ESPECÍFICOS PARA LA SEGURIDAD DE LA INFORMACIÓN

Estos lineamientos se establecen de acuerdo con los activos de información de la compañía, los procesos y los servicios de información que presenta SITCAR S.A., enmarcados dentro del proceso de gestión de TI.

6.1 Organización para la seguridad de la información

SITCAR S.A., garantiza el apoyo al proceso de establecimiento, implementación, operación, seguimiento, revisión, mantenimiento y mejora del Sistema de Gestión de la Seguridad de la Información, del cual hace parte integral la presenta política, por medio de la creación de una comisión técnica denominada área de Seguridad de la Información cuya composición y funciones serán reglamentadas por una mesa de trabajo compuesta por:

- Directora general.
- Ingeniero de sistemas,
- Técnicos de sistemas

En todo caso, dicha comisión o la mesa de trabajo, deberá revisar y actualizar anualmente esta política finalizando con su respectiva aceptación.

6.1.1 Roles y responsabilidades en la seguridad de la información

La Política de Seguridad de la Información es de aplicación obligatoria para todo el personal de SITCAR S.A., cualquiera sea su situación contractual, la dependencia a la cual se encuentre adscrito y el nivel de las tareas que desempeñe.

El Responsable de Seguridad de la Información es el líder del Equipo de trabajo de tecnología de la información, quien orienta y apoya a técnicos para la implementación, implantación, puesta en marcha, mantenimiento, supervisión y mejora continua del Sistema de Gestión de Seguridad de la Información. Este rol tiene las siguientes responsabilidades:

- Velar por la implementación, puesta en marcha y mantenimiento del Sistema de Gestión de Seguridad de la Información.

- Velar por la revisión de la estructura (políticas, procedimientos, instructivos, roles, responsables y responsabilidades) del Sistema de Gestión de Seguridad de la Información.

- Hacer seguimiento al plan de trabajo que permita el logro de los objetivos específicos de seguridad de la información.

- Presentar los cambios, proyectos e iniciativas del SGSI a la Dirección.

- Presentar las necesidades de recursos financieros para el desarrollo de proyectos que fortalezcan la gestión de la seguridad de la información con el fin de lograr los objetivos misionales y estratégicos.

El coordinador del área de Seguridad de la Información o también designado como Oficial de Seguridad de la Información es aquel profesional o contratista quien implementa y mantiene operativamente el Sistema de Gestión de Seguridad de la Información. En sus responsabilidades están:

- Aplicar conocimientos, habilidades, herramientas, y técnicas a la ejecución del Plan Operativo de Seguridad de la Información las actividades propias del proyecto, de manera que cumpla o exceda las necesidades y expectativas de los interesados en el mismo.

- Identificar la brecha entre el Modelo de seguridad y privacidad de la información y la situación de la entidad.

- Generar el cronograma de la implementación del Modelo de Seguridad y privacidad de la información.

- Planear e implementar las tareas, fechas y plan de trabajo para el cumplimiento de los objetivos específicos de seguridad de la información de SITCAR S.A.

- Gestionar el equipo de proyecto de la entidad, definiendo roles, responsabilidades, entregables y tiempos.

- Coordinar las actividades de los colaboradores con responsabilidades críticas en el SGSI y proporcionar apoyo administrativo.

- Planear y ejecutar de los planes de trabajo propuestos del SGSI, bajo un enfoque orientado a riesgos para darle solución oportuna y escalar al responsable de seguridad de la información en caso de ser necesario.

- Trabajar de manera integrada con el grupo o áreas asignadas.

- Velar por el mantenimiento documental del SGSI, su custodia y protección.

- Contribuir al enriquecimiento en la gestión del conocimiento en materia de seguridad y privacidad de la información apoyando la documentación de las lecciones aprendidas.

- Participar en las reuniones de seguimiento y velar por la actualización de los indicadores de gestión del SGSI.

Responsables críticos de la seguridad digital: Son funcionarios o colaboradores que por sus funciones gestionan, administran o supervisan activos de información críticos la compañía. A este rol pertenecen los funcionarios directivos y/o líderes de procesos, los colaboradores de Mesa de Servicios y el responsable de infraestructura y servicios tecnológicos. En sus responsabilidades está:

- Cumplir y velar por el estricto cumplimiento de las políticas de seguridad de la información a título personal y en los colaboradores o equipos de trabajo bajo su cargo.

- Atender los requerimientos de seguridad que les soliciten y en caso de ser requerido escalarlo al líder técnico de seguridad de la información o al responsable de seguridad de la información.

- Participar en las reuniones de seguridad de la información cuando sean convocados.

- Brindar y poner a disposición sus conocimientos, habilidades y capacidades

en la resolución de problemas e incidentes de seguridad de la información y de seguridad digital.

Responsables de la seguridad de la información: Son responsables por la seguridad de la información todos los funcionarios y colaboradores vinculados o que son partes interesadas de la compañía. Deben cumplir con las políticas de seguridad de la información y cuando identifiquen algún posible riesgo de seguridad de la información deben notificarlo al equipo de trabajo responsable de la seguridad de la información

El área de Seguridad de la Información de la institución es responsable de revisar y proponer las directrices para su aprobación, las funciones generales en materia de seguridad de la información y la estructuración, recomendación, seguimiento y mejora del Sistema de Gestión de Seguridad de la institución.

