1. OBJETIVO

Determinar los lineamientos necesarios para garantizar la protección de los activos de información ante cualquier posible amenaza o materialización de los riesgos asociados al tratamiento de esta.

2. ALCANCE

La presente política aplica para todos los procesos, actividades y partes interesadas de **VEHÍCULOS DEL LLANO SAS**, así como todos aquellos que cuenten con acceso o administren información confidencial.

Índice

3. DESARROLLO

3.1 Política general de seguridad y privacidad de la información.

La empresa **VEHÍCULOS DEL LLANO S.A.S**, entendiendo la importancia de una adecuada gestión de la información, se ha comprometido con la implementación de directrices que garanticen la seguridad de la información buscando establecer un marco de confianza en el ejercicio de sus deberes con sus partes interesadas y todo enmarcado en el estricto cumplimiento de las leyes y en concordancia con la misión y visión de la entidad.

Para **VEHÍCULOS DEL LLANO S.A.S**, la protección de la información busca disminuir el impacto generado sobre los activos de información y sus riesgos asociados e identificados de manera sistemática, se tiene como objetivo el mantener un nivel de exposición que permita responder por la integridad, confidencialidad y la disponibilidad de la misma, acorde con las necesidades de los diferentes grupos de interés identificados.

A continuación, la empresa da a conocer los siguientes 11 principios de la seguridad de la información:

a) Las responsabilidades frente a la seguridad de la información serán definidas, compartidas, publicadas y aceptadas por cada uno de los colaboradores, proveedores, socios del negocio o visitantes.

b) Protegerá la información generada, procesada o resguardada por los procesos de negocio, su infraestructura tecnológica y activos del riesgo que se genera de los accesos otorgados a terceros (ej.: proveedores o clientes), o como resultado de un servicio interno en outsourcing.

c) Protegerá la información creada, procesada, transmitida o resguardada por sus procesos de negocio, con el fin de minimizar impactos financieros, operativos o legales debido a un uso incorrecto de esta. Para ello es fundamental la aplicación de controles de acuerdo con la clasificación de la información de su propiedad o en custodia.

d) La empresa protegerá su información de las amenazas originadas por parte del personal.

e) **VEHÍCULOS DEL LLANO S.A.S** protegerá las instalaciones de procesamiento y la infraestructura tecnológica que soporta sus procesos críticos.

f) Controlará la operación de sus procesos de negocio garantizando la seguridad de los recursos tecnológicos y las redes de datos.

g) Implementará control de acceso a la información, sistemas y recursos de red.

h) Garantizará que la seguridad sea parte integral del ciclo de vida de los sistemas de información.

i) **VEHÍCULOS DEL LLANO S.A.S** garantizará a través de una adecuada gestión de los eventos de seguridad las debilidades asociadas con los sistemas de información, una mejora efectiva de su modelo de seguridad.

j) La empresa garantizará la disponibilidad de sus procesos de negocio y la continuidad de su operación basada en el impacto que pueden generar los eventos.

k) **VEHÍCULOS DEL LLANO S.A.S** garantizará el cumplimiento de las obligaciones legales, regulatorias y contractuales establecidas.

3.1.1. Otras disposiciones

- El concesionario cuenta con la facultad de actualizar o ajustar el presente manual de políticas de acuerdo a sus necesidades o requerimientos legales, así como de dar a conocer y garantizar la disponibilidad de esta en su última versión.

- El administrador de tecnología enviara a través de los correos corporativos y de manera periódica alertas, tips de seguridad, noticias, entre otros con el fin de generar conciencia y minimizar el riesgo en los correos electrónicos o cualquier otro medio que maneje información.

- El concesionario será responsable de capacitar al personal que administre y trate información u operaciones en misión del del mismo. Así mismo serán responsables de mantener informado todos los cambios o mejoras que se generen junto con su administrador tecnológico.

- **VEHÍCULOS DEL LLANO S.A.S** a través de los procedimientos, políticas o demás directrices establecidas por el administrador tecnológico y aquellas que se implementen en el concesionario garantizara el correcto funcionamiento de la operación frente a la seguridad y administración de la información.

- La organización es responsable de garantizar y vigilar el cumplimiento de las presentes directrices.

- Se evaluará por lo menos 1 vez al año, el cumplimiento frente a la administración de información confidencial en cada lugar o área de trabajo y se registrará en el GCA-FO-008 formato de Informe de Auditoría.

- Todos los resultados de auditoria deberán evidenciar planes de acción liderados por el Kaizen o jefe de Calidad.

- Todos los colaborades de **VEHÍCULOS DEL LLANO S.A.S** se comprometen a conocer, concientizar y cumplir con lo exigido en el presente documento.

- Las respectivas sanciones al incumplimiento de la presente política se realizarán de acuerdo a lo indicado en el reglamento interno, contratos de concesiones o a través de los organismos de control nacional según aplique.

- El concesionario asignara los responsables para que realicen validación a través de auditorías de él buen uso de la información confidencial en todos los puestos o áreas de trabajo.

- Nuestro manual de políticas se encuentra alineado a las directrices dadas en **GF-PL-GIT-03** Política de Seguridad Informática de nuestro administrador tecnológico, esta tiene por objetivo salvaguardar la información en caso de presentarse la explotación de una vulnerabilidad a causa de ciberataques y se convierte en la capa de protección para los activos de información tanto de su propiedad como los que se encuentra administrando.

