POLITICAS Y NORMAS GENERALES DE TECNOLOGÍA INFORMÁTICA.

CONTENIDO

1 INTRODUCCIÓN

Este documento pretende establecer las políticas de tecnología informática con lineamientos claros los cuales están definidos a través del mismo, para así optimizar y mejorar los proyectos y recursos de TI que contribuye al cumplimiento de la misión y objetivos estratégicos de la Compañía. Teniendo como base la seguridad de la información en sus tres pilares (confiabilidad, disponibilidad e integridad).

2 ALCANCE

El presente documento es aplicable a todos los empleados, consultores, contratistas, colaboradores, practicantes, incluyendo a todo el personal externo que en algún momento cuente con acceso a los recursos informáticos o información de La Compañía.
La elaboración de las políticas de tecnología está fundamentada bajo la metodología ITIL, la norma ISO 27000 y las guías del MINTIC.
Las políticas definidas están en concordancia con los estatutos y reglamentos internos de la compañía, asegurando la seguridad y optimización de los sistemas tecnológicos brindándole al usuario garantías básicas.

3 OBJETIVO

Brindar la información necesaria a la totalidad de los usuarios de tecnología, (directivos, gerentes, empleados) de las normas y mecanismos que deben cumplir y utilizar para proteger el hardware y software de la red, así como la información que es procesada y almacenada en estos.
Planear, organizar, dirigir y controlar las actividades para mantener y garantizar la integridad física de los recursos informáticos, así como resguardar los activos de la Compañía.

3.1 Objetivos específicos

- Mantener la confidencialidad, integridad y disponibilidad de los activos de información de la Compañía.
- Establecer las políticas para resguardo y garantía de acceso apropiado de la información.
- Vigilar que la Compañía cuente con los recursos de software legal necesario para su funcionamiento.
- Adquirir tecnología acorde a las necesidades institucionales aprovechando al máximo las capacidades de los funcionarios y el presupuesto asignado.

4 OBLIGACIONES

Las políticas de tecnologías de la información de obligatorio cumplimiento por todos los usuarios permanentes o que tengan acceso a los servicios tecnológicos.

5 DEFINICIONES

- **Activo**: En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de la misma (sistemas, soportes, locación/edificio, personas) que tenga valor para la organización.
- **Seguridad de la información:** Preservación de la confidencialidad, integridad, y disponibilidad de la información.
- **Confidencialidad:** Es la garantía de que la información no está disponible o divulgada a personas, entidades o procesos no autorizados.
- **Integridad:** Es la capacidad de garantizar que los datos no han sido modificados desde su creación sin autorización. La información que disponemos es válida y consistente.
- **Disponibilidad:** Es la garantía de que los usuarios autorizados tienen acceso a la información en el menor tiempo posible junto con los activos asociados cuando lo requieren.
- **Seguridad perimetral:** La seguridad perimetral es un concepto emergente asume la integración de elementos y sistemas, tanto electrónicos como mecánicos, para la protección de perímetros físicos, detección de tentativas de intrusos en instalaciones especialmente sensibles.
- **Plan de recuperación de desastres (DRP):** Se entiende por plan de contingencia el conjunto de procedimientos alternativos a la operación normal en una organización, cuyo objetivo principal es permitir el continuo funcionamiento y desarrollo normal de sus operaciones, preparándose para superar cualquier eventualidad ante accidentes de origen interno o externo, que ocasionen pérdidas importantes de información.

6 POLÍTICAS GENERALES

- Los recursos informáticos sólo pueden ser utilizados por los usuarios y contratistas u otros usuarios que cuentan con la debida autorización del subdirector IT, Administrador IT o la Gerencia Administrativa y financiera.
- Las políticas de tecnologías de información serán aprobadas por el subdirector IT. Su socialización estará a cargo del Administrador IT, estas políticas serán materia obligada en los procesos de inducción a los nuevos funcionarios, anualmente será

incluida en la reinducción anual para todo el personal.

- El desarrollo de nuevos proyectos que involucren el uso de recursos tecnológicos será validados y liderados por el área de tecnología informática.
- La adquisición de bienes y/o servicios, donde se incluyan equipos informáticos como parte integrante o complementaria de otros, serán validados por el área de tecnología informática.
- Verificará que los equipos tecnológicos tengan: disponibilidad de energía eléctrica, cableado estructurado y mantengan las condiciones físicas aceptables y adecuadas de temperatura, para su debido funcionamiento, entre otros.
- El área de TI debe velar por la debida privacidad y confidencialidad de los datos registrados en los sistemas de información y en general en la plataforma e infraestructura tecnológica de la Compañía y solo se permitirá el acceso a información propia de los usuarios de la Compañía cuando sea solicitado de manera formal por una autoridad competente y con la respectiva justificación.
- Los servicios ofrecidos por el área de TI, (mesa ayuda, backup etc.) se solicitarán formalmente y siguiendo los procedimientos que se emitan para ese fin.
- El área TI tiene como una de sus funciones la de proponer y revisar el cumplimiento de normas y políticas de seguridad, que garanticen acciones preventivas y correctivas para la salvaguarda de equipos e instalaciones de cómputo, así como de bancos de datos de información automatizada en general.

7 RESPONSABILIDADES DE LOS USUARIOS.

- El equipo asignado es de uso personal, por lo tanto, cada usuario es responsable de este y del buen uso del mismo.
- Los usuarios tienen la obligación de proteger las unidades de almacenamiento que se encuentren bajo su responsabilidad, aun cuando no se utilicen y contengan información confidencial o importante de la compañía.
- No realizar cambios en las configuraciones de hardware o software instalado en los equipos de cómputo ya que este solo lo realiza el área de tecnología informática para evitar incompatibilidades o malos funcionamientos.
- A no divulgar la clave de acceso ya que esta es de uso personal e intransferible, como consecuencia se entiende para todos los efectos que solo la conoce el responsable del equipo y el administrador de la red.
- El usuario que detecte o tenga conocimiento de la posible ocurrencia de un incidente de seguridad informática deberá reportarlo al área TI lo antes posible, indicando claramente los datos por los cuales lo considera un incidente de seguridad informática.

- Cuando exista la sospecha o el conocimiento de que información confidencial o reservada ha sido revelada, modificada, alterada o borrada sin la autorización de las directivas, el usuario informático deberá notificar al área TI.
- Cualquier incidente generado durante la utilización u operación de los activos de tecnología de información debe ser reportado al área TI.
- El usuario tiene la obligación de almacenar la información según el proceso establecido por TI.
- Los usuarios no deben interferir en los procesos computacionales de la Compañía ni en el buen funcionamiento de los servicios y recursos de la misma mediante acciones deliberadas que disminuyan el desempeño, la capacidad o la seguridad de los equipos instalados. Se considerará justa causa de terminación del contrato el manejo indebido de los sistemas de tecnología.
- Está prohibido mover o reubicar los equipos de cómputo o de comunicaciones, instalar o desinstalar dispositivos, o retirar sellos de los mismos. Lo anterior es responsabilidad exclusiva del área TI, por lo tanto, en caso de requerir este servicio deberá solicitarlo.
- Es responsabilidad del usuario hacer uso del antivirus antes de copiar o ejecutar archivos para que los equipos no sean infectados. Los usuarios pueden pedir apoyo al departamento de sistemas para el uso de antivirus.

8 LICENCIAMIENTO DE SOFTWARE

- Todo software adquirido para el uso de la Compañía debe estar debidamente licenciado y es responsabilidad directa del área de TI cumplir la norma.
- La adquisición de cualquier software debe tener el aval y aprobación del área de TI.
- El área de TI debe realizar al menos una vez al año inspecciones a los equipos de la Compañía para asegurarse que el software instalado en los computadores se encuentre debidamente licenciado.
- Todos los productos de software que se utilicen deberán contar con su factura y licencia de uso respectiva; por lo que se promoverá la regularización o eliminación de los productos que no cuenten con el debido licenciamiento.

9 DERECHOS DE AUTOR

Para asegurarse de no violar los derechos de autor, no está permitido a los usuarios copiar ningún programa instalado en los computadores de la Compañía bajo ninguna circunstancia sin la autorización escrita del área de TI.

No está permitido instalar ningún programa en su computadora sin la autorización escrita de T.I Está prohibido cargue o descargue programas informáticos no autorizados de Internet, (Ej. Kazaa,) que pueden utilizarse para comercializar trabajos protegidos por los derechos de autor.

- Está prohibido realizar intercambios o descargas de archivos digitales de música (MP3, WAV, etc.) de los cuales no es el autor o bien no posee los derechos de distribución del mismo.
- Si un usuario desea utilizar programas informáticos autorizados por la Compañía en su hogar, debe consultar con el área de TI para asegurarse de que ese uso esté permitido por la licencia del editor.
- Los usuarios utilizarán los programas informáticos sólo en virtud de los acuerdos de licencia y no instalarán copias no autorizadas de los programas informáticos comerciales.
- Según las leyes vigentes de derechos de autor, las personas involucradas en la reproducción ilegal de programas informáticos pueden estar sujetas a sanciones civiles y penales, incluidas multas y prisión. No se permite la duplicación ilegal de programas informáticos.

10 SOPORTE

La Compañía contratará los servicios profesionales para la mesa de ayuda, cuyos funcionarios tendrán las siguientes atribuciones y/o responsabilidades:

- Podrán ingresar de forma remota a computadoras única y exclusivamente para la solución de problemas y bajo solicitud explícita del propietario de la computadora, y con los programas remotos autorizados por el área de TI (VNC,Teamviewer).
- Deben actualizar la información de los recursos de cómputo de la Compañía, cada vez que adquiera e instale equipos o software.
- Deben auditar periódicamente y sin previo aviso los sistemas y los servicios de red, para verificar la existencia de archivos no autorizados, música, configuraciones no válidas o permisos extra que pongan en riesgo la seguridad de la información.
- Realizar la instalación o adaptación de sus sistemas de cómputo de acuerdo con los requerimientos en materia de seguridad.
- Reportar al área de IT los incidentes de violación de seguridad, junto con cualquier experiencia o información que ayude a fortalecer la seguridad de los sistemas de cómputo.

11 EQUIPO DE COMPUTO

- Para el correcto funcionamiento del equipo de cómputo deberá realizarse como mínimo mantenimientos preventivos una vez al año, de acuerdo al plan de mantenimiento preventivo elaborado por el área TI.
- El área de TI será el encargado de asignar y distribuir el equipo de cómputo.
- IT deberá determinar la vida útil de los equipos de informática, con la finalidad de optimizar su uso.
- El área de TI instalará todas las aplicaciones de los equipos y programas informáticos utilizados por la Compañía.
- Verificará que los proveedores de programas de computadoras suministren los manuales correspondientes al funcionamiento de los equipos o programas especializados.
- El área de TI llevará inventario de hardware y software (programas) instalados en la Compañía el cual se consultará anualmente con contabilidad.

12 DESARROLLOS DE SISTEMAS DE INFORMACIÓN

- El área de TI podrá recurrir al desarrollo sistemas de información por “outsourcing”, cuando no cuente con el recurso humano y/o tecnológico necesario, para llevar a cabo los desarrollos de forma interna, además cuando otros factores como el tiempo no lo permitan.
- Las solicitudes de nuevos sistemas de información a desarrollar en la modalidad de “outsourcing”, deberán ser formalmente presentadas por las gerencias, en forma escrita e indicando en éstas los requerimientos generales por cubrir.
- Para los proyectos de desarrollo de sistemas de información por “outsourcing”, deberá seguirse el procedimiento de compras y contratación que permita las condiciones de la contratación, las tecnologías a utilizar y los mecanismos de control.
- El control y monitoreo del avance de proyectos de sistemas de información por “outsourcing” estará a cargo del área de TI.
- El área de TI estará pendiente que las empresas contratadas para el desarrollo de sistemas de información, vigilando que brinden la capacitación a sus funcionarios en administración, uso y mantenimiento del nuevo sistema de información.
- Los sistemas de información desarrollados por empresas externas, deberán ser entregados por éstas, de manera formal y debidamente documentados, incluyendo los entregables de documentación definidos por el área de TI tales como manuales de usuario y estructura técnica.

- Los programas desarrollados o adquiridos externamente serán de uso exclusivo de la Compañía y no se permite el uso para funciones que no correspondan a las operaciones normales de La Compañía.

13 SEGURIDAD

13.1 Seguridad del recurso humano

- Todo el personal nuevo de la Compañía, deberá ser notificado al área TI por la Gerencia Administrativa y Financiera de tal forma que se asigne los recursos correspondientes (Equipo de cómputo, creación de usuarios para accesos a las plataformas) o en caso de retiro, anular y cancelar los derechos otorgados como usuario informático junto con los accesos otorgados.
- El otorgamiento de acceso a la información está regulado mediante las normas y procedimientos definidos para tal fin.
- Todos los usuarios empleados, contratistas y terceras personas deberán devolver todos los activos de la Compañía que tengan a su cargo a la terminación de su empleo, contrato o acuerdo.

13.2 Acuerdo de confidencialidad

Los acuerdos de confidencialidad o no divulgación deben tener en cuenta el requerimiento de proteger la información confidencial, para identificar los requerimientos de los acuerdos de confidencialidad o no divulgación, se debe considerar los siguientes elementos:

- Una definición de la información a protegerse (por ejemplo, información confidencial)
- Responsabilidades y acciones de los de los firmantes para evitar la divulgación de información no autorizada (tal como “sólo lo que necesita saber” para el cumplimiento de su trabajo).
- Propiedad de la información, secretos comerciales y propiedad intelectual, y cómo se relaciona esto con la protección de la información confidencial.
- Uso permitido de la información confidencial y los derechos del firmante para utilizar la información.

13.3 Centro de datos

- El acceso al centro de datos es restringido y solo personal autorizado por el área de TI puede tener acceso a él.
- El acceso a los servidores de la Compañía ya sea usando la consola de administración local o una consola de administración remota es restringido y solo de uso personal autorizado por el área de TI.

- Limpiar los equipos al menos una vez por mes, que permita mantenerse libre de polvo.
- Estar libre de contactos e instalaciones eléctricas en mal estado.
- El Centro de datos debe mantener la temperatura del aire acondicionado entre 18 a 21 grados centígrados para evitar daños en los equipos o en los peores casos incidentes relacionados con fuego.
- Seguir los estándares de protección eléctrica vigentes para minimizar el riesgo de daños físicos de los equipos de telecomunicaciones y servidores.
- Contar con algún esquema que asegure la continuidad del servicio.
- Contar por lo menos un extintor de incendio adecuado y cercano al centro de datos.

13.4 Seguridad perimetral o red

- Los equipos electrónicos de gestión e infraestructura de la red de La Compañía serán instalados, configurados y mantenidos exclusivamente por el área de tecnología informática.
- No es permitido a ningún funcionario, excepto el área de tecnología informática, manipular los componentes activos de la red (switches, routers, dispositivos inalámbricos, cableado, etc.).
- El área de TI es la responsable de proporcionar a los usuarios el acceso a los recursos de conectividad.

13.5 Seguridad de la información

- Los usuarios deben guardar la información en las carpetas asignadas y de acuerdo a las tablas de retención documental, en el proceso que corresponda y de acuerdo a la política de archivo, para garantizar que dicha información sea respaldada.
- Se debe usar los canales para el almacenamiento provistos por el área de TI (FTP, DRIVE, CLOUD).
- Los equipos deberán contar con salvapantallas protegido por contraseña con un tiempo de espera de 10 minutos para evitar accesos no autorizados.
- Todos los accesos a los programas principales ERP’s estarán protegidos mediante un mecanismo de usuario y contraseña, así como permisos de acceso. De igual forma, las sesiones de Windows personales estarán protegidas con contraseña.
- Los usuarios deberán abstenerse de divulgar o compartir sus datos de acceso a los programas y sesiones de Windows.
- No es responsabilidad del área de TI la pérdida de información personal que se encuentre en cada equipo, la información corporativa debe ser trabajada en las

carpetas designadas para el backup vía FTP o desde las carpetas compartidas asignadas para cada área previamente configuradas en el servidor.

- Todo acceso a la información de la Compañía deberá tener las respectivas autorizaciones y accesos, que garanticen su respectiva seguridad, integridad y confidencialidad de la información almacenada.
- Los funcionarios deben realizar revisiones periódicas de su información almacenada con el fin de no mantener información innecesaria.
- Los funcionarios deben almacenar la información de manera ordenada y jerarquizada, todo esto para que el área de TI pueda hacer los respaldos correctamente y no exista pérdida de información relevante para el proceso laboral de los mismos funcionarios.
- Las copias de seguridad o respaldos se deben realizar de acuerdo al plan definido.

13.6 Restauración de las copias de seguridad

Las copias de seguridad se restaurarán de forma aleatoria con una frecuencia semestral, para validar la integridad de los datos respaldados.

13.7 Continuidad de los servicios TI

- La Compañía desarrollará un plan integral de continuidad de servicios de TI, y realizará mejoras de forma periódica o ante cambios significativos tales como procesos, y/o tecnología; para lo cual deberán participar activamente en dicha revisión las distintas áreas de los procesos identificados como críticos.
- Se debe tener disponibilidad de plataformas computacionales, comunicaciones e información, necesarias para soportar las operaciones definidas como de misión crítica de la Compañía en los tiempos esperados y acordados.
- El área de TI debe tener actualizada la documentación de roles detallados y tareas para cada una de las personas involucradas en la ejecución del plan de continuidad de servicios TI.
- La estrategia de continuidad de servicios de tecnologías de información y recuperación de la Compañía deberá diseñar e implementar actividades de prevención y de recuperación que ofrezcan las garantías necesarias para el restablecimiento de las operaciones de la Compañía después de un desastre.
- Se debe establecer el tiempo aceptable para recuperar los datos que tiene la Compañía en caso de una interrupción o desastre (RPO), y garantizar una recuperación eficaz.
- Se debe garantizar la divulgación y concientización de las políticas y del plan de

continuidad de servicios de TI y recuperación de desastres dentro de la Compañía.

- Se debe realizar copia de seguridad (Backup) de las aplicaciones, bases de datos y bodegas de archivos alojados en servidores, con el propósito de salvaguardar la información. Estas se deben realizar periódicamente por el área de TI de acuerdo las indicaciones establecidas en el plan de continuidad y se deberán almacenar en un sitio alterno fuera del edificio.

14 USO DE INTERNET

En caso de que se identifique que algún acceso que se solicite amenace la seguridad de la información de la Compañía no se concederán los permisos, tales como accesos remotos, VPN externas, carpetas públicas, etc.

14.1 Prohibiciones de internet.

- Páginas con contenido pornográfico.
- Descargue de ninguna aplicación sin autorización del área de tecnología.

15 CORREO ELECTRÓNICO

Teniendo en cuenta que el correo electrónico es una herramienta que provee la empresa para el cumplimiento de las funciones, toda la información manejada y almacenada es propiedad de la Compañía incluyendo las copias de seguridad del mismo.

- El manejo del correo se realizará de acuerdo a la política establecida.

16 RENOVACIÓN DE EQUIPOS

- Se deberán definir los tiempos estimados de vida útil de los equipos de cómputo y telecomunicaciones para programar con anticipación su renovación.
- Cuando las áreas requieran de un equipo para el desempeño de sus funciones ya sea por (5 años) sustitución o para el mejor desempeño de sus actividades, estas deberán realizar una consulta al área de tecnología a fin de que se seleccione el equipo adecuado. Sin el visto bueno de tecnología no podrá liberarse una orden de compra.

BIBLIOGRAFIA

- ICONTEC, ISO 27000:2013/ Sistema de seguridad de la información.
- MIN TIC/ Guía No. 3 Procedimiento de seguridad de la información. 25 de abril de 2016.
- ITL, Versión 3

17. CONTROL DE CAMBIOS

1	Septiembre 2019	Elaboración del documento

ELABORO	REVISO	APROBÓ
Carlos Andres Preciado	**Ivan David Lopez**	**Andres Oyola**
ADMINISTRADOR IT	SUBDIRECTOR IT	GERENTE