Los propietarios de activos de información son responsables de la clasificación, mantenimiento y actualización de la misma; así como de documentar y mantener actualizada la clasificación efectuada, definiendo qué usuarios debe tener permisos de acceso a la información de acuerdo a sus funciones y competencia. En general, tienen la responsabilidad de mantener íntegro, confidencial y disponible el activo de información mientras que es desarrollado, producido, mantenido y utilizado.

El jefe de Recursos Humanos cumplirá la función de notificar a todo el personal que se vincula contractualmente con la compañía, de las obligaciones respecto del cumplimiento de la Política de Seguridad de la Información y de todos los estándares, procesos, procedimientos, prácticas y guías que surjan del Sistema de Gestión de la Seguridad de la Información. De igual forma, será responsable de la notificación de la presente Política y de los cambios que en ella se produzcan a todo el personal, a través de la suscripción de los Compromisos de Confidencialidad y de tareas de capacitación continua en materia de seguridad según lineamientos dictados por el área de Seguridad de la Información.

Los técnicos de sistemas deben seguir los lineamientos de la presente política y cumplir los requerimientos que en materia de seguridad informática se establezcan para la operación, administración, comunicación y mantenimiento de los sistemas de información y los recursos de tecnología de la entidad.

Corresponde a dichas jefaturas determinar el inventario de activos de información y recursos tecnológicos de los cuales son propietarios o custodios, el cual será revisado y avalado por el Jefe de Almacén

El jefe de la Oficina Jurídica verificará el cumplimiento de la presente Política en la gestión de todos los contratos, acuerdos u otra documentación de la entidad con empleados y con terceros. Asimismo, asesorará en materia legal a la entidad en lo que se refiere a la seguridad de la información.

Los usuarios de la información y de los sistemas utilizados para su procesamiento son responsables de conocer y cumplir la Política de Seguridad de la Información vigente.

6.2 Políticas para uso de dispositivos móviles.

Por medio de este lineamiento se establecen las directrices de uso y manejo de dispositivos móviles (teléfonos inteligentes, portátiles, entre otros), entre otros suministrados por la entidad y personales que hagan uso de los servicios de información de SITCAR S.A., Así mismo se establecen lineamientos bajo las situaciones de las modalidades de trabajo en casa y teletrabajo.

- Los dispositivos móviles provistos por el SITCAR S.A., (teléfonos inteligentes, portátiles, entre otros), son una herramienta de trabajo que se deben utilizar únicamente para facilitar las comunicaciones y las actividades de los colaboradores de la entidad en el ejercicio de sus funciones o de sus obligaciones contractuales.

- Los dispositivos móviles asignados por el SITCAR S.A., deben tener la configuración realizada por el área de Tecnología de la Información, así mismo solo podrá configurarse únicamente las cuentas de correo electrónico asignadas al usuario por la entidad.

- Se autoriza el uso de WhatsApp pero no se permite por esta aplicación, el envío de fotografías, audios y videos clasificados como información pública reservada o información pública clasificada (privada o semiprivada).

- Los dispositivos móviles deben tener contraseña de ingreso y bloqueo del equipo de manera automática y manual.

- Los dispositivos móviles institucionales deben tener únicamente la tarjeta sim asignada por la entidad, de igual forma la tarjeta sim únicamente debe instalarse en los equipos asignados por la entidad.

- Ante la pérdida del equipo, ya sea por extravío o hurto, deberá informar de

manera inmediata al Equipo de Trabajo de RRHH, y continuar con el procedimiento administrativo por pérdida de elementos establecido por la entidad.

- Los usuarios no están autorizados a cambiar la configuración, ni a la desinstalación de software de los equipos móviles institucionales posterior a su recibo; únicamente se deben aceptar y aplicar las actualizaciones.

- Los usuarios de dispositivos móviles asignados por la entidad deben evitar hacer uso de lugares con algún riesgo de seguridad, evitando el extravío o hurto del equipo.

- Los usuarios de dispositivos móviles institucionales no deben conectarlos en computadores y/o puertos USB de uso público (Restaurantes, café internet, aeropuertos, etc.).

- Los usuarios de dispositivos móviles institucionales NO deben hacer uso de redes inalámbricas públicas.

- En caso de requerir instalación de aplicaciones adicionales en el dispositivo móvil institucional se debe solicitar al área de tecnología quienes evaluarán si se escala o no la solicitud.

- Todo acceso remoto a los recursos de la red corporativa de SITCAR S.A., deben ser por medio de VPN debidamente solicitadas por el jefe inmediato o líder del área de Tecnología de la Información.

- Todo correo enviado desde una cuenta institucional debe llevar la firma del remitente para su identificación. En caso de gestionar el correo desde equipos que no son propiedad de la compañía, se debe configurar la firma institucional para su uso.

- No se debe acceder remotamente a los recursos de la red corporativa de SITCAR S.A o terceros, desde equipos que no cuenten con antivirus actualizado y funcionando, o que no cuenten con las actualizaciones de seguridad del sistema operativo o que sea de uso público (café Internet, por ejemplo) o que se sospeche que no es seguro.