3.2 Política de autenticación personal y uso adecuado de usuarios.

El jefe del área correspondiente que necesite el usuario debe enviar por correo electrónico al área de tecnología la solicitud de creación, eliminación o modificación del usuario. Esta a su vez diligencia el formato correspondiente “Creación, modificación o eliminación de usuario” y es enviado por correo al proveedor tecnológico. Una vez recibido el usuario, este es compartido por el área de tecnología al solicitante. Siempre se realiza la recomendación de cambiar las contraseñas inicialmente generadas.

La empresa **VEHÍCULOS DEL LLANO S.A.S** adopta las siguientes directrices para la creación, asignación, autenticación, administración y eliminación de usuarios o contraseñas en equipos como portátiles, computadores, Tablet, celulares corporativos, entre otros:

- El acceso de todos los equipos que administren información de **VEHÍCULOS DEL LLANO S.A.S** y que pertenezcan a esta, deberán proteger el acceso a través de usuarios y contraseñas asignadas únicamente a los colaboradores de la empresa y según los roles o permisos asignados.

- Se realiza limitación los perfiles de internet para evitar el acceso y fuga de información por medio de páginas para compartir archivos. Esto se realiza por medio de gestión franca.

- Únicamente los colaboradores asignados son responsables de la seguridad de su usuario de acceso y clave, la única persona a quien se le permite utilizar el usuario de acceso y clave es el funcionario para quien fue creada o asignada.

- Todos los usuarios deben garantizar el uso adecuado y seguridad de la información tratada o asignada a su cargo, únicamente podrá ser usada con fines para garantizar la operación del concesionario.

- Cuando se requiera el cambio en los perfiles de navegación únicamente podrá ser autorizado por el líder de proceso y el administrador tecnológico.

- El administrador tecnológico creará el usuario con sus respectivos permisos de acceso a la información o alcance, así mismo asignará una contraseña temporal al usuario el quien procederá a realizar el cambio de la misma, su correo corporativo y demás requerimientos.

- El administrador tecnológico enviara periódicamente el listado de los usuarios activos de la empresa al área de tecnología para la respectiva validación, con el fin de algún usuario que haya finalizado relación laboral con la compañía se encuentre activo. En caso de que se presente esta novedad el área de tecnología de vehillanos remite solicitud de eliminación de dicho usuario al administrador tecnológico.

- Todos los usuarios creados para los colaboradores son intransferibles, únicos y personales, no está permitido prestar o entregar esta información cuando el personal se encuentre ausente de sus labores, cuando se considere necesario se deberán elevar los respectivos cambios (temporales o definitivos) con el administrador tecnológico.

- Las contraseñas deberán cumplir como mínimo lo siguiente: No contener el nombre de la cuenta del usuario o nombres y apellidos completos del usuario, tener una longitud mínima de ocho (08) caracteres, lo recomendable es Incluir caracteres de tres de las siguientes categorías, mayúsculas (de la A a la Z), minúsculas (de la A a la Z), dígitos de base 10 (del 0 al 9) y caracteres no alfanuméricos (por ejemplo: $, #, %, *).

- Si los usuarios asignados presentan inconsistencias o restricción de acceso a la información, plataformas o equipo el usuario deberá informar de manera inmediata con el líder de proceso para la gestión con el administrador tecnológico.

- Los equipos de cómputo o mesas de trabajo estarán programados para actualizar la contraseña del usuario cada 30 días o cuando el administrador de tecnología lo considere.

- Cuando se le efectué cambio de equipo definitivo o temporal a un colaborador, este siempre deberá ingresar con el usuario y contraseña asignada, no se tiene permitido el acceso con usuarios no asignados a este.

NOTA: En los casos de urgencia operacional, el líder o jefe del proceso será el único con la facultado para solicitar al administrador tecnológico el acceso al equipo donde el usuario se encuentra ausente con el fin de garantizar la continuidad del negocio.

- Los colaboradores se comprometen a efectuar uso adecuado, respeto y la correcta administración de los usuarios, así como la información que tiene acceso en los equipos de cómputo o plataformas tecnológicas de **VEHÍCULOS DEL LLANO S.A.S**.

- Cuando un usuario requiera efectuar cambios en el alcance o permisos de acceso a la información, este deberá ser aprobado por su jefe directo y se gestionara a través del administrador tecnológico.

- Cuando un colaborador cambie de puesto, proceso, área o sea promovido, su jefe directo será el responsable de solicitar los cambios al administrador tecnológico.

- Todos los colaboradores se comprometen a garantizar un uso adecuado y responsable de la información administrada por el mismo a través de los usuarios asignados cumpliendo con lo indicado en la **GA-PO-004** Política para la Administración de Herramientas Electrónicas-de Navegación, Equipos y Usuarios Asignados y las directrices del presente documento.

- Los usuarios o roles asignados serán utilizados únicamente en beneficio de la empresa y para la operación de sus procesos, cuando se evidencie uso inadecuado de los mismos se procederá a tomar las respectivas acciones legales o disciplinarias.

- Ningún colaborador podrá conservar registros de las contraseñas en archivos físicos o en papel, en caso de olvido deberá solicitar nuevamente una temporal al administrador de tecnología, posteriormente actualizar a una definitiva.

- Cuando el administrador tecnológico ingrese por motivos de ausencia del colaborador y por autorización del jefe directo de este, deberá solicitar al colaborador cuando se re incorpore a labores la actualización de su contraseña nuevamente.

- El concesionario se compromete a través del administrador tecnológico a realizar revisiones periódicas con el fin de validar los permisos, acceso de la información o inactividad de usuarios.

- Cada que se requiera inactivar o eliminar un usuario el jefe de área será el responsable de informar a través de correo de manera inmediata al área de tecnología del concesionario, y este a su vez informara la solicitud al proveedor tecnológico por medio de email adjuntando el formato correspondiente a la solicitud.

