CONTENIDO

1 DEFINICIONES

- BACKUP: una copia de seguridad, respaldo de los datos originales que se realiza con el fin de disponer de un medio para recuperarlos en caso de su pérdida.
- CORREO ELECTRÓNICO: es un servicio de red que permite a los usuarios enviar y recibir mensajes mediante redes de comunicación electrónica.
- TI: Tecnología Informática.
- TIC: Tecnología de la Información y las Comunicaciones.
- USUARIO: es una persona que utiliza una computadora o un servicio de red. Los usuarios de sistemas informáticos y productos de software generalmente carecen de la experiencia técnica necesaria para comprender completamente cómo funcionan.
- Datos personales: toda información que, recopilada y puesta en relación, pueda llevar a la identificación de una persona determinada.
- Recursos informáticos: son componentes físicos o virtuales necesarios para que una computadora o sistema de Gestión de la información funcione adecuadamente.
- Recursos TI: se refiere al conjunto de hardware, software, redes y servicios necesarios para el funcionamiento de los sistemas informáticos de la empresa.

2 OBJETIVO

Orientar a todos los trabajadores del Proyecto Concesionario Autopista Magdalena Medio S.A.S en las prácticas de seguridad, con el fin de preservar la confidencialidad, la integridad, y la disponibilidad del sistema de información.

3 ALCANCE

La presente política debe ser cumplida por todos los trabajadores, contratistas y terceros de todas las gestiones organizacionales del Concesionario Autopista Magdalena Medio S.A.S, que tengan acceso a sus instalaciones y/o servicios tecnológicos. Lo anterior, con el fin de proteger los servicios tecnológicos y de comunicaciones de la sociedad.

4 RESPONSABLES

4.1 Usuarios Y Terceros

Los usuarios y terceros de la Sociedad deberán:

- Observar y cumplir las directrices de la presente Política;
- Preservar la integridad y mantener la confidencialidad de la información que utilizan, así como asegurar y proteger los respectivos recursos de procesamiento de información;
- Mantener la confidencialidad de la contraseña, para acceder a los recursos y sistemas de la Sociedad, y a la información externa adquirida;
- No compartir, de ninguna manera, información confidencial con otros que no tengan la debida autorización de acceso;
- No desconocer ni incumplirla legislación de propiedad intelectual vigente.
- Proteger, a nivel físico y lógico, los activos que almacenan o procesan datos de la Sociedad, relacionados con el desarrollo de sus actividades;
- Al acceder o procesar Datos Personales, cumplir con los deberes de confidencialidad de los Datos Personales;
- Comunicar inmediatamente a su director y/o al Ingeniero de TI, cualquier irregularidad o desviación.

4.2 Directores de área

Además de la responsabilidad de los Usuarios y Terceros mencionada en el punto anterior, los directores también tienen la responsabilidad de:

- Influir en su equipo de trabajo sobre la importancia de proteger la información de la Sociedad, y garantizar el cumplimiento de las pautas establecidas en este documento;
- Cuando sea necesario, documentar pautas específicas para clasificar la información, regulando los niveles de confidencialidad de la información que generan y procesan, así como los derechos de acceso a dicha información;
- Definir qué usuarios y terceros, bajo su liderazgo, pueden acceder a la información del Concesionario Autopista Magdalena Medio S.A.S, siguiendo pautas de clasificación de información y los perfiles;
- Revisar periódicamente los derechos de acceso a la información del Concesionario Autopista Magdalena Medio S.A.S de sus empleados y sus terceros;
- Decidir, junto con Gestión de Talento Humano y el equipo jurídico, sobre las medidas a tomar en caso de violación de las normas de protección establecidas.

4.3 Equipo de tecnología de la información

El equipo de TIC es responsable de:

- Establecer las reglas, procedimientos y procesos para la protección de los activos de tecnología de la información del Concesionario.
- Revisar periódicamente las normas de protección establecidas;
- Restringir y controlar el acceso y los privilegios de los Usuarios, en alineación con las necesidades de la empresa;
- Asegurar la capacitación de los Usuarios, sobre los riesgos asociados con la Seguridad de la Información;
- Detectar, identificar, registrar violaciones relevantes y significativas o intentos de acceso no autorizados para acciones correctivas, legales y de auditoría.

