Plan De Seguridad Y Privacidad De La Información - TIC

2022

servicioalcliente@aquaterraesp.gov.co
www.aquaterraesp.gov.co
314 880 1262
604 551 51 84
Carrera 50 N° 42-100 local 209

EMPRESA DE SERVICIOS PUBLICOS DE GUARNE, CRECIENDO JUNTOS

1. INTRODUCCION.

El gran desarrollo de las tecnologías de las Telecomunicaciones y de la informática en las últimas décadas ha permitido el crecimiento exponencial del servicio de internet. Al presente todos pueden acceder a este servicio. La información ha sido globalizada.[1] Y con ella las amenazas que se pueden presentar en todo momento.

De acuerdo con lo anterior, la política de alto nivel o política general aborda la necesidad de la implementación de un sistema de gestión de seguridad de la información (SGSI) planteado desde la descripción del quién, qué, por qué, cuándo y cómo, en torno al desarrollo de la implementación del SGSI.

Es así como, teniendo en cuenta la importancia que tiene que la entidad defina las necesidades de sus grupos de interés, y la valoración de los controles precisos para mantener la seguridad de la información, se debe establecer una política que tenga en cuenta el marco general del funcionamiento de la entidad, sus objetivos institucionales, sus procesos misionales, y que este adaptada a las condiciones específicas y particulares para que sea aprobada y guiada por la Dirección.[2]

De esta forma se han definido las siguientes políticas para la empresa de Servicios públicos de Guarne EMPRESA DE SERVICIOS PÚBLICOS DE GUARNE . de tal forma que sean concisas, fáciles de leer y comprender, flexibles y fáciles de hacer cumplir para todos los miembros de la entidad.

2. PROPÓSITO

Este documento define políticas para el buen uso de las Tecnologías de la Información y Comunicación como herramienta dentro y fuera de la empresa, dando prioridad al buen nombre, seguridad, integridad y accesibilidad de la información.

[1] http://www.scielo.org.bo/scielo.php?script=sci_arttext&pid=S2071-081X2008000100008#:~:text=Las%20pol%C3%ADticas%20de%20seguridad%20se,y%20disponibilidad%20de%20la%20informaci%C3%B3n.
[2] https://www.mintic.gov.co/gestionti/615/articles-5482_G2_Politica_General.pdf

3. DEFINICIONES

Usuario: Persona que usa una o más herramientas de Tecnología de la Información y comunicación.

Encargado de sistemas: persona encargada de la administración y gestión de los elementos informático dentro de la compañía.

Base de datos: Motor que almacena la información relacional a nivel de tabal y registros y normalmente es común en más de un usuario.

Buscadores en Internet: Son páginas de internet que saca un listado de sitios basados en una palabra o cadena de caracteres, el más conocido es Google.

Debe, deberá: o cualquier conjugación del verbo deber es una obligación no una recomendación u opción. Según la RAE **Deber:** Estar obligado a algo por la ley divina, natural o positiva.

Escritorio: Para este documento cuando se hable de escritorio se refiere al fondo inicial del equipo de cómputo o la pantalla por defecto del equipo de cómputo, como ejemplo el Escritorio de Windows, o el inicio o pantalla inicial en un dispositivo móvil.

Equipos de cómputo: Son todos los Equipos electrónicos (Hardware) que almacenan, procesan o transmiten datos y/o información: Computadoras, Tablet, Teléfonos, Unidades de almacenamiento, Servidores, UTM, Impresoras, Scanner, entre otros.

Equipos computo ajenos a la empresa: Son todos los equipos de cómputo que no fueron asignados por la entidad para la realización del trabajo con EMPRESA DE SERVICIOS PÚBLICOS DE GUARNE ., ejemplo Teléfonos personales, Tablet personales, portátil de un visitante, Memoria de almacenamiento de un visitante o personal, entre otros.

Archivo o fichero informático: es un conjunto de bits que son almacenados en un dispositivo, ejemplo un archivo de Excel, un documento de Word, una canción en mp3, un ejecutable .exe, entre otros.

Carpeta o Directorios: para este documento, es un contenedor virtual en el que se puede almacenar una agrupación de archivo de datos, ejemplo la carpeta mis documentos, favoritos, escritorio de Windows, entre otros.