- Cuando se acceda remotamente a la información de SITCAR S.A., se debe cumplir con las políticas de pantalla limpia (aplica para el trabajo desde casa).

6.3 Políticas de uso de internet

Por medio de esta política se establecen los lineamientos que garanticen la navegación segura y el uso adecuado de la red por parte de los usuarios finales, evitando errores, pérdidas, modificaciones no autorizadas o uso inadecuado de la información en las aplicaciones WEB.

- La navegación en Internet debe realizarse de forma razonable y con propósitos laborales.

- No se debe visitar y/o navegar en sitios o portales web con contenidos contrarios a la ley o a las políticas o que representen peligro para la entidad como: pornografía, terrorismo, hacktivismo, segregación racial u otras fuentes definidas. El acceso a este tipo de contenidos con propósitos de estudio de seguridad o de investigación, debe contar con la autorización expresa de los responsables técnicos en seguridad de la información del área de tecnología.

- El área de Tecnología de la Información otorgara o no la autorización de navegación a los usuarios de SITCAR S.A., previa solicitud del jefe de la dependencia.

- El área de Tecnología de la Información implementara herramientas para evitar la descarga de software no autorizado y/o código malicioso en los equipos institucionales.

- La descarga de archivos de internet debe ser con propósitos laborales y de forma razonable para no afectar las operaciones, en forma específica el usuario debe cumplir los requerimientos de la política.

- Los usuarios de los activos de información de SITCAR S.A., tiene prohibido el acceso a redes sociales, sistemas de mensajería instantánea y cuentas de correo no institucional.

6.4 Políticas de dispositivos informáticos, medios y equipos

Esta política es hacer frente a la suspensión de actividades de SITCAR S.A., proteger sus procesos críticos contra los efectos de fallas importantes en los sistemas de información o contra desastres y proponer por su recuperación oportuna, permitiendo la confidencialidad, integridad y disponibilidad de la información.

- Los medios y equipos donde se almacena, procesa o comunica la información, deben mantenerse con las medidas de protección física y lógica, que permitan su monitoreo y correctivo de funcionamiento, para ello se debe realizar los mantenimientos preventivos y correctivos que se requieran.

- Está restringido del uso de medios removibles de almacenamiento, por lo cual se deshabilita la funcionalidad de los puertos USB, unidades ópticas de grabación en todos los equipos de cómputo institucionales; la autorización de uso de los medios removibles debe ser tramitada a través área de Seguridad de la Información

6.5 Políticas de usos de Activos de información

Todo activo de información debe ser identificado, clasificado y tenido en cuenta para la gestión de riesgos de seguridad de la información y de seguridad digital.

Identificación y Clasificación de los Activos de Información: Debe realizarse y mantenerse un inventario de activos de información que permita identificar lo siguiente:

- Propiedad del activo: nombre, propietario y custodio técnico del activo

    - Acceso: Derechos de acceso sobre el activo.
    - Tipo de activo: Si es información, software, físico, servicios o un intangible.
    - Valor del activo: Definida por su confidencialidad, integridad, disponibilidad.
    - Clasificación: Determinar su clasificación de acuerdo con la criticidad, sensibilidad y reserva del activo.
    - Ubicación: Establecer si la ubicación es física o electrónica y el lugar donde se encuentra.

- Propietarios de activos de información: SITCAR S.A., es el dueño de la propiedad intelectual de los avances tecnológicos e intelectuales desarrollados por los funcionarios contratistas de la entidad, derivadas del objeto del cumplimiento de funciones y/o tareas asignadas, como las necesarias para el cumplimiento del objeto del contrato.

- Custodios de activos de información: son responsables de la cadena de custodia la cual se apoya en la aplicación de controles para la protección de la información según su nivel de clasificación y el recurso en donde esta se almacene.

El objetivo de estas políticas es lograr mantener la protección adecuada de los activos de información mediante la asignación a los usuarios finales que deban administrarlos de acuerdo con sus roles y funciones.

- Los activos de información son almacenados por SITCAR S.A., y el uso de estos debe emplearse exclusivamente con propósitos laborales.

- Los usuarios deberán utilizar únicamente los recursos tecnológicos autorizados por el área de Tecnología de la Información o el área de Seguridad de la Información.

- SITCAR S.A., proporcionará al usuario, los equipos informáticos y los programas instalados en ellos; los datos/información creados, almacenados y recibidos, serán propiedad De SITCAR S.A., los funcionarios solo podrán realizar copia de respaldo de sus archivos personales o de información pública. Para copiar cualquier tipo de información clasificada o reservada debe pedir autorización a su jefe inmediato, de acuerdo con las normas sobre clasificación de la información de acuerdo con los niveles de seguridad establecidos por la entidad; Su copia, sustracción, daño intencional o utilización para fines distintos a las labores propias de la Institución, serán sancionadas de acuerdo con las normas y legislación vigentes.

- Cualquier convenio o contrato con otra entidad, SITCAR S.A., proporcionara los equipos informáticos y programas instalados, y el área de Tecnología de la Información de la entidad llevara a cabo las configuraciones de red e instalación de programas faltantes.