5 DESARROLLO DE LA METODOLOGÍA / SEGURIDAD DE LA INFORMACIÓN

5.1 Propiedad de los recursos y uso de la información

- Los Recursos Informáticos puestos a disposición de los usuarios, son propiedad del Concesionario y estos están configurados, con el fin de garantizar la seguridad de la información. Toda la información producida, transmitida o almacenada a través de los Recursos Informáticos del Concesionario pasa a ser de su propiedad.
- Los recursos de TI disponibles deben utilizarse para satisfacer las necesidades del trabajo del usuario. Por lo tanto, no pueden ser utilizados para expresar opiniones, distribución o acceso de material protegido por derechos de autor, procesamiento de Datos Personales, fuera de las hipótesis legales permitidas, anuncios, bromas, contenido pornográfico, cadenas solidarias, juegos electrónicos, o para difundir opiniones de carácter político, religioso o discriminatorio.
- El uso de los recursos informáticos disponibles para asuntos individuales, como correos electrónicos privados, acceso a bancos y otros, debe hacerse de manera razonable y mesurada, para no causar sobrecarga en la red. Por razones de seguridad, el Concesionario puede bloquear el acceso a sitios web sospechosos, o sitios web con dudosa reputación.
- Toda la información del Concesionario no puede ser transferida a los Recursos de TI privados del usuario, como correo electrónico, OneDrive u ordenadores privados, así como utilizada o compartida de una manera diferente a la prevista en la presente Política.

5.2 Privacidad

El Concesionario, valora la privacidad de sus empleados y terceros, y se compromete a respetarla. Sin embargo, los usuarios deben ser conscientes de que el Concesionario,

tiene el derecho de monitorear cualquier acceso, recuperar o capturar cualquier actividad electrónica que ocurra a través del equipo o la comunicación de la empresa (por ejemplo, correos electrónicos e Internet). El seguimiento tiene por objetivos:

- Cumplimiento de la disposición legal;
- Hacer cumplir los términos de la presente política;
- Responder a quejas de contenido que viole los derechos de terceros;
- Proteger derechos, propiedad, intereses o mantener la seguridad del Concesionario o de terceros.

Si el usuario necesita almacenar temporalmente archivos privados en el equipo corporativo, le corresponde a él llevar a cabo, el proceso de eliminación después de su uso. No obstante, la empresa queda exenta de responsabilidad ante un posible incidente de seguridad que afecte, total o parcialmente, la integridad, confidencialidad o disponibilidad de este.

5.3 Gestión de incidentes de seguridad de la información

Definición incidente de TI: es cualquier interrupción en los servicios de TI de una organización que afecta cualquier elemento asociado, desde un solo usuario hasta toda la empresa. En pocas palabras, un incidente es cualquier cosa que interrumpe la continuidad del negocio.

Ejemplos de incidentes TI:

- Un acceso no autorizado.
- El hurto de contraseñas.
- Prácticas de Ingeniería Social.
- La utilización de fallas en los procesos de autenticación para obtener accesos indebidos. El hurto de información.
- El borrado de información de terceros.
- La alteración de la información de terceros.

Para la gestión de incidentes en el Concesionario, se tienen los siguientes parámetros:

- Todos los colaboradores y terceros del Concesionario tienen la responsabilidad de reportar de forma inmediata los eventos, incidentes o debilidades en cuanto a la seguridad de la información que identifiquen o se presenten.

- Se debe dar un tratamiento adecuado a todos los incidentes de seguridad de la información reportados.

- Se deben establecer las responsabilidades de la gestión de incidentes de seguridad de la información.

- Se debe realizar sensibilización a todos los usuarios, sobre los incidentes de seguridad de la información.

- El Equipo de TIC debe tener implementado un proceso de gestión de incidentes de

seguridad de la información, de manera que, en caso de un evento, se produzca una acción rápida y coordinada con el fin de preservar los criterios de confidencialidad, integridad y disponibilidad de los sistemas de información.