- Cuando algún colaborador se encuentre ausente de la empresa bien sea por vacaciones, incapacidad, permisos entre otros, el jefe directo del área deberá reasignar las funciones de dicho colaborador a otro colaborador para no afectar las operaciones. En este orden de ideas es el jefe quien informa al área de tecnología si es necesario realizar modificación de los permisos del usuario que realizara las tareas asignadas y de realizar direccionamiento del correo de manera momentánea a otro usuario. El área de tecnología a su vez realiza la solicitud al proveedor tecnológico por medio del formato de solicitudes especiales.

- Cuando algún colaborador se encuentre ausente de la empresa bien sea por vacaciones, incapacidad, permisos entre otros, el jefe directo del área deberá resguardar los equipos tecnológicos en caso de que la ausencia no supere los 5 días. En caso de superarlos los equipos deberán ser entregados al área de tecnología para su respectiva custodia.

- El administrador tecnológico es responsable de garantizar la inhabilidad o eliminación inmediata de los usuarios y equipos con el fin de garantizar la seguridad de la información.

NOTA: El presente numeral no aplica para los usuarios y contraseñas externas como las aseguradoras, para este caso se procederá a utilizar el asignado de manera temporal mientras el líder o responsable tramita el cambio con el ente externo.

Prohibiciones:

- Ningún usuario podrá anular cualquier restricción o seguridad colocada para utilizar inadecuadamente el Internet.
- Almacenar, visualizar, transmitir o recibir cualquier material obsceno, vulgar, ofensivo, acosador, repetitivo o de naturaleza ilegal.
- Está prohibido realizar cualquier intento por descubrir el usuario o la clave de otro funcionario, o de servicios a los cuales no tiene acceso autorizado.

- Está prohibido acceder a cuentas de otros usuarios de la empresa o externos sin autorización de los mismos con el fin de extraer información, y usar esta con fines personales, delictivos o ajenos a su rol.
- Está prohibido conectarse a sitios web que no sean parte de su actividad de trabajo y/o acceder a grupos de noticias relacionados con sexo, drogas ilegales, conocimientos criminales, declaraciones de odio, apuestas en línea, música sin licencias, entre otros
- Está prohibido enviar mensajes sobre noticias internamente a menos que su contenido y propósito sea autorizado por la administración.
- Se prohíbe ocasionar excesiva congestión de la red a través de descargas prolongadas, no asociadas a su cargo.
- Se prohíbe acceder a sitios de conversación o mensajería instantánea diferentes a los establecidos y autorizados por la empresa.

3.3 Política de comunicaciones externas y corta fuegos.

- Todos los accesos y configuraciones desde y hacia las redes externas como lo puede ser a través de la red de internet son protegidas y monitoreadas por medio de firewall de seguridad, de esta manera garantizaremos el aislamiento de nuestra red local frente a ciberataques o acceso no permitido a los servidores.

- Así mismo el administrador tecnológico tomara acciones preventivas como el bloqueo de trafico de malware intruso o servidores no autorizados, parches de seguridad, configuraciones de filtrado del firewall (permitir/bloquear la comunicación), implementación de mecanismos para detectar una falsificación del sitio web abierto al público en Internet, entre otros; el proveedor tecnológico se compromete través de sus políticas y procedimientos establecidos a la protección de la red o servidores internos de accesos externos no autorizados, así como a generar revisiones periódicas y planes de acción correspondientes.

- Todas las reglas de filtrado o corta fuego serán validadas de manera periódica y se definirá un backup de estas con el fin de garantizar el adecuado funcionamiento.

- Las alertas de seguridad y de comportamiento inusual, basadas en la criticidad, son enviadas por el proveedor tecnológico a un sistema integrado para su seguimiento, investigación y remediación.

- El proveedor tecnológico implementa mecanismos y herramientas SOC y NOC para prevenir y mitigar ataques o vulnerabilidades, detección inteligente de amenazas y respuesta automatizada ante incidentes. Su alcance cubre todos nuestros entornos tecnológicos: redes, servidores, nube, aplicaciones y más.

- Al navegar por un sitio público de Internet en HTTPS, se inspecciona el certificado para verificar que la autoridad certificadora sea una fuente interna, lo que demuestra que el proxy está realizando una inspección intermedia del tráfico SSL. Este procedimiento es realizado por el proveedor tecnológico.

- La red corporativa se encuentra configurada para no permitir que los puntos finales se comuniquen con Internet sin pasar por el proxy, excepto una lista de destinos web requeridos por el sistema. Esta configuración es administrada por el proveedor tecnológico.

- El proveedor tecnológico ejecuta un análisis completo, como mínimo, semanalmente de los equipos. Se permiten excepciones para hardware o casos de uso en los que esto afectaría la funcionalidad o afectaría gravemente el rendimiento. En ese caso, aún se requiere un escaneo rápido semanal.

- El proveedor tecnológico realiza configuraciones pertinentes para el bloqueo o interrupción del tráfico a direcciones IP, dominios, archivos o contenidos de comunicación maliciosos conocidos.

- El proveedor tecnológico garantiza que la comunicación entre el agente y el proxy de la nube es un túnel cifrado y lógicamente aislado.

- El proveedor tecnológico garantiza que el proxy solo funcione para usuarios autenticados que forman parte de un grupo de cuentas humanas y de máquinas con aprobación para navegar por Internet.

- El Antivirus puede proporcionar protección incluso cuando no existe conexión a Internet.