- Periódicamente, el área de Tecnología de la Información efectuará la revisión de los programas utilizados en cada dependencia. La descarga, instalación o uso de aplicativos o programas informáticos NO autorizados será considerada como una violación a las Políticas de Seguridad de la Información de la entidad.

- Todos los requerimientos de aplicativos, sistemas y equipos informáticos deben ser solicitados por el jefe de la dependencia al E. T. de Tecnología de Información.

- Estarán bajo custodia del área de Tecnología de la Información los medios magnéticos/electrónicos (disquetes, CDs u otros) que vengan originalmente con el software y sus respectivos manuales y licencias de uso, adicionalmente las claves para descargar el software de fabricantes de sus páginas web o sitios en internet y las contraseñas de administración de los equipos informáticos, sistemas de información o aplicativos.

- En caso de ser necesario y previa autorización del área de seguridad de la Información de SITCAR S.A., los funcionarios de la entidad podrán acceder a revisar cualquier tipo de activo de información y material que los usuarios creen, almacenen, envíen o reciban, a través de Internet o de cualquier otra red o medio, en los equipos informáticos a su uso.

- Los recursos informáticos de SITCAR S.A., no podrán ser utilizados, sin previa autorización escrita, para divulgar, propagar o almacenar contenido personal o comercial de publicidad, promociones, ofertas, programas destructivos (virus), propaganda política, material religioso o cualquier otro uso que no esté autorizado.

- Los usuarios no deben realizar intencionalmente actos que impliquen un mal uso de los recursos tecnológicos o que vayan en contravía de las políticas de seguridad de la información entre ellos envíos o reenvíos masivos de correos electrónicos o spam, practica de juegos en línea, uso permanente de redes sociales personales, conexión de periféricos o equipos que causen molestia a compañeros de trabajo, etc.

- Los usuarios no podrán efectuar ninguna de las siguientes labores sin previa autorización del área de Tecnología de la Información:

    - Instalar software en cualquier equipo del SITCAR S.A;
    - Bajar o descargar software de Internet u otro servicio en línea en cualquier equipo se SITCAR S.A;
    - Modificar, revisar, transformar o adaptar cualquier software propiedad de la entidad;
    - Copiar o distribuir cualquier software de propiedad de SITCAR S.A.
    - Cambiar la configuración de hardware de propiedad de SITCAR S.A.

- El usuario deberá informar al Jefe Inmediato de cualquier violación de las políticas de seguridad, uso indebido y debilidades de seguridad de la información de SITCAR S.A., que tenga conocimiento y al Equipo de Trabajo de Tecnología de Información.

- El usuario será responsable de todas las transacciones o acciones efectuadas con su "cuenta de usuario".

- Ningún usuario deberá acceder a la red o a los servicios TIC de SITCAR S.A., utilizando una cuenta de usuario o clave de otro usuario.

- Los usuarios no están autorizados para hacer uso de redes externas a través de dispositivos personales en las instalaciones de la entidad (modem USB, enrutador, wifi público, etc.), esto compromete la seguridad de los recursos informáticos de SITCAR S.A.

- El área de Tecnología de Información de SITCAR S.A., es el área responsable de realizar el aseguramiento de los accesos a internet, a las redes de la entidad; esta responsabilidad incluye, pero no se limita a prevenir que intrusos tengan acceso a los recursos informáticos y a prevenir la

introducción y propagación de virus.

- Todo archivo o material descargado o recibido a través de medio magnético/electrónico o descarga de Internet o de cualquier red externa, deberá ser revisado para detección de virus y otros programas maliciosos antes de ser instalados en la infraestructura TIC de SITCAR S.A.

- Todos los archivos provenientes de equipos externos a SITCAR S.A., deben ser revisados para detección de virus antes de su utilización dentro de la red de la entidad.

- Todo cambio a la infraestructura informática deberá estar controlado y será realizado de acuerdo con los procedimientos de gestión de cambios del área de Tecnología de Información de SITCAR S.A.

- La información de SITCAR S.A., debe ser respaldada de forma frecuente, debe ser almacenada en lugares apropiados en los cuales se pueda lograr su custodia y confidencialidad y pueda ser recuperada en caso de desastre o de incidentes catastróficos y con los equipos de procesamiento que tenga predefinido el área de Tecnología de la Información.

- Los funcionarios deberán realizar la devolución de todos los activos físicos y/o electrónicos asignados por SITCAR S.A., en el proceso de desvinculación, de igual manera deberán documentar y entregar a SITCAR S.A., los conocimientos importantes que posee de la labor que ejecutan.

6.6 Políticas de seguridad para los recursos humanos.

Por medio de esta política se establecen las directrices para que los funcionarios, contratistas y demás colaboradores de SITCAR S.A., entiendan sus responsabilidades y las funciones de sus roles y usuarios, con el fin de reducir el riesgo de hurto, fraude, filtraciones o uso inadecuado de la información y de las instalaciones.