- El equipo de TIC proporcionará mecanismos y controles para detectar incidentes de seguridad relacionados con el entorno informático bajo su responsabilidad.

5.4 Copia de seguridad

- Es responsabilidad del equipo de TIC, asegurar la formalización de los procedimientos de Backus y recuperación, asegurar que dichos procedimientos sean actualizados y probados regularmente, con el fin de asegurar la Disponibilidad de Información, registros legales e impuestos históricos.

- Se explica a los usuarios el uso de OneDrive, la sincronización que realizamos a las carpetas principales de su equipo (Escritorio, Documentos e Imágenes). Esta acción la realiza el sistema directamente en tiempo real de manera inmediata y constante.

6 ELEGIBILIDAD Y USO DE LOS RECURSOS DE TI

6.1 Equipos de Tecnología

- Corresponde al director de área y al equipo de TIC, establecer los criterios de elegibilidad del equipo informático que se proporcionará a los usuarios, para el desempeño de sus actividades.

- Solo los equipos corporativos aprobados y autorizados, incluidos entre otros, portátiles, computadoras de escritorio e impresoras, pueden acceder a los datos almacenados en los recursos y sistemas de información del Concesionario.

- Todo equipo debe tener una configuración, que impida que el usuario tenga privilegios administrativos, evitando así la instalación de software no autorizado;

- Todos los equipos deben tener protección Antivirus;

- El Concesionario, asignará los recursos tecnológicos necesarios al personal, con el fin de que se usen para el cumplimento de sus funciones mantenimiento buenas prácticas y cumpliendo con las políticas establecidas en este manual.

- La instalación siempre estará bajo la responsabilidad del área de TIC, y, por ende, es el único personal responsable e idóneo para atender requerimientos de instalación, así también el único con las claves de administrador para la instalación.

- Si se encuentran usuarios con software instalado sin autorización en el equipo de cómputo de la organización, se procederá con la desinstalación de este sin previo aviso. El personal de TIC que haga la desinstalación de este debe reportar a la Dirección Administrativa y a la Dirección del área correspondiente o donde pertenece el profesional o colaborador.

- El área de TIC es la responsable de mantener los equipos actualizados. Durante esta actividad, se validará el correcto uso de los equipos.

- Los reportes de falla deben ser notificados al área de TIC.

6.2 Solicitud de equipo

- En caso de admisión de nuevo trabajador o identificación de necesidad de un usuario,

  corresponde al equipo de Gestión de Talento Humano, informar al área TI, sobre los requerimientos tecnológicos reportados en la solicitud de personal.

- Luego el Ingeniero de TI, revisará el presupuesto y validará la disponibilidad de los recursos de TI.

6.3 Devolución de equipos

- En casos de retiro del colaborador/trabajador, el equipo de Gestión de Talento Humano debe informar al área de TI, para la devolución inmediata del equipo, mediante acta de entrega de equipos al Ingeniero de TI (GA-F-008 ACTA RECIBO DE EQUIPOS).

6.4 Cuidado en el uso del equipo

- Todo usuario que utilice equipos informáticos puestos a disposición por el Concesionario tiene la responsabilidad de velar por el equipo, así como de comprender, respetar y seguir esta Política.

Se deben observar las siguientes precauciones:

- No está permitido intercambiar piezas sin el análisis y la aprobación del TIC local responsable;

- Precaución al transportar notebooks fuera del entorno corporativo, preservando así el equipo y la información contenida en ellos;

- Es responsabilidad del usuario almacenar en lugares no visibles cuando se transportan en vehículos de motor.

- Es una obligación evitar comer encima del equipo y a su vez mantener alejado todo tipo de bebidas, esto con el ánimo de evitar accidentes.

- Para una duración más prolongada de la batería, "se recomienda que el equipo esté conectado a la corriente solo cuando se esté cargando y no dejarla siempre conectada".