- Se implementa un sistema para detectar y bloquear el acceso no autorizado en tiempo real el cual es administrado por el proveedor tecnológico.

3.4 Política para el control de acceso a los empleados

VEHÍCULOS DEL LLANO S.A.S establece siguientes directrices para garantizar el control de acceso y salidas por reconocimiento dactilar (biométrico) de sus colaboradores a las instalaciones del concesionario:

- El líder de proceso o jefe directo del colaborador asignara el horario laboral de acuerdo a las necesidades de la operación.

- El colaborador autorizara a la empresa para el tratamiento de sus datos personales y la empresa a su vez, garantizara el cumplimiento de lo indicado en **GER-PS-003** Política de Privacidad y uso de Información.

- Será responsabilidad del proceso de gestión humana y el colaborador de garantizar la información idónea y actual en la plataforma del biométrico, la inscripción a este se efectuará de acuerdo a lo indicado en el **GH-PR-002** Procedimiento de Selección y Contratación

- El uso del biométrico será de exclusivamente para todos los colaboradores de **VEHÍCULOS DEL LLANO S.A.S**, el control de acceso para terceros, contratistas o demás se efectuará acorde a lo indicado en el numeral 5.6 de la presente política para el control de entradas y salidas del concesionario.

- Ningún colaborador podrá ingresar a las instalaciones sin registrar la huella a través del biométrico o de lo contrario deberá contar con autorización de Gerencia o Gestión humana.

- La empresa realizara seguimiento y control de los movimientos registrados en el biométrico, así como el cumplimiento de sus horarios de manera periódica o cuando se requiera.

- No se tiene permitido el acceso a personal ajeno al concesionario a zonas restringidas que no se encuentre autorizado.

- Cuando un colaborador requiera ingresar a las instalaciones en un horario no habitual, este deberá contar con autorización o debida programación del jefe directo y a su vez únicamente podrá realizar actividades para las cuales está autorizado.

- El registro de los colaboradores en el biométrico se realizará durante el proceso de contratación. Estos serán parametrizados con el horario laboral según el caso de cada cargo.

- Una vez el colaborador culmina su relación laboral con la compañía, sus datos son inactivados del biométrico.

- La revisión tanto de los registros del biométrico y sus permisos se realizarán de manera periódicas por el área de gestión humana y el área de tecnología.

3.5 Política para el control de entradas y salidas del concesionario

Con el fin de garantizar un manejo adecuado de sus visitantes y de salvaguardar la seguridad de sus colaboradores o activos del concesionario se establecen las siguientes directrices:

- Todos los colaboradores se identificarán a través de sus carnets corporativos, uniforme laboral y con la lectura del biométrico, así como el personal de seguridad privada externa.

- El acceso de los contratistas o proveedores de productos o servicios serán responsabilidad del proceso de compras o en su defecto de cada líder del proceso en el cual se encuentran desarrollando operaciones.

- Con el fin de garantizar la seguridad industrial en las operaciones realizadas dentro de nuestras instalaciones, todos los proveedores o contratistas están en la OBLIGACIÓN de evidenciar al ingreso del concesionario los soportes de seguridad social vigente y demás requisitos exigidos por el concesionario.

- Los clientes únicamente podrán ingresar hasta la sala de ventas para los casos de compra o entrega de vehículo nuevo y usado, cuando vienen por compra de repuestos, accesorios o demás, únicamente podrán acceder a la sala o recepción de venta al público y para aquellos que aplica para servicio o colisión únicamente tienen la autorización de estar en la sala de espera asignada o cuando se requiera en la zona de recepción.

- Todas las zonas de acceso a terceros o publico estarán identificadas con el fin de dar a conocer los lugares restringidos o zonas de circulación libre.

- El concesionario se encuentra en la obligación de dar a conocer a sus colaboradores, así como estos están en la obligación de cumplir con las directrices dadas por el presente numeral y demás consideradas por el concesionario.

- Cuando se evidencie personal sin su debida identificación (escarapela, cinta, carnet, entre otros.) ya sea colaborador, visitante o proveedor, estará en la responsabilidad de dar a conocer las presentes directrices y en los casos donde se presente de manera repetitiva la situación, deberá informar a Gerencia para que se proceda con la respectiva toma de acciones.

- Si se presenta la situación donde se evidencien visitantes que se consideren sospechosos y no cuenten con su respectiva identificación, o ingresen a zonas no autorizadas será monitoreado y se deberá informar a Gerencia cuando se considere necesario.

- El concesionario realizara seguimiento y vigilancia por CCTV de manera periódica durante las 24 horas con el fin de identificar personal que no cumpla con los requerimientos de

seguridad, identificación o situación sospechosa, así mismo se cuenta con el contrato de servicio de vigilancia de seguridad.

NOTA: todos los terceros, visitantes, proveedores o acompañantes deberán efectuar registro en la planilla de ingreso y portar la respectiva identificación asignada en lugares visibles e identificables.

El formato o control de registro se llevará a través de la persona asignada por **VEHÍCULOS DEL LLANO S.A.S** y es de carácter obligatorio efectuarlo previo al ingreso, además de lo anterior, la persona responsable debe confirmar el ingreso con el líder de proceso o área respectiva.

El concesionario tiene la potestad si así lo considera de solicitar un documento que identifique la persona que ingresa, este será devuelto hasta la salida de las instalaciones y la devolución de la escarapela o carnet asignado, el guarda o a quien defina el concesionario será responsable de salvaguardar dichos documentos.

- Únicamente se permitirá el acceso del personal visitante a las zonas o lugares donde fue autorizado, todo el personal colaborador del concesionario está en la obligación de identificar e informar cuando se presenten este tipo de acciones.