4. METODOLOGÍA

Este documento está desglosado en numerales de tal manera que se pueda usar como documento de consulta por los usuarios los cuales a su vez tendrán la asesoría del encargado de sistemas; se evitan las palabras técnicas, algunas frases o palabras son aclaradas en el numeral tercero, **Definiciones**; pueden existir ejemplos de nombres, marcas, entre otros con el único fin de hacer más clara la información.

5. POLÍTICA DE SEGURIDAD DE TECNOLOGÍA DE LA INFORMACIÓN

La junta directiva de EMPRESA DE SERVICIOS PÚBLICOS DE GUARNE , entendiendo la importancia de una adecuada gestión de la información, se ha comprometido con la implementación de un sistema de gestión de seguridad de la información buscando establecer un marco de confianza en el ejercicio de sus deberes con el Estado y los ciudadanos, todo enmarcado en el estricto cumplimiento de las leyes (marco legal) y en concordancia con la misión y visión de la entidad.

Para EMPRESA DE SERVICIOS PÚBLICOS DE GUARNE , la protección de la información busca la disminución del impacto generado sobre sus activos, por los riesgos identificados de manera sistemática con objeto de mantener un nivel de exposición que permita responder por la integridad, confidencialidad y la disponibilidad de esta, acorde con las necesidades de los diferentes grupos de interés identificados.

De acuerdo con lo anterior, esta política aplica a la Entidad, sus funcionarios, terceros, aprendices, practicantes, proveedores y la ciudadanía en general, teniendo en cuenta que los principios sobre los que se basa el desarrollo de las acciones o toma de decisiones alrededor del sistema general de seguridad de la información SGSI estarán determinadas por las siguientes premisas:

- Minimizar el riesgo en las funciones más importantes de la entidad.
- Cumplir con los principios de seguridad de la información.
- Cumplir con los principios de la función administrativa.
- Mantener la confianza de sus clientes y empleados.
- Apoyar la innovación tecnológica.
- Proteger los activos tecnológicos.
- Establecer las políticas, procedimientos e instructivos en materia de seguridad de la información.
- Fortalecer la cultura de seguridad de la información en los funcionarios, terceros, aprendices, practicantes y clientes de EMPRESA DE SERVICIOS PÚBLICOS DE GUARNE

- Garantizar la continuidad del negocio frente a incidentes.

EMPRESA DE SERVICIOS PÚBLICOS DE GUARNE ha decidido definir, implementar, operar y mejorar de forma continua un Sistema de Gestión de Seguridad de la Información, soportado en lineamientos claros alineados a las necesidades del negocio, y a los requerimientos regulatorios.

En concordancia con lo anterior se hacen explícitos los siguientes elementos:

5.1 Acceso a la información

Todos los funcionarios que laboran para EMPRESA DE SERVICIOS PÚBLICOS DE GUARNE . deben tener acceso sólo a la información necesaria para el desarrollo de sus actividades, en el caso de personas ajenas a EMPRESA DE SERVICIOS PÚBLICOS DE GUARNE . La oficina responsable de generar la información debe autorizar sólo el acceso indispensable de acuerdo con el trabajo realizado por estas personas y exigiendo previamente la justificación de la necesidad de dicha información, adicionalmente para otorgar el acceso a la información se tendrá en cuenta la clasificación de esta al interior de la entidad.

Mediante el registro de eventos en los diversos componentes de la plataforma tecnológica se efectuará seguimiento a los accesos realizados por los usuarios a la información de la empresa con el objeto de minimizar el riesgo de pérdida, integridad y trazabilidad de la información

Cuando se presenten eventos que pongan en riesgo la integridad, veracidad y consistencia de la información se deberán documentar y realizar las acciones tendientes a su solución.

Las transacciones en lo posible serán registradas con usuarios, fecha y hora para poder hacer seguimiento de todo lo que se realiza.

5.2 Administración de cambios

Todo cambio a un componente de la plataforma tecnológica relacionado con modificación de accesos, mantenimiento de software o modificación de parámetros debe realizarse de tal forma que no disminuya la seguridad existente.