6.5 Pérdida o hurto

Inmediatamente posterior a la pérdida y/o hurto, se deben efectuar las siguientes acciones:

  - Instaurar el registro respectivo ante las autoridades competentes y este

enviarlo al director del área y al equipo de TI; e informar inmediatamente el suceso a la Dirección Administrativa y al equipo TI;

- El área de TI debe realizar los procedimientos necesarios (cambio de contraseña de la cuenta de Office 365).

7 TELEFONÍA MÓVIL

- El Concesionario a través del equipo de TI, pone a disposición los modelos de teléfonos inteligentes a sus colaboradores, estos acordes a sus necesidades que requiera en el ejercicio de su labor para el que fue contratado.

- Dichos dispositivos tienen especificaciones suficientes para cumplir con todas las aplicaciones necesarias, para el desarrollo de las actividades en la empresa y son asignados de acuerdo con el perfil del integrante y las necesidades del área.

- Las solicitudes deben hacerse formalmente mediante correo electrónico al área de TI.

7.1 Devolución de Telefonía móvil

- Para devolver el equipo de telefonía móvil, el usuario debe eliminar la cuenta de correo electrónico vinculada al dispositivo.

- En el caso que el usuario NO devuelva el equipo asignado, este deberá asumir el costo de compra.

7.2 Mantenimiento

- Si el equipo presenta algún tipo de problema técnico, el Usuario deberá informar al Ingeniero TI.

7.3 Pérdida, hurto o daño

- En casos de pérdida, hurto o daño del dispositivo, el usuario deberá comunicarse inmediatamente con el ingeniero TI, para informar de lo sucedido y solicitar el bloqueo de la línea si es necesario.

- En casos de hurto, el usuario deberá presentar el registro respectivo ante las autoridades competentes y enviarlo a la Dirección Administrativa y al equipo al área de TI, para que se puedan tomar las medidas necesarias con respecto a la sustitución del equipo.

- Si se comprueba que el teléfono inteligente es perdido por descuido del usuario éste asumirá el costo del equipo asignado, en caso contrario el costo de la sustitución o reparación será a juicio del CONCESIONARIO AUTOPISTA MAGDALENA MEDIO S.A.S

8 CORREO ELECTRÓNICO CORPORATIVO

Establecer las directrices generales del buen uso y buenas prácticas del correo electrónico del CONCESIONARIO AUTOPISTA MAGDALENA MEDIO S.A.S

.

8.1 Usos aceptados

- Se debe utilizar exclusivamente para las actividades propias del desempeño de las funciones o actividades laborales. No se debe utilizar para otros fines.

- Se debe utilizar de manera ética, razonable, eficiente, responsable, no abusiva y sin generar riesgos para la operación de equipos o sistemas de información e imagen del Concesionario.

- Todos los colaboradores y terceros que son autorizados para acceder a la red de datos y los componentes de tecnología de información son responsables de todas las actividades que se ejecuten con sus credenciales de acceso a los buzones de correo, y automáticamente aceptan las políticas de Tecnología del Concesionario.

- El servicio de correo electrónico debe ser empleado para servir a una finalidad operativa y administrativa con relación a las funciones encomendadas.

- Todas las comunicaciones establecidas mediante este servicio, por medio de sus buzones y copias de seguridad, se consideran de propiedad del Concesionario y pueden ser revisadas o auditadas por el administrador del servicio en cualquier momento; ejecutando así, seguimiento, vigilancia y control, o en caso de una investigación o incidentes de seguridad de la información.

- Todos los mensajes enviados deben respetar el estándar del formato e imagen corporativa definido por el Concesionario. Se deberá conservar los estándares previamente ya definidos como firmas, tipo de letra, logos y colores.

- La única plataforma de correo electrónico controlada es la asignada directamente por el área de Tecnología de la Información, las cuales cumplen con todos los requerimientos técnicos y de seguridad necesarios para evitar ataques informáticos, virus, spyware y otro tipo de software o código malicioso.