  En los casos donde se requiera el acceso de visitantes a lugares no autorizados como se informó inicialmente al ingreso, se procederá a informar al jefe de área y este a su vez será el responsable del mismo.

3.6 Política de confidencialidad.

3.6.1 Directrices para la confidencialidad de la información

Los documentos serán clasificados según las series establecidas Tabla de Retención Documental y el nivel de acceso de acuerdo a la Tabla de Control de Acceso información contenida en cada expediente, los niveles de acceso establecidos son:

• Publico: Documentación que puede ser consultada por cualquier persona, dentro o fuera de la organización, sin que ello represente un riesgo para la entidad ni para tercero. Su divulgación no afecta la integridad de las personas, la seguridad de la empresa ni continuidad del negocio.

• Restringido: Documentación de acceso limitado a determinados colaboradores o áreas, debido a que su divulgación no autorizada podría generar afectaciones moderadas a la entidad o persona involucrada.

• Confidencial: Documentación altamente sensible, cuyo acceso esta estrictamente autorizado a un grupo muy reducido de colaboradores. La divulgación no autoriza de este nivel puede generar graves consecuencias, comprometiendo la integridad de las personas, seguridad de la empresa o la continuidad del negocio.

3.6.2 Buenas prácticas

En Vehículos del Llano S.A.S, implementamos buenas prácticas que nos permitan prevenir y fomentar la adecuada administración de la información en sus diferentes medios.

1.Limitar el acceso de la documentación clasificada como restringida y confidencial al personal no autorizado.
2. Almacenar la información en espacios seguros.
3. Evitar la exposición innecesaria de la información.
4. Llevar control de las solicitudes y prestamos de documentos tanto físicos como electrónicos.
5. Cifrar la documentación clasificada como confidencial en el envió de documentos electrónicos.
6. Usar canales institucionales para el envío de información.
7. Usar los equipos corporativos para el almacenamiento de la información.
8. Emplear el uso de etiquetas para clasificar la información
9. Evitar habla de la información en frente del personal no autorizado.
10. Respetar y cumplir con las Políticas de Seguridad Informática.

Nota: La divulgación inadecuada de la información, sin importar su nivel de clasificación genera riesgos que afectan a la organización y a las personas involucradas.

3.6.3 Cláusula de confidencialidad

Para **VEHÍCULOS DEL LLANO S.A.S** es de vital importancia garantizar un adecuado uso de la información o bases de datos, para ello la empresa cuenta con el registro de **GH-FT-010** Clausula Adicional de Confidencialidad para cada colaborador, grupo de interés o tercero que por sus operaciones es necesario tener acceso a nuestra información.

Para el caso de nuestros colaboradores, la cláusula se evidenciará de manera integral de los contratos directos con el concesionario o por prestación de servicios utilizando términos legalmente ejecutables y contemplando factores como responsabilidades y acciones de los firmantes para evitar la divulgación de información no autorizada. Este requerimiento también se aplicará para los casos de contratación temporal o cuando se permita el acceso a información y/o a los recursos a personas o Entidades externas.

Así mismo, la empresa adopta medidas para garantizar la confidencialidad de la información y sus procesos ante los visitantes o partes interesadas.

VEHÍCULOS DEL LLANO S.A.S respalda la confidencialidad de la información administrada o compartida con nuestros aliados a través de:

- Contratos de concesión, dentro de estos contratos el administrador tecnológico garantizara cláusulas de confidencialidad para su personal o colaboradores.

- Políticas de Seguridad de la información.

- Confidencialidad en la contratación de personal (todos los aliados deben contar con esta cláusula al interior de su organización, estas cláusulas deberán ser aceptadas y firmadas por el colaborador.)

- Las cláusulas deberán ser evidenciadas para todos los tipos de contratos ya sea temporal directamente con el concesionario o aquellos externos considerados in-house.

- Las reglas refrentes a la confidencialidad de la información se encuentran establecidas y claramente estipuladas en las cláusulas aceptadas por el titular.

- Revisión periódica del cumplimiento en las cláusulas de confidencialidad, aliados, de concesión o de cualquier otra índole con el fin de garantizar el cumplimiento de las directrices.

- Envió de reporte o informes de seguridad, materialización del riesgo, brechas de seguridad o ataques entre sus aliados, administradores tecnológicos o de información confidencial en periodos establecidos o cuando se consideren.

La empresa tiene la facultad para adoptar o implementar diferentes mecanismos que garanticen la confidencialidad de la información tratada por nuestros aliados, así como de realizar seguimiento al cumplimiento y respecto de sus directrices.

Así mismo, **VEHÍCULOS DEL LLANO S.A.S** estipula que al vencimiento de los acuerdos o términos de cualquier índole entre sus partes interesadas deberán proceder a garantizar la confidencialidad y absoluta reserva de la información.

Todo incumplimiento que se evidencie frente a los acuerdos de confidencialidad tendrá tratamiento de acuerdo a lo indicado en el reglamento interno del trabajo o según lo indique la normatividad legal aplicable.

3.7 Política de formación y toma de conciencia en temas de seguridad de la información

3.7.1 Inducción y Reinducción

- Al inicio de la relación laboral o contractual, el administrador tecnológico deberá socializar esta política y los lineamientos de seguridad informática a todas las partes interesadas.

- La reinducción será realizada en caso de cambios significativos en las políticas de seguridad, retorno de personal después de una ausencia prolongada o cuando se identifiquen riesgos relevantes que así lo requieran.