- Se debe asegurar que los funcionarios, contratistas y demás colaboradores de SITCAR S.A., adopten sus responsabilidades para atender y cumplir las políticas de seguridad de la información de la entidad y actúen de manera consistente frente a las mismas, con el fin de reducir el riesgo de pérdida de integridad, confidencialidad y/o disponibilidad de la información o de los activos de información.

- Los candidatos, aspirantes, contratistas y proveedores deben dar aprobación a SITCAR S.A., para el tratamiento de sus datos personales de acuerdo con la Ley 1581 de 2012, por el cual se dictan disposiciones generales del Habeas Data y se regula el manejo de la información contenida en base de datos personales.

- A la firma del contrato laboral o posesión del cargo el funcionario debe firmar un acuerdo de confidencialidad para con SITCAR S.A.

- Se debe capacitar y sensibilizar a los funcionarios durante la inducción sobre las políticas de seguridad de la información.

- Los funcionarios de SITCAR S.A., deben cumplir con el manual de Excelencia Ética y Buen Gobierno, Resolución 390 de 2017.

6.7 Políticas de uso de estaciones cliente

El objetivo de este lineamiento es garantizar que la seguridad es parte integral de los activos de información y la correcta utilización por los usuarios finales.

- La instalación de software en los computadores suministrados por SIRCAT S.A., o terceros, es una función exclusiva del proceso de Gestión de arquitectura de TI, el cual mantendrá una lista actualizada del software autorizado para instalar en los computadores.

- Los usuarios que hagan uso de equipos, NO deberán almacenar de forma permanente información pública reservada y pública clasificada en dichos equipos y por lo tanto esta información se debe almacenar en los espacios de almacenamiento definidos por el área de Tecnología de Información y así mismo realizar el borrado seguro de dicha información cuando se haga la devolución del correspondiente equipo.

- Los usuarios no deben mantener almacenados en los discos duros de las estaciones cliente o discos virtuales de red, archivos de vídeo, música y fotos que no sean de producto de su gestión en el marco del cumplimiento de sus funciones o de sus obligaciones contractuales.

- En el Disco C:\ de los equipos -equipos de escritorio y/o portátiles- asignados a los colaboradores (usuarios) se tiene configurado el sistema operativo, aplicaciones y perfil de usuario. El usuario deberá abstenerse de realizar modificaciones a estos archivos.

- Los usuarios podrán trabajar sus archivos de gestión en los equipos -equipos

de escritorio y/o portátiles- que les fueron asignados por SITCAR S.A., y deberán ubicar copias y documentos finales en las carpetas de Drive de Google y en Mis Documentos para garantizar la copia de respaldo que se hace diariamente.

- El préstamo de recursos tecnológicos como equipos de cómputo, computadores portátiles, etc., se debe hacer a través de la mesa de ayuda de TI con anticipación y se proveerá de acuerdo con la disponibilidad.

- Los equipos que ingresan temporalmente a SITCAR S.A., que son de propiedad de terceros, deben ser registrados en los controles de acceso de la entidad para poder realizar su retiro; el Fondo Adaptación no se hace responsable por pérdida o daño de los recursos tecnológicos como equipos portátiles, dispositivos móviles, etc., de uso personal o de terceros.

6.8 Políticas de establecimiento, uso y protección de claves de acceso

El objetivo de este lineamiento es definir los criterios y usos aceptables de claves de acceso.

- Se debe concientizar y controlar a los usuarios para que apliquen buenas prácticas de seguridad en la selección, uso y protección de claves o contraseñas, las cuales constituyen un medio de validación de la identidad de un usuario y consecuentemente un medio para establecer derechos de acceso a las instalaciones, equipos o servicios informáticos.

- Los usuarios son responsables por el uso de las claves o contraseñas de acceso que se le asignen para la utilización de los equipos o servicios informáticos de la compañía. Los usuarios y contraseñas son personales e intransferibles.

- El cambio de contraseña debe ser solicitado solamente por el titular de la cuenta o su jefe inmediato.

- A partir del quinto intento consecutivo sin éxito de inicio de sesión, se bloquea la cuenta de usuario.

- Los usuarios deben tener en cuenta los siguientes aspectos:

    - No incluir contraseñas en ningún proceso de registro automatizado, por ejemplo, almacenadas en un macro o en mecanismos de almacenamiento de terceros ni de los exploradores web.
    - Terminar las sesiones activas cuando finalice, o asegurarlas con el mecanismo de bloqueo cuando no estén en uso.

- La clave de acceso será desbloqueada luego de la solicitud formal al área de Tecnología de Información por parte del responsable de la cuenta.

Las claves o contraseñas deben:

- Poseer algún grado de complejidad y no deben ser palabras comunes que se puedan encontrar en diccionarios, ni tener información personal, ni productos a resaltar de su entidad, evite asociarla con fechas especiales, por ejemplo: fechas de cumpleaños, nombre de los hijos, placas de automóvil, etc.

- Nunca utilice sus contraseñas personales en el entorno laboral.

- Tener mínimo ocho caracteres alfanuméricos y caracteres especiales.

- Cambiarse obligatoriamente la primera vez que el usuario ingrese al sistema.

- Cambiarse obligatoriamente cada 90 días, o cuando lo establezca el área. de Tecnología de Información.