- Se realiza copia de respaldo de información a los registros de buzón de correo (e-mail) cuando el buzón llegue a 94% de capacidad, este Backus se efectúa con el fin que el usuario pueda eliminar email, para liberar espacio en buzón, el borrado de E-mail se dará del más antiguo al más reciente. El Backus estará en custodia de TIC y a disposición del usuario correspondiente al buzón y del jefe inmediato.

- El tamaño del buzón de correo electrónico es de 50 GB para todo el personal, la capacidad especifica es definida y administrada por la oficina de Tecnología de la Información de la empresa.

- Todos los colaboradores y terceros son responsables de informar si tienen accesos a contenidos o servicios que no estén autorizados y no correspondan a sus funciones o actividades designadas en la organización, para que de esta forma el área de TIC realice el

ajuste de permisos requerido.

- El usuario debe reportar cuando reciba correos de tipo SPAM; es decir, correo no deseado o no solicitado, correos de dudosa procedencia o con virus a TIC; con el fin de tomar las acciones necesarias que impidan el ingreso la red de la organización.

- Cuando un colaborador se retire del Concesionario, el área de Gestión de Talento Humano deberá informar de manera inmediata, con el fin de bloquear y resguardar los accesos a correo electrónico e información de este.

- Los mensajes y la información contenida en los buzones de correo son de propiedad del

  Concesionario.

- Los archivos que se encuentren sincronizados del usuario, y que estén en la nube de su buzón, una vez se retire de la organización serán descartados, siendo este el Backus usuario. Así mismo, esta información quedará bajo la custodia de TIC, y podrá ser consultada cuando se requiera, por parte del jefe del área encargada, o una en la jerarquía superior dentro del organigrama.

- Cada usuario se debe asegurar que, en el reenvió de correos electrónicos, la dirección de destino sea correcta, de manera que este siendo enviado a los destinatarios que son. Si tiene lista de distribución, también se deben depurar.

- El envío de información a personas no autorizadas es responsabilidad de quien envía el mensaje de correo electrónico.

- La información almacenada en los archivos de tipo .PST, (Un archivo de carpetas personales pst es un archivo de datos de Outlook que almacena sus mensajes y otros elementos en su equipo) es responsabilidad de cada uno de los Usuarios, y cada usuario debe realizar la depuración periódica del buzón para evitar que alcance su límite.

- Los grupos creados en la plataforma de correo (Facturación, Correspondencia, etc.), deben tener una persona responsable que haga depuración del buzón periódicamente.

- Todo usuario es responsable de reportar los mensajes, cuyo origen sean desconocidos, y asume la responsabilidad de las consecuencias que puede ocasionar la ejecución de cualquier archivo adjunto. En los casos en que un usuario o tercero desconfié del remitente de un correo electrónico, debe remitirse al área de TIC, vía celular, con el fin de elevar la consulta y evitar en reenvió del mensaje.

- Si una cuenta de correo es interceptada por personas mal intencionadas o delincuentes informáticos (crackers), o se reciba cantidad excesiva de correos no deseado (SPAM), el Área de TIC, actuara según sea el caso.

- Ningún usuario y/o tercero debe suscribirse en boletines en línea, publicidad o que no tenga que ver con sus actividades laborales.

- El usuario y/o tercero no debe responder mensajes donde les solicitan información personal o financiera que indican que son sorteos, ofertas laborales, ofertas comerciales o peticiones de ayuda humanitaria; por el contrario; deben notificar a TIC, con el fin de ejecutar las

acciones pertinentes.

- Los buzones son dados de baja de la plataforma, un mes después que el usuario haya sido bloqueado por el retiro de la empresa o antes de ser necesario; esto con el fin de atender requerimiento de usuarios nuevos que requieren buzón, pero para ello, siempre se garantizara un Backus, de la información allí contenida.

- Todos los usuarios de correo electrónico se les notificará que, el tamaño máximo para recibir o enviar mensajes es de 25MB (incluyendo la suma de todos los adjuntos), tener en cuenta que se debe validar que remitente cuando es externo tenga la capacidad de recibir este mismo tamaño de 25 MB.

8.2 Usos no permitidos

- Envío de correos masivos, que no hayan sido previamente autorizados por los directores de cada área.