3.7.2 Capacitación y Concientización

- El administrador tecnológico será responsable de realizar como mínimo una (1) capacitación anual en seguridad informática dirigida a todos los colaboradores y partes interesadas.

- Estas capacitaciones incluirán temas como: manejo seguro de la información, prevención de ciberataques, protección de credenciales, uso adecuado de dispositivos y canales digitales, entre otros.

- Todos los colaboradores deberán superar con un mínimo de 70% la calificación de la prueba o evaluación realizada; cuando este no supere dicha evaluación, se deberá repetir la inducción y nuevamente ejecutar la evaluación las veces que se consideren necesarias y hasta que este supere la nota mínima.

- Así mismo, cuando se presente **actualizaciones** de las políticas o procesos inmersos a la seguridad de la información, el responsable asignado por la Gerencia deberá garantizar la socialización de los mismos.

3.7.3 Comunicación Preventiva

- Se enviarán periódicamente alertas, noticias, tips de seguridad u otra información relevante mediante correo electrónico, con el objetivo de mantener informadas a las partes interesadas y reforzar la cultura de seguridad digital.

- La frecuencia y el contenido de estas comunicaciones serán definidos por el administrador tecnológico según la evolución de los riesgos y las buenas prácticas del sector.

3.7.4 Responsabilidad del Administrador Tecnológico

- Transmitir por correo electrónico los planes de prevención y reacción ante la materialización de riesgos tecnológicos.

3.8 Política de gestión de dispositivos inteligentes.

El objetivo de la presente directriz es implantar acciones para reducir al máximo; los riesgos asociados a la administración de base de datos por medio de dispositivos inteligentes, como lo pueden ser todos aquellos aparatos electrónicos o de tecnología que por lo general está conectado a otro dispositivo o red a través de diferentes protocolos como bluetooth, NFC, WI-Fi, 3G, X10, entre otros.

Es por lo anterior que nos comprometemos a:

- Disponer y dotar de celulares, tablets o cualquier otro dispositivo de uso corporativo a todos los colaboradores que por sus funciones den un tratamiento o tengan acceso y seguimiento a información correspondiente a nuestra operación, productos, servicios y clientes a través de estos dispositivos.

- Por ningún motivo se permitirá el uso de equipos o teléfonos personales del colaborador para administrar, manejar, modificar o descargar información de las bases de datos tratadas a su cargo.

NOTA: Únicamente y por autorización previa de Gerencia se permitirá el uso de equipos personales que manipulen bases de datos tratadas a su cargo, siempre y cuando el colaborador autorice al concesionario la instalación de un software que garantice la separación del ambiente de trabajo y el que se considere personal para el colaborador, así mismo el colaborador aceptará las condiciones dadas por el concesionario y la validación de su dispositivo de manera periódica o cuando se considere necesario.

- La información tratada en estos equipos únicamente deberá ser almacenada en los programas o software permitidos por el concesionario, lo anterior con el fin de respaldar la base de datos en la nube o interfaz interna.

- Con el fin de no detener o retrasar la operación de un colaborador al inicio de su relación laboral con el concesionario, el proceso de gestión humana o administrativa deberán garantizar la disponibilidad de los equipos con sus respectivos requerimientos o controles.

- En los dispositivos corporativos únicamente tendrán permiso para acceder a las plataformas o información necesaria para el desarrollo de sus operaciones.

- Todos los dispositivos deberán ser bloqueados por contraseñas definidas por el concesionario, no se aceptará el uso de reconocimiento facial o dactilar de los equipos corporativos.

- El concesionario deberá garantizar la conexión directa y eficaz con el proveedor equipos inteligentes con el fin de borrar o salvaguardar la información de este cuando se evidencie pérdida o robo.

- No se podrán instalar o utilizar redes sociales no autorizadas o manejo personal de los mismos o el almacenamiento de información ajena a la operación del concesionario.

- Queda prohibida la navegación en páginas de internet con fines personales con el fin de garantizar la protección de la información por ataques maliciosos o virus en el dispositivo, únicamente se permitirá el acceso a plataformas autorizadas por el concesionario.

- Es prohibición del colaborador descargar información de las plataformas o redes autorizadas por el concesionario para uso personal.

- El colaborador no podrá instalar o desinstalar programas, software o aplicación que no sea permitida por la organización o cuando no se considere necesaria para su operación.

- Para las playas de venta o exposición externa de vehículos el área comercial siempre deberá contar con una Tablet o equipo de celular para garantizar que la información de clientes potenciales sea tratada únicamente a través de dispositivos corporativos o autorizados por el concesionario.

- La empresa realizara seguimiento a la administración de estos dispositivos de manera periódica y por lo menos una vez al año.

- Al momento de finalizar la relación laboral, el colaborador deberá entregar el dispositivo junto con toda la información pertinente a las operaciones del concesionario.

- Cuando algún colaborador se encuentre ausente de la empresa bien sea por vacaciones, incapacidad, permisos, entre otros, el jefe directo del área deberá reasignar las funciones de dicho colaborador a otro colaborador para no afectar las operaciones. En este orden de ideas es el jefe quien informa al área de tecnología si es necesario resguardar los equipos tecnológicos del colaborador ausente o serán asignados temporalmente a otro colaborador. Para esto se tiene estipulado el procedimiento **Solicitud, alistamiento y entrega de equipos inteligentes** donde se establecen los parámetros para dicho resguardo o traslado de los equipos.

• Todo celular corporativo debe estar controlado por el software de control, administrado por el proveedor tecnológico y este quien administra la lista blanca de aplicaciones

3.9 Política para la administración y uso adecuado estaciones de trabajo o equipos de cómputo.

Se definen en las siguientes directrices para el control de las estaciones de trabajo o equipos de cómputo:

a) Cuando un colaborador requiera equipo de cómputo o estación de trabajo, se realizará la gestión a través del proceso administrativo quien deberá contar con la respectiva autorización de Gerencia para efectuar la requisición y compra, posteriormente procederá con la asignación del puesto o lugar de trabajo y firma acta de entrega, compromisos o responsabilidades del colaborador junto con la validación del **GA-FT-013** Check List Herramientas Tecnológicas.

NOTA: Todos los cambios que se requieran anexar a la asignación inicial deberán ser autorizados por Gerencia y el administrador tecnológico.

b) Con el propósito de proteger la integridad de los sistemas informáticos y de telecomunicaciones, es imprescindible que todos y cada uno de los equipos involucrados dispongan de software de seguridad o antivirus, estos deberán garantizar una actualización de manera constante a todos los equipos activos o con acceso a la red y así mismo aquellos que se encuentran inactivos.

c) Es responsabilidad absoluta del administrador tecnológico garantizar la instalación de antivirus y programas autorizados en todos los equipos del concesionario y mantenerlos actualizados en tiempos establecidos.

d) Todas estaciones de trabajo, equipos de cómputo o portátiles contaran con los respectivos parches de seguridad con el fin de garantizar la actualización constante y automática. Sin embargo, estas serán supervisadas y validadas por el administrador tecnológico. Estos serán aplicados y ejecutados de manera inmediata a los servidores públicos e internos cada que se presente un ciberataque o una posible violación a los activos de información. Nuestro administrador tecnológico garantizara la actualización de nuestros sistemas con el fin de evitar y prevenir la materialización de un riesgo o ataque.

e) Cuando se considere necesario la instalación de dispositivos extraíbles o externos en los equipos se deberá efectuar análisis con el antivirus, sin embargo y por directrices internas todos los puertos de los equipos o estaciones de trabajo se encuentran bloqueados para no permitir la extracción de información.

NOTA: Cuando se requiera el manejo de estos dispositivos externos se procederá a enviar solicitud al administrador tecnológico y este será quien considere el acceso o no de los dispositivos extraíbles según el requerimiento.

f) Está prohibido descargar o tener información personal o software no permitidos en los equipos pertenecientes al concesionario, lo anterior con el fin de garantizar el uso adecuado del equipo y el acceso a virus o ataques posibles.

g) Ninguno de los usuarios o colaboradores del concesionario tienen permitida la desactivación temporal o total de los antivirus instalados, únicamente y cuando se requiera podrá ser ejecutado por el administrador tecnológico.

h) Cuando se presenten ataques, los procedimientos a seguir será llevados a cabo por el administrador tecnológico y estos mismos serán responsables de dar aviso inmediato a los usuarios, así como de comprobar la eliminación total de los ataques evidenciados.

i) Con el fin de prevenir los daños o ataques en las estaciones de trabajo, equipos de cómputo o portátiles, el único autorizado para realizar instalación de software es el proveedor tecnológico.

j) El listado de software permitidos en el concesionario es aquellos que se encuentran definidos en el **GER-FO-010** Formato de Check List Herramientas Tecnológicas, no se permitirá la instalación de software que no cuenten con licencia.

k) No se tiene permitido el almacenamiento de datos o información que se considere critica para las operaciones de la empresa en las carpetas de almacenamiento del equipo o escritorio del mismo, esta información deberá ser protegida de cualquier tipo de ataque y deberá reposar en los mecanismos de almacenamiento que considere el proveedor tecnológico o el área de tecnología de la empresa.

l) El equipo deberá contar con la política de escritorio limpio la cual se gestiona desde el proveedor tecnológico.

m) Será responsabilidad única de la pérdida o daños ocasionados al equipo por el uso inadecuado del usuario o responsable del mismo.

n) Está prohibido retirar partes o componentes de los sistemas de cómputo de propiedad de **VEHÍCULOS DEL LLANO S.A.S**. sin previa aprobación por gerencia y/o el área de tecnología de la empresa.

o) Todas las bajas de estaciones de trabajo o equipos de cómputo se efectuarán de acuerdo a lo indicado en la Política Baja de Activos.

p) En caso de que el colaborador necesite retirar el equipo de cómputo de las instalaciones, deberá validar inicialmente con el jefe directo y después diligenciar el formulario que se encuentra en el sharepoint del área de sistemas con el fin de generar dicha aprobación de salida por parte de la gerencia administrativa y financiera y área de tecnología.

q) Todos los equipos o estaciones de trabajo deberán estar programados para bloquear la pantalla o acceso a este como mínimo 5 minutos desde su abandono o desatención del usuario, dado al superar este tiempo límite, se requiera del acceso con usuario y contraseña. Si la persona necesita ausentarse de su puesto de trabajo, deberá suspender el equipo o bloquear la pantalla.

r) Informar al área de tecnología del concesionario cuando se requiera trasladar/asignar el equipo a otra persona por diferentes motivos (cambio de cargo, retiro, etc....), de no ser así el equipo seguirá siendo responsabilidad de la persona inicialmente asignada.

s) No se podrá realizar cualquier actividad que sea considerada como ilegal o incorrecta de acuerdo con las normas legales que rigen la operación de sistemas de cómputo y de la Información, se liberará de toda responsabilidad patrimonial a **VEHÍCULOS DEL LLANO S.A.S** por tal motivo.

t) Es responsabilidad del colaborador informar de manera inmediata al administrador de tecnología o al jefe de tecnología de la empresa con respecto a necesidades o novedades que se presenten con el cómputo.

u) Cuando algún colaborador se encuentre ausente de la empresa bien sea por vacaciones, incapacidad, permisos entre otros, el jefe directo del área deberá reasignar las funciones de dicho colaborador a otro colaborador para no afectar las operaciones. En este orden de ideas es el jefe quien informa al área de tecnología si es necesario resguardar los equipos tecnológicos del colaborador ausente o serán asignados temporalmente a otro colaborador. Para esto se tiene estipulado el

procedimiento **Solicitud, alistamiento y entrega de equipos de computo** donde se establecen los parámetros para dicho resguardo o traslado de los equipos.

De igual manera el jefe de área es quien informa al área de tecnología si es necesario realizar modificación de los permisos del usuario que realizara las tareas asignadas temporalmente y si se debe realizar direccionamiento del correo del colaborador ausente al nuevo colaborador de manera temporal. El área de tecnología a su vez realiza la solicitud al proveedor tecnológico por medio del formato de solicitudes especiales.

La empresa y el administrador tecnológico tienen la facultad para efectuar inspección del cumplimiento a la presente política sin previo aviso del usuario o colaborador con el fin de identificar el cumplimiento de las mismas, esta inspección o seguimiento se deberá realizar por lo menos una vez al año.

3.10 Política para la administración de servidores o racks

Las siguientes medidas de seguridad son implementadas por **VEHÍCULOS DEL LLANO S.A.S** con el fin de garantizar la protección y correcta administración de los servidores o racks

a) De la información tratada o almacenada en los servidores o racks; esta será únicamente manejada por el administrador tecnológico estos a su vez, tienen la facultad de emitir las normas o requerimientos necesarios para garantizar la seguridad de la información.

b) Con el fin de velar por la correcta administración de la información que se considere critica para la operación, todo el personal deberá almacenarla únicamente en las rutas o accesos de red asignados por el administrador tecnológico.

c) La estructura física del rack o los centros de cableado, se renovarán de acuerdo a las necesidades de ampliación, actualización y cambios tecnológicos para **VEHÍCULOS DEL LLANO S.A.S**; dicha actividad será contratada por el proveedor o tercero autorizado por el administrador tecnológico.

d) De los servidores o racks físicos; el administrador tecnológico velara por el correcto y adecuado funcionamiento, así mismo el concesionario será responsable de monitorear, informar o reportar novedades físicas que se presenten, el acceso al lugar será de carácter restringido, únicamente podrá ingresar el personal autorizado y deberá mantener bajo llave; cuando se requiera ingresar a este por algún motivo deberá ser con acompañamiento o supervisión del personal autorizado.

e) El servidor deberá contar con un sistema de enfriamiento para garantizar su correcta operación y prevenir incendios o calentamiento del mismo.

f) La administración de los usuarios y el acceso a los servidores o rack es únicamente responsabilidad del administrador tecnológico.

* Cuando se realice algún cambio en la configuración del servidor o rack deberá ser controlado y registrado por los administradores.

g) Todos los requerimientos de seguridad serán documentados, así como los resultados de escaneo y contramedidas mantenidas por el administrador tecnológico.

h) Los servidores con acceso público o aquellos de acceso interno previo a su activación se tomarán contramedidas para la vulnerabilidad expuesta.

i) Para aquellas plataformas que no son administradas por el proveedor tecnológico, se realizara pruebas de vulnerabilidad por lo menos una vez al año con el fin de garantizar el cumplimiento de los requisitos mínimos.

j) Todas las aplicaciones que se publican en internet serán analizadas previamente y se especificarán los requisitos de seguridad por parte del administrador tecnológico.

k) Para aquellas plataformas que no son administradas por el proveedor tecnológico, se realizara pruebas de vulnerabilidad por lo menos una vez al año con el fin de garantizar el cumplimiento de los requisitos mínimos.

l) Para preservar la seguridad de los equipos de los servidores y equipos de comunicaciones y en general todos los dispositivos de los datacenter, servidores o racks deben permanecer cerrados e identificados en zonas de restricción a personal no autorizado.

m) El acceso remoto a los servidores únicamente se ejecutará por los usuarios autorizados o por el administrador tecnológico.

n) Únicamente se permite el acceso a los servidores los usuarios administradores y estos no serán transferibles o revelados a personal ajeno o no asignado de estas funciones.

o) El acceso al data center de la compañía es un área restringida. El acceso será limitado y autorizado por el jefe de tecnología. De igual manera se controlará el ingreso a

través del registro en el formulario que se encuentra en el sharepoint. Toda persona que ingrese deberá siempre estar en acompañamiento por el jefe o auxiliar de tecnología.

p) Los servidores de archivos de Gestión Franca tienen restricciones de seguridad que no permiten el almacenamiento de archivos de imagen (jpg, tiff, bmp, etc.), audio (mp3, wav, wma, etc.) o video (mp4, 3gp, avi, etc.), con excepción de carpetas especificas solicitadas por las áreas que lo requieren para las funciones de su trabajo.

q) El respaldo de la información alojada en los servidores o rack será únicamente responsabilidad del administrador tecnológico, quien ha sistematizado copias de seguridad a intervalos definidos y cuenta con metodologías definidas para garantizar la prevalencia de la información.

r) La administración, disposición final o destrucción de los discos duros o cualquier otro medio utilizado para el respaldo de la información deberán ser trazables y con soportes de su tratamiento de baja.

NOTA: Únicamente se permitirá la destrucción total o la disposición final a través de entidades externas calificadas ya que un formateo de los mimos no garantiza la eliminación total.

s) Los permisos y autorizaciones