- Cada vez que se cambien estas deben ser distintas por lo menos de las últimas tres anteriores.

- Cambiar la contraseña si ha estado bajo riesgo o se ha detectado anomalía en la cuenta de usuario.

- No se deben usar caracteres idénticos consecutivos, ni que sean todos numéricos, ni todos alfabéticos.

- No debe ser visible en la pantalla, al momento de ser ingresada o mostrarse o compartirse.

- No ser reveladas a ninguna persona, incluyendo al personal del área de Tecnología de Información.

- No registrarlas en papel, archivos digitales o dispositivos manuales, a menos que se puedan almacenar de forma segura y el método de almacenamiento este aprobado.

6.9 Políticas de respaldo y restauración de información

El objetivo de este lineamiento es proporcionar los medios de respaldo adecuados para asegurar que toda la información esencial y el software, se pueda recuperar después de

una falla.

- La información de cada sistema debe ser respaldada sobre un medio de almacenamiento como cinta, cartucho, CD, DVD, o sistemas remotos de almacenamiento en centros de datos de terceros contratados para tal fin.

- Los administradores de los servidores, los sistemas de información o los equipos de comunicaciones, son los responsables de definir la frecuencia de respaldo y los requerimientos de seguridad de la información (codificación); de igual manera el administrador del sistema de respaldo, es el responsable de realizar los respaldos periódicos.

- Todas las copias de información crítica deben ser almacenadas en un área adecuada y con control de acceso.

- Las copias de respaldo se guardan únicamente con el objetivo de restaurar el sistema luego de la infección de un virus informático, defectos en los discos de almacenamiento, problemas de los servidores o computadores, materialización de amenazas, catástrofes o por requerimiento legal.

- Ningún tipo de información relevante 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 compartidas remotas o en los espacios de almacenamiento en la nube destinados para este fin.

- La restauración de copias de respaldo en ambientes de producción debe estar debidamente aprobada por el propietario de la información.

- Semanalmente los administradores de infraestructura del SITCAR S.A., o de terceros si se requiere verificarán la correcta ejecución de los procesos de copias de respaldo.

- El área de Tecnología de Información debe mantener un inventario actualizado de las copias de respaldo de la información y los aplicativos o sistemas de SITCAR S.A., o servicio con otra compañía en convenio que requiera tal proceso.

6.10 Políticas para la realización de copias en los computadores de usuario final

El objetivo de este lineamiento es asegurar la operación de realización de copias de información en estaciones de trabajo de usuario final.

- En el evento de retiro de un funcionario o traslado de dependencia, previa notificación del área de Talento Humano, el área de Tecnología de Información generará una copia de la información contenida en el equipo asignado al perfil del usuario (C:\usuarios\nombre-usuario), a una unidad de almacenamiento.

- Si se requiere información gestionada por un funcionario o colaborador retirado se debe solicitar a Mesa de Servicios quien escalará al Líder del área de Tecnología de Información y al líder del proceso al que pertenecía el funcionario o colaborador retirado quienes autorizarán o no la entrega de dicha información.

- Se debe seguir el procedimiento de Borrado Seguro para equipos devueltos a almacén o para dar de baja, a fin de garantizar la copia de la información para la compañía y la eliminación de la información almacenada en el disco local.

- Ningún usuario final debe realizar copias de la información contenida en la estación de trabajo a medios extraíbles de información, excepto aquellos que se encuentren habilitados los privilegios de escritura por puertos USB.

- En caso de presentarse alguna falla en los equipos de cómputo, se debe reportar a la mesa de ayuda del área de Tecnología de Información y en caso de requerirse copia de la información, ésta se realizará de manera temporal durante las diferentes labores de reparación o mantenimiento.

6.11 Políticas de uso de puntos de red de datos (red de área local – LAN)

El objetivo de este lineamiento es asegurar la correcta y segura operación de los puntos de red.

- Los usuarios deberán emplear los puntos de red, para la conexión de equipos informáticos o equipos de contratistas debidamente autorizados.

- Los equipos de visitantes, solo tendrán acceso a servicios limitados destinados a invitados o visitantes, estos equipos deben ser conectados a los puntos de acceso autorizados y redes WIFI definidos por el área de Tecnología de Información de la entidad.

- La instalación, activación y gestión de los puntos de red es responsabilidad del área de Tecnología de Información.

- Ningún usuario debe utilizar equipo diferente al asignado para copiar algún tipo de archivo, excepto al autorizado por jefe inmediato.

- Es responsabilidad de cada dependencia deberá mantener depurada la información de las carpetas virtuales como Google Drive para la optimización del uso de los recursos de almacenamiento que se le entra a los usuarios.

- La configuración de enrutadores, switches, firewall, sistemas de detección de intrusos y otros dispositivos de seguridad de red; debe ser documentada, respaldada por copia de seguridad y mantenida por la Red de Datos.

6.12 Políticas de administración de las comunicaciones y operaciones.

6.12.1 Protección contra software maliciosos y hacking

Todos los sistemas informáticos deben ser protegidos teniendo en cuenta un enfoque multi-nivel que involucre controles humanos, físicos técnicos y administrativos. El área de Tecnología de la Información elaborara y mantendrá un conjunto de políticas, normas, estándares, procedimiento y guías que garanticen la mitigación de riesgos asociados a amenazas de software malicioso y técnicas de hacking

En todo caso y como control mínimo, las estaciones de trabajo de la Universidad deben estar protegidas por software antivirus con capacidad de actualización automática en cuanto a firmas de virus. Los usuarios de las estaciones no están autorizados a deshabilitar este control.

El área de Tecnóloga de la Información podrá hacer seguimiento al tráfico de la red cuando se tenga evidencias de actividad inusual o detrimentos en el desempeño. La dependencia que realice dicho seguimiento deberá informar a la comunidad a través de correo electrónico.

El área de Tecnología de la Información debe mantener actualizada una base de datos con alertas de seguridad reportadas por organismo competentes y actuar en conformidad cuando una alerta puede tener un impacto considerable en el desempeño de los sistemas informáticos.

6.12.2 Reporte e investigación de incidentes de seguridad

El personal de SITCAR S.A., debe reporta con diligencia, prontitud y responsabilidad presuntas violaciones de seguridad a través de su jefe de dependencia. En casos especiales dichos reportes podrían realizarse directamente al área de Tecnología de la Información, la cual debe garantizar las herramientas informáticas para que formalmente se realicen tales denuncias.

El área de Seguridad de la Información debe preparar, mantener y difundir las normas, procesos y guías para el reporte e investigación de incidentes de seguridad.

SITCAR S.A., en conjunto con el área de Tecnología de la Información mantendrá

procedimiento escritos para la operación de sistemas cuya no disponibilidad suponga un impacto alto en el desarrollo de actividades. A dichos sistemas se debe realizar seguimiento continuo del desempeño para asegurar la confiabilidad del servicio que prestan.

7 PROCESO DISCIPLINARIO

Dentro de la estrategia de seguridad de la información de SITCAR S.A., está establecido un proceso disciplinario formal para los funcionarios que hayan cometido alguna violación de la Política de Seguridad de la Información. El proceso disciplinario también se debería utilizar como disuasión para evitar que los funcionarios, contratistas y los otros colaboradores de SITCAR S.A., violen las políticas y los procedimientos de seguridad de la información, así como para cualquier otra violación de la seguridad. Las investigaciones disciplinarias corresponden a actividades pertenecientes al proceso de Recursos Humanos.

Actuaciones que conllevan a la violación de la seguridad de la información establecidas por SITCAR S.A:

- No firmar los acuerdos de confidencialidad o de entrega de información o de activos de información.

- Ingresar a carpetas de otros procesos, unidades, grupos o áreas, sin autorización y no reportarlo al área de Seguridad o al área de Tecnología de Información.

- No reportar los incidentes de seguridad o las violaciones a las políticas de seguridad, cuando se tenga conocimiento de ello.

- No actualizar la información de los activos de información a su cargo.

- Clasificar y registrar de manera inadecuada la información, desconociendo los estándares establecidos para este fin.

- No guardar de forma segura la información cuando se ausenta de su puesto de trabajo o al terminar la jornada laboral, "documentos impresos que contengan información pública reservada, información pública clasificada (privada o semiprivada)".

- No guardar la información digital, producto del procesamiento de la información perteneciente a SITCAR S.A., o de terceros.

- Dejar información pública reservada, en carpetas compartidas o en lugares distintos al servidor de archivos, obviando las medidas de seguridad.

- Dejar las gavetas abiertas o con las llaves puestas en los escritorios.

- Dejar los computadores encendidos en horas no laborables.

- Permitir que personas ajenas SITCAR S.A, o de entidades en convenio deambulen sin acompañamiento, al interior de las instalaciones, en áreas no destinadas al público.

- Almacenar en los discos duros de los computadores personales de los usuarios, la información de la entidad.

- Solicitar cambio de contraseña de otro usuario, sin la debida autorización del titular o su jefe inmediato.

- Hacer uso de la red de datos de la institución, para obtener, mantener o difundir en los equipos de sistemas, material pornográfico (penalizado por la ley) u ofensivo, cadenas de correos y correos masivos no autorizados.

- Utilización de software no relacionados con la actividad laboral y que pueda degradar el desempeño de la plataforma tecnológica institucional.

- Recibir o enviar información institucional a través de correos electrónicos personales, diferentes a los asignados por la compañía.

- Enviar información pública reservada o información pública clasificada (privada o semiprivada) por correo, copia impresa o electrónica sin la debida autorización y sin la utilización de los protocolos establecidos para la divulgación.

- Utilizar equipos electrónicos o tecnológicos desatendidos o que, a través de sistemas de interconexión inalámbrica, sirvan para transmitir, recibir y almacenar datos.

- Usar dispositivos de almacenamiento externo en los computadores, cuya autorización no haya sido otorgada por el área de Tecnología de Información.

- Permitir el acceso de funcionarios a la red corporativa, sin la autorización del área de Tecnología de Información.

- Utilización de servicios disponibles a través de internet, como FTP y Telnet, no permitidos o de protocolos y servicios que no se requieran y que puedan generar riesgo para la seguridad.

- Negligencia en el cuidado de los equipos, dispositivos portátiles o móviles entregados para actividades propias.

- No cumplir con las actividades designadas para la protección de los activos de información.

- Destruir o desechar de forma incorrecta la documentación de la compañía.

- Descuidar documentación con información pública reservada o clasificada de la entidad, sin las medidas apropiadas de seguridad que garanticen su protección.

- Registrar información pública reservada o clasificada, apuntes, agendas, libretas,

etc. Sin el debido cuidado.

- Almacenar información pública reservada o clasificada, en cualquier dispositivo de almacenamiento que no permanezca a la compañía o conectar computadores portátiles u otros sistemas eléctricos o electrónicos personales a la red de datos, sin la debida autorización.

- Archivar información pública reservada o clasificada, sin claves de seguridad o cifrado de datos.

- Promoción o mantenimiento de negocios personales, o utilización de los recursos tecnológicos para beneficio personal.

- El que sin autorización acceda en todo o parte del sistema informático o se mantenga dentro del mismo en contra de la voluntad.

- El que impida u obstaculice el funcionamiento o el acceso normal al sistema informático, los datos informáticos o las redes de telecomunicaciones, sin estar autorizado.

- El que destruya, dañe, borre, deteriore o suprima datos informáticos o un sistema de tratamiento de información.

- El que distribuya, envíe, introduzca software malicioso u otros programas de computación de efectos dañinos en la plataforma tecnológica.

- El que viole datos personales de las bases de datos.

- El que superando las medidas de seguridad informática suplante un usuario ante los sistemas de autenticación y autorización establecidos.

- No mantener la confidencialidad de las contraseñas de acceso a la red de datos, los recursos tecnológicos o los sistemas de información o permitir que otras personas accedan con el usuario y clave del titular a éstos.

- Permitir el acceso u otorgar privilegios de acceso a las redes de datos a personas no autorizadas.

- Llevar a cabo actividades fraudulentas o ilegales, o intentar acceso no autorizado a cualquier computador o de terceros.

- Ejecutar acciones tendientes a eludir o variar los controles establecidos.

- Retirar de las instalaciones de la institución, estaciones de trabajo o computadores portátiles que contengan información institucional sin la autorización pertinente.

- Sustraer de las instalaciones, documentos con información institucional calificada como información pública reservada o clasificada, o abandonarlos en lugares

públicos o de fácil acceso.

- Entregar, enseñar y divulgar información de la compañía, calificada como información pública reservada y clasificada a personas o entidades no autorizadas.

- No realizar el borrado seguro de la información en equipos o dispositivos de almacenamiento, para traslado, reasignación o para disposición final.

- Ejecución de cualquier acción que pretenda difamar, abusar, afectar la reputación o presentar una mala imagen o de alguno de sus funcionarios.

- Realizar cambios no autorizados en la plataforma tecnológica.

- Acceder, almacenar o distribuir pornografía infantil.

- Instalar programas o software no autorizados en las estaciones de trabajo o equipos portátiles institucionales, cuyo uso no esté autorizado por el área de Tecnología de Información.

- Copiar sin autorización los programas, o violar los derechos de autor o acuerdos de licenciamiento.

8 CUMPLIMIENTO

Todo uso y seguimiento de uso a los recursos de TI en SITCAR S.A., debe estar de acuerdo a las normas y estatutos internos así como a la legislación nacional en la materia, incluido pero no restringido a:

Constitución Política de Colombia
Ley 527•1999 Ley de comercio electrónico.
NTC 27001:2006. Sistema de Gestión de Seguridad de la Información.
ISO/IEC 17799:2005 Information technology • Security techniques • Code of practice for informationsecurity management
PIGA – Plan Institucional de Gestión Ambiental

9 REFERENCIAS

ISO 27001:2005. Sistemas de gestión de Seguridad en la Información– Requerimientos.
ISO/IEC 13335•1:2004. Tecnología de la información – Técnicas de seguridad – Gestión de seguridad en tecnología de información y comunicaciones – Parte 1: Conceptos y modelos para la gestión de seguridad en la tecnología de la información y comunicaciones.
ISO/IEC TR 13335•3:1998. Lineamientos para la Gestión de Seguridad TI – Parte 3:

Técnicas para la gestión de la seguridad TI.
ISO/IEC 13335•4:2000. Lineamientos para la Gestión de la Seguridad TI – Parte 4: Selección desalvaguardas.
ISO 14001:2004. Sistemas de gestión ambiental – Requerimientos con lineamiento para su uso
ISO/IEC TR 18044:2004.Tecnología de la información – Técnicas de seguridad – Gestión deincidentes en la seguridad de la información.
ISO/IEC 19011:2002. Lineamientos para la auditoría de sistemas de auditoría y/o gestiónambiental
ISO/IEC Guía 62:1996. Requerimientos generales para los organismos que operan la evaluación ycertificación/registro de sistemas de calidad.
ISO/IEC Guía 73:2002. Gestión de riesgo –Vocabulario – Lineamientos para el uso enestándares.
NIST SP 800•30. Guía de Gestión de Riesgo para los Sistemas de Tecnología de la Información.
ISO 9001:2000. Sistemas de gestión de calidad – Requerimientos.