- Envío, reenvío o intercambio de mensajes no deseados o considerados como SPAM, cadena de mensajes o publicidad.

- Envío o intercambio de mensajes que promuevan discriminación de raza, nacionalidad, genero, edad, estado marital, orientación sexual, religión o discapacidad, o que inciten a realizar prácticas ilícitas o promuevan actividades ilegales.

- Envío de mensajes que contengan amenazas o mensajes violentos.

- Crear, almacenar o intercambiar mensajes que atenten contra las leyes de derechos de autor.

- Divulgación no autorizada de información de propiedad del Concesionario.

- Enviar, crear, modificar o eliminar mensajes de otro usuario sin su autorización.

- Abrir o hacer uso y revisión no autorizada de la cuenta de correo electrónico de otro usuario sin su autorización.

- Adulterar o intentar adulterar mensajes de correo electrónico.

- Enviar correos masivos, con excepción directores o superior, quienes sean previamente autorizados para ello, o que en calidad de sus funciones amerite la excepción.

- Cualquier actividad con propósito inmoral, ilegal diferente a los aquí expresado en este manual de políticas TIC del Concesionario.

9 CANALES DE INTERNET

9.1 Usos aceptados

- Este servicio es de uso exclusivo para el cumplimiento de las funciones de todos los colaboradores que, dentro de sus funciones, requieran este tipo de servicio.

- Los usuarios son responsables de evitar que, con las prácticas puedan poner en riesgo los activos digitales, tecnológicos e integridad de la Sociedad.

- Todas las comunicaciones que se establezcan por este medio pueden ser auditadas bien sea por el área TI, previa autorización de la Gerencia y/o por el área encargada del sistema de auditorías Internas del concesionario (cuando sea necesario).

- Los usuarios son responsables de las credenciales de acceso vía WIFI, cuando así sean entregadas.

- Todos y cada uno de los usuarios del Concesionario, son responsables de dar buen uso de este recurso; por tal motivo, está prohibido realizar prácticas ilícitas o mal intencionadas, que atenten contra terceros y contra la organización. Esto sustentado bajo la legislación vigente (colombiana) y las políticas contenidas en este manual.

- Este recurso puede ser utilizado para uso personal, siempre y cuando se realice de manera ética, razonable, responsable, no abusiva y sin afectar la productividad del Concesionario.

9.2 Usos no permitidos

- No se permite la conexión de celulares no corporativos.

- No se permite la conexión de equipos de cómputo que no cuenten con un antivirus licenciado.

- Los Usuarios invitados deben cumplir con las políticas y requerimientos de conexión del Concesionario.

- No está permitido instalar programas de chat personales, redes sociales, juegos, foros, etc., que afecten la integridad y confidencialidad de la información.

- No se permite descargar ningún tipo de software, que no esté autorizado por el jefe inmediato y previa validación área de TI, sobre el licenciamiento de este.

- El acceso a internet está destinado únicamente para fines corporativos, está totalmente prohibido el uso de Internet para consultas personales, videos de YouTube, redes sociales, etc.; que no hagan parte de la empresa.

10 WHASAPP

WhatsApp queda establecido como uno de los soportes de comunicación desde el ámbito profesional, es decir quienes cuentan con teléfonos suministrados por la empresa a nivel corporativo e institucional y que han aceptado el uso de los mismos, esto debido a su versatilidad y facilidad de uso. Por esta razón esta aplicación o tipo de mensajería la adoptamos como una evidencia objetiva de comunicación, podemos afirmar así y darnos cuenta de que el objetivo de WhatsApp es lograr adaptar las características de una comunicación oral a la escrita, por ende, la declaramos valida dentro de nuestra Organización.

11 LICENCIAS DE SOFTWARE

11.1 Uso e instalación de software

- Las licencias de software que proporciona el Concesionario se deben utilizar exclusivamente para las actividades propias del desempeño de las funciones o actividades laborales. No se debe utilizar para otros fines.

- Las actualizaciones de software solo podrán ser efectuadas por el personal TI,

- El licenciamiento de Microsoft, solo se puede usar en los equipos de propiedad del Concesionario, como son por suscripción de cuenta de usuario. No deben ser usados en equipos diferentes.