Todo cambio que afecte la plataforma tecnológica debe ser requerido por los usuarios de la información y aprobado formalmente por el responsable de la administración del componente tecnológico, al nivel de gerencia, directores o a quienes estos formalmente deleguen, siempre con el acompañamiento del encargado de sistemas quien asegurará la trazabilidad y seguridad de la información.

En ninguna circunstancia un cambio puede ser aprobado, realizado e implantado por la misma persona o área.

Para la administración de cambios se efectuará el procedimiento correspondiente definido por EMPRESA DE SERVICIOS PÚBLICOS DE GUARNE . de acuerdo con el tipo de cambio solicitado en la plataforma tecnológica.

Cualquier tipo de cambio en la plataforma tecnológica debe quedar formalmente documentado desde su solicitud hasta su implantación, Este mecanismo proveerá herramientas para efectuar seguimiento y garantizar el cumplimiento de los procedimientos definidos.

Los cambios tecnológicos en software administrativo serán aprobados por el director del área afectada en este cambio, si el software no es administrativo será aprobado por el encargado de sistemas con el acompañamiento de gerencia financiera y con el acompañamiento de un tercero experto en el tema.

El cambio o actualización en la estructura de base de datos en el software administrativo deberá ser respaldado con copia de seguridad, el encargado de sistemas deberá estar enterado del cambio y del sitio donde se respalda.

5.3 Comunicaciones electrónicas

Las comunicaciones electrónicas dentro de EMPRESA DE SERVICIOS PÚBLICOS DE GUARNE . y de EMPRESA DE SERVICIOS PÚBLICOS DE GUARNE . hacia el exterior, deben establecerse de acuerdo con las normas de seguridad informática definidas y con los mecanismos que aseguren tanto la autenticidad de quienes realizan la conexión, como la confidencialidad, integridad y disponibilidad de esta.

Las comunicaciones electrónicas deben tener la característica de cordialidad y respeto, siguiendo los conductos regulares de EMPRESA DE SERVICIOS PÚBLICOS DE GUARNE . respetando el fuero y ámbito de decisión de las diferentes instancias.
Las comunicaciones electrónicas tendrán la misma validez que las comunicaciones realizadas en forma impresa en todos los casos que así la ley lo permita.

5.4 Transacciones electrónicas

Las transacciones que se realicen a través de medios electrónicos dentro de EMPRESA DE SERVICIOS PÚBLICOS DE GUARNE . deben establecerse de acuerdo con los estándares y mecanismos que aseguren la autenticidad de quienes realizan la transacción asegurando la confidencialidad e integridad de esta.

Se deben realizar verificaciones periódicas dependiendo del tipo de transacción, de la efectividad de los controles depende minimizar los riesgos de fraude a través de todos los procesos.

5.5 Administración de seguridad de la información

La administración de la seguridad de la información relacionada con el acceso a la información y las comunicaciones electrónicas serán responsabilidad del encargado de sistemas siempre con la revisión de un tercero experto, lo relacionado con las transacciones financieras electrónicas está a cargo de la Gerencia y la dirección financiera acompañado y soportado por el encargado de sistemas, quienes deben asegurar que se cumplan las políticas y procedimientos para tal fin.

5.6 Almacenamiento y respaldo de la información

La información más sensible está almacenada en los servidores de EMPRESA DE SERVICIOS PÚBLICOS DE GUARNE . a la cual sólo tiene acceso el área que la genera y el encargado de sistemas. El acceso está permitido únicamente a nivel del gerente y directores de área, se han definido procedimientos claros para respaldar diaria, semanal y mensualmente la información de estos. De tal forma que se mantienen copias de seguridad dentro de la compañía y en varias de sus localizaciones con el fin de preservar su integridad y fácil restablecimiento en caso de ser necesario.

Existen varios tipos de copias: la de usuario final se hace tres veces a la semana y se revisará mensualmente, es responsabilidad del encargado de sistemas la ejecución y administración de las tareas, es responsabilidad del usuario final el correcto almacenamiento de la información e informar cualquier cambio en el sistema de almacenamiento.

Las copias de servidores de bases de datos se realizarán una vez al día, se revisarán con pruebas de restauración mínima una vez al mes.
Las copias de servidor se hacen con imágenes que se copian semanales y se revisan cada 6 meses.

Todas las copias tendrán que ser padre hijo o mínimo las dos últimas copias, dependiendo del tamaño.

Todas las copias deberán tener como mínimo una réplica que estén fuera de las instalaciones o por lo menos muy alejadas de su origen.

5.7 Confidencialidad de la información

Para garantizar el acceso a la información por parte de los diferentes usuarios de EMPRESA DE SERVICIOS PÚBLICOS DE GUARNE . se tienen políticas establecidas que definen los niveles de acceso y los directores de cada área determinarán qué tipo de usuarios pueden consultarla o modificarla.

Las modificaciones serán revisadas y en caso de encontrar anomalías el encargado de sistemas con el acompañamiento del jefe de área identificará y analizarán el uso que se esté dando a la misma.

El contrato de cada uno de los empleados deberá registrar una cláusula de confidencialidad de la información.

5.8 Administración de activos tecnológicos.

La administración de los activos estará a cargo del encargado de sistemas bajo la revisión de la dirección financiera y comercial, y del Técnico Administrativo de Compras y Bienes.

5.9 Responsabilidad del personal

El personal de EMPRESA DE SERVICIOS PÚBLICOS DE GUARNE . que tenga acceso a una estación de trabajo o computador es responsable de sus contraseñas, las cuales son personales e intransferibles, no se escriben y se deben memorizar, las contraseñas deberán tener niveles altos de seguridad.

Es responsabilidad del usuario cambiar la contraseña en los siguientes casos:

- Cada que se cumple el tiempo estipulado
- En caso de que el personal del área de Sistemas por evento de mantenimiento la solicite
- Si se tienen dudas de que esta pudiera haber sido vista por alguna persona.

En lo posible cada usuario cambiará su contraseña en el momento que él lo requiera por sus propios medios, si necesita ayuda puede solicitar orientación al encargado de sistemas, pero sin que este conozca su contraseña personal.

Para los usuarios de equipos portátiles éstos deberán garantizar su uso sólo para gestiones relacionadas con su actividad laboral y quedará prohibido el uso del mismo por personas ajenas a la compañía y la instalación de software diferente a los estrictamente necesarios para desarrollar sus labores o software sin licencia.

5.10 Seguridad física y perimetral

EMPRESA DE SERVICIOS PÚBLICOS DE GUARNE . contará con seguridad física y perimetral en sus diferentes sedes manteniendo un riguroso mantenimiento y monitoreo. Las instalaciones deben contar con un CCTV -Circuito Cerrado de Televisión- y su respectivo DVR que garantice la reproducción de eventos ocurridos en semanas anteriores.

La entidad debe contar con espacios dedicados a el almacenamiento centralizado de la información con las condiciones necesarias físicas y de seguridad para proteger los activos de información.

5.11 Control de acceso

Todas las estaciones y equipos portátiles están habilitados con seguridad y control de acceso para que sean usados únicamente por las personas autorizadas.

Las contraseñas de red deben cumplir los siguientes requisitos:
mínimo 8 caracteres, debe contener letras mayúsculas, minúsculas y números, no se puede repetir la contraseña por lo menos en 6 ocasiones, el cambio debe ser cada 30 días máximo.

Después de 3 intentos la contraseña de red se bloquea y solo el encargado de sistemas podrá habilitar el uso de la cuenta.

Es responsabilidad del Técnico Administrativo de Talento Humano y Gestión de Calidad informar al encargado de sistemas el retiro de un empleado con el tiempo necesario para poder ser deshabilitado o borrado de los diferentes software o aplicaciones.

5.12 Desarrollo, adquisición y mantenimiento de sistemas de información.

Para el desarrollo de nuevos sistemas de información, adquisición y mantenimiento se deben realizar los estudios pertinentes, de ser necesario solicitar asesoría externa antes de realizar el proceso de contratación.

En todos los casos se firman contratos de confidencialidad de la información. Los desarrolladores solo podrán acceder a la información estrictamente necesaria, y en lo posible muestras de la información.

El software debe estar licenciado y la compra deberá ser aprobada por la gerencia.

El software no administrativo deberá estar licenciado y la compra deberá ser aprobada por la gerencia con el acompañamiento del encargado de sistemas.

La empresa debe contar con tecnología a nivel de software y hardware para los procesos de seguridad perimetral, interna, de acceso y respaldo de la información todo esto acompañado por el cumplimiento de las políticas definidas para tal fin.

La empresa entregará al encargado de sistemas los recursos necesarios en personal y tecnología para que al interior haya una administración del día a día en seguridad y tecnología, los proyectos nuevos o modificaciones importantes estarán acompañadas por terceros expertos.

Esta política se revisará y/o actualizará una vez al año por el encargado de sistemas y será informado a la gerencia a través de la dirección financiera y comercial.

6. POLITICAS DE USABILIDAD DE LOS RECURSOS DE TI COMO HERRAMIENTA DE TRABAJO PARA LA COMPAÑÍA.

EMPRESA DE SERVICIOS PÚBLICOS DE GUARNE . ha establecido las siguientes

normas que permiten garantizar el buen funcionamiento de todos los recursos informáticos disponibles en la compañía:

6.1 Uso de equipo de cómputo asignado por la empresa.

El usuario debe velar por el cuidado del equipo asignado, minimizar el daño físico, lógico, pérdida, deterioro.

El usuario no debe conectar ningún dispositivo diferente a los suministrados por la entidad como celulares, memorias USB, ventiladores, entre otros.

Si el usuario deja su puesto de trabajo debe bloquear manualmente el equipo.

El equipo debe apagarse diariamente y en forma correcta excepto los días de copia de seguridad o por algún trabajo planeado.

No se permite fumar, comer o beber mientras se está usando un equipo de cómputo.

Los equipos de la Compañía sólo deben usarse para actividades de trabajo con la compañía y no para otros fines, tales como juegos y pasatiempos, entre otros.

6.2 Movimientos o cambios en los equipos.

Cualquier movimiento temporal de equipos (ingreso, cambio, cambio de partes o retiro) de equipos de cómputo se debe informar al encargado de sistemas.

Solo el encargado de sistemas puede mover los equipos informáticos para ser reubicados o modificados.

Para retirar un equipo de la Compañía se requiere una autorización escrita del gerente o director de área.

La pérdida o robo de cualquier componente de hardware o programa de software debe ser reportada inmediatamente por escrito al encargado de sistemas.

6.3 Reporte de Incidentes.

Cualquier falla en los computadores o en las aplicaciones de la red debe reportarse inmediatamente al encargado de sistemas, con el fin de evitar la pérdida de datos y la inestabilidad en la comunicación con los servidores.

Queda totalmente prohibido la modificación de la configuración de hardware y software a los equipos de la entidad sin consentimiento del encargado de sistemas.

6.4 Software instalado en los equipos de cómputo asignados por la empresa.

Un usuario solo debe tener instaladas las aplicaciones proporcionadas por la

entidad para el uso de sus tareas diarias, ningún usuario podrá instalar o ejecutar una aplicación sin ser aprobada por el encargado de sistemas.

Está prohibido la ejecución o instalación de Juegos y demás distracciones en el puesto de trabajo.

Cada usuario debe ser responsable del manejo de las aplicaciones asignadas al puesto y la información que ingrese en la misma.

No se deben dejar aplicaciones de la red abiertas si no están siendo utilizadas.

Está prohibido traer, bajar, distribuir e instalar software sin licencia en los equipos informáticos de la compañía.

Solo está permitido modificar e instalar software por el encargado de sistemas.

6.5 Uso en los archivos almacenados en los equipos de cómputo asignado por la empresa.

En estos equipos únicamente se debe almacenar archivos necesarios para el trabajo en EMPRESA DE SERVICIOS PÚBLICOS DE GUARNE . No está permitido almacenar ningún tipo de archivos, programas o ejecutables diferentes a los suministrados por la entidad.

6.6 Compartir Carpetas o Archivos.

El usuario no podrá compartir carpetas o archivos desde su equipo de cómputo, solo se podrán compartir carpetas desde los servidores de archivos administrados por TI, las carpetas compartidas deberán ser accedidas sola y exclusivamente con los accesos necesarios para el cumplimiento de sus funciones, si usted o alguien tiene acceso a información no necesaria para la ejecución de sus funciones debe reportarlo al encargado de sistemas.

6.7 Correo electrónico, Chat o cualquier comunicación escrita en forma **electrónica.**

El usuario solo podrá utilizar estas herramientas asignadas por el área de TI para el trabajo con EMPRESA DE SERVICIOS PÚBLICOS DE GUARNE ., debe hacerlo con respeto y teniendo en cuenta que todo lo que envíe por este medio es información que compromete a la compañía y esta deberá ser tan precisa que no comprometa el buen nombre o la seguridad de la información.

Los contactos de estas herramientas deberán ser solo los necesarios para el cumplimiento de sus funciones con EMPRESA DE SERVICIOS PÚBLICOS DE GUARNE . Al recibir correspondencia debe asegurarse que quien envía es realmente su contacto, para esto es posible verificar el dominio del remitente (Ejemplo: @aquaterra.gov.co), simplemente preguntándole al remitente si es él

quien envía esta información, entre otras.

No se dirija a un link o abra archivos si no lo está esperando o no está completamente seguro que este archivo es de una fuente confiable y no tiene ningún riesgo al abrirlo o ejecutarlo, si presenta inquietud o dudas frente a esto consultelo con el encargado de sistemas para que se realicen las pruebas necesarias antes de ser abierto o ejecutado.

Cuando el usuario reciba mail de dudosa procedencia, éste se debe abstener de abrirlo y debe ser eliminado de todas las carpetas.

Está prohibido acceder o configurar otras cuentas de correo electrónico o chat tales como (Hotmail, Google, Yahoo!, Une, entre otras) que no sea la asignada por el servidor de correo de la entidad.

6.8 Transferencia de Archivos.

El envío o recepción de archivos se deberá hacer sola y exclusivamente por el correo electrónico, teniendo en cuenta que la información que se envía o recibe es propiedad de EMPRESA DE SERVICIOS PÚBLICOS DE GUARNE . y esto no puede poner en riesgo el buen nombre o la seguridad de la información.

Si por tamaño o tipo de archivo no se puede hacer por medio del correo electrónico, el encargado de sistemas habilitará a algunos usuarios un sitio por el cual puede transferir dejando claro que es responsabilidad de estos usuarios cualquier daño o perjuicio que se puede presentar por la transferencia de esto tanto para EMPRESA DE SERVICIOS PÚBLICOS DE GUARNE . o para terceros.

6.9 Uso del escritorio.

El usuario no debe almacenar ningún tipo de información en el escritorio de su equipo, este debe tener única y exclusivamente los accesos directos de aplicaciones para el cumplimento de sus actividades, todas estas aplicaciones deberán tener un usuario y contraseña para ingresar la información.

6.10 Equipos computo ajenos a la empresa.

Los equipos ajenos a la empresa y que están dentro de las instalaciones de la compañía podrán acceder a la red a través de conexión inalámbrica wifi exclusiva para invitados que se encuentre por fuera del segmento de red de los servidores.

Los visitantes deberán estar acompañados y supervisado por uno o varios usuarios quienes serán responsables de cualquier acto que ponga en riesgo a EMPRESA DE SERVICIOS PÚBLICOS DE GUARNE . el buen nombre o seguridad de la información.

6.11 Equipos computo ajenos a la empresa, con información de la empresa.

En algunas ocasiones los usuarios podrán almacenar información de EMPRESA DE SERVICIOS PÚBLICOS DE GUARNE . y en equipos ajenos a la empresa. Es su responsabilidad el almacenamiento, uso y divulgación por la persona responsable de la custodia de esta información y por la persona que cedió esta información por parte de la compañía, esta información sólo puede regresar nuevamente a la compañía por correo electrónico o por un medio autorizado.

6.12 Uso de dispositivos de almacenamiento externo.

No está permitido conectar ningún dispositivo de almacenamiento externo a los equipos de cómputo asignados por la compañía.

6.13 Uso información de la compañía.

La información de la entidad podrá ser publicada de acuerdo a su clasificación y las normativas legales, previa revisión y autorización del área que la genera.

6.14 Uso de las transacciones en las diferentes aplicaciones.

Los usuarios podrán hacer transacciones como consultar, crear, modificar o eliminar registros dentro de las aplicaciones para el ejercicio normal de sus funciones con permisos limitados y aprobados por el responsable del área en la cual trabaja.

Un usuario no puede acceder a información diferente a la necesaria para la ejecución de su trabajo o con los límites establecidos por el responsable del área.

Un usuario no puede manipular ningún registro a nombre de otro, el usuarios solo lo podrá hacer con sus credenciales de acceso.

6.15 Uso documentos e información del Usuario.

Los documentos, archivos deberán estar almacenados en las carpetas asignadas para la copia de seguridad en los equipos de cómputo asignados por la compañía.

6.16 Uso de canales internos de comunicación.

Los canales internos deben ser utilizados única y exclusivamente para la ejecución de las funciones propias por parte del usuario, el usuario no podrá acceder a recursos, peticiones internas o permitir el acceso de peticiones al interior que pongan en riesgo el buen nombre o la seguridad de la información.

6.17 Uso de canales externos de comunicación.

Los canales externos deben ser utilizados única y exclusivamente para la ejecución de las funciones propias por parte del usuario, el usuario no podrá acceder a sitios, peticiones externas o permitir el acceso de peticiones externas que pongan en

riesgo el buen nombre o la seguridad de la información.

6.18 Uso de los Buscadores en internet.

Los buscadores de internet listan una serie de sitios que en algunos casos pueden ser peligrosos, por tal motivo el usuario debe estar seguro de querer acceder al sitio web antes de dar click y si encuentra algo sospechoso deberá cerrar inmediatamente todos los navegadores y reportar si encuentra algún comportamiento atípico en el equipo de cómputo, ningún sito en el cual se pretende hacer una transacción de dinero podrá ser buscado desde un buscador, se debe digitar directamente en la barra de direcciones del navegador.

6.19 Uso Red Física, Cableado eléctrico y de datos.

La toma de datos solo se podrá conectar el equipo de cómputo asignado por la compañía, en la toma eléctrica de color naranja solo se podrán conectar los equipos de cómputo asignados por la compañía.

6.20 Uso Red Inalámbrica de datos WiFi.

Las redes inalámbricas solo se podrán utilizar para conectar los equipos de cómputo asignado por la entidad o los equipos externos teniendo cuidado de brindar las credenciales de autenticación de la red de invitados.

6.21 Invitados y externos.

Por ningún motivo un usuario externo puede conectarse a la red de datos, tomas de energía color naranja, el visitante siempre deberá estar acompañado y supervisado por la persona que lo invitó.

6.22 Almacenamiento de contraseñas.

Las contraseñas no deberán ser escritas o almacenadas en un archivo del equipo de cómputo, salvo los usuarios que manejan un número alto lo podrán almacenar en un software que esté encriptado con base de datos.

6.23 Transacciones Bancarias.

Las transacciones bancarias de la compañía sólo podrán hacerse desde los equipos asignados para este fin, en los equipos asignados para bancos solo se podrán hacer transacciones bancarias de la entidad.

6.24 Copias de seguridad archivos de Usuario.

Los usuarios deben mantener organizada la información de su equipo en una sola carpeta Documentos creada por el sistema operativo, con el fin de poder garantizar una copia de la información realmente importante para la compañía.

En la carpeta Documentos hay una llamada correos, esa carpeta no debe ser accedida, modificada o eliminada por el usuario.

La copia será como mínimo una vez a la semana.

6.25 Conexiones externas Escritorio remoto, VPN.

Actualmente la empresa cuenta con este servicio para los usuarios de la compañía, está dedicado sola y exclusivamente para trabajo con la compañía.

7. ACCESO AL CUARTO FRÍO DE CÓMPUTO DE TI.

Solo el encargado de sistemas o personal autorizado por gerencia puede ingresar al cuarto frio o manipular los equipos que allí se encuentran incluyendo servidores, Switch, File Server, Backups, DVR o Aire acondicionado.

Para esto se requiere que el ingreso al cuarto se realice mediante identificación biométrica, quedando guardado los datos de quien realiza el ingreso, así como la fecha y hora del mismo.

8. EL CONDUCTO REGULAR DE SOPORTE.

Las fallas o solicitudes se deben realizar en primer lugar al encargado de sistemas, si este no responde de manera adecuada a la solicitud se hablará con el supervisor del contrato o jefe inmediato y por último se podría elevar una queja formal a gerencia.

El mal uso de las herramientas de TI acarreará sanciones definidas por el área de GESTION HUMANA.