- Las licencias de AUTOCAD, LT, CIVIL, ARCGIS, ACROBAT PRO, entre otros, son asignadas por suscripción al integrante, y estas no puede estar asociadas en equipos diferentes que no sean propiedad del Concesionario.

- El equipo de TI podrá desactivar las licencias, en caso detecte mal uso de estas.

11.2 Asignación de licencias de software

- Las licencias de software serán asignadas, según aprobación a nivel de Gerencia para respaldar su uso.

- La asignación de una licencia otorga el derecho de uso por el periodo asignado, cuando dicho tiempo está próximo a caducar el colaborador solicitará la extensión para garantizar la continuidad de las actividades requeridas por el Software para el periodo que fuese necesario.

11.3 Uso e instalación de software

- Si se requiere instalar software adicional, este debe ser de uso libre y cumplir con los estándares de seguridad establecidos por el Concesionario. La instalación deberá contar con la validación y autorización del equipo de TI.

- Hasta el momento, los siguientes aplicativos están aprobados para su uso:

    - PDF24
    - Google Earth
    - Google Chrome
    - Adobe Reader
    - QGIS
    - DWG
    - BaseCamp
    - Zoom
    - R Studio
    - Java

- Global Mapper
- Agisoft Metashape

- El equipo de TI supervisará y controlará la instalación de estas herramientas para garantizar su correcto funcionamiento y compatibilidad con los sistemas corporativos.

12 POLITICA CONTROL DE ACCESO

12.1 Control de acceso a redes cableadas o WIFI.

- El área TI, se encargará de asignar la red y contraseña directamente a los equipos en las sedes administrativas del Concesionario.

- En caso de que se entregue las credenciales a personal del Concesionario, estas no pueden ser filtradas a otros usuarios (divulgadas).

12.2 Gestión de acceso a usuarios

- Los usuarios pueden solicitar el cambiar sus claves de acceso periódicamente, inclusive antes de que el director lo solicite, como política previa configurada o expire.

- Las contraseñas deben contener mayúsculas, minúsculas, números y por lo menos un carácter especial y de una longitud no menor a ocho caracteres.

- El sistema debe obligar al usuario a cambiar la contraseña por lo menos 1 vez, cada 180 días.

- Todos los usuarios en su primer inicio de sesión deben cambiar las contraseñas suministradas por TI.

- Todos los usuarios deben dar un buen uso a las claves de acceso suministradas, y no deben escribirlas o dejarlas a la vista.

- El área TI, debe cambiar todas las claves de acceso que vienen predeterminadas por el fabricante, una vez instalado y configurado el software o el hardware (por ejemplo, router, impresoras, Switch, herramientas de seguridad, correo, etc.).

- Reportar al área de Tecnología y sistemas de información, sobre cualquier incidente o sospecha de que otra persona este utilizando su contraseña o usuario asignado.

13 DOCUMENTOS RELACIONADOS

- Política de seguridad de la información.

- GA-F-30: ACTA PARA DAR DE BAJA ACTIVOS FIJOS, Aceptación de responsabilidad y confidencialidad (accesos a equipos, plataformas y redes sociales) acuerdo de responsabilidad y confidencialidad usuario.

* * * * *

CONTROL DE CAMBIOS					
Versión	**Fecha**	**Descripción**	**Elaboró**	**Revisó**	**Aprobó**
1	06/03/2024	Creación	Ingeniero TI Coordinación de Calidad	Dirección Administrativa	Gerente General
2	20/02/2025	Actualización / Redacción y ajustes al documento	Ingeniero TI Coordinación de Calidad	Dirección Administrativa	Gerente General
3	03/03/2025	Actualización / WhatsApp validado como soporte de comunicación – Pág. 14	Ingeniero TI Coordinación de Calidad	Dirección Administrativa	Gerente General

Ing. Salomón Niño Ortiz
Gerente General
Autopista Magdalena Medio S.A.S.
NIT. 901.602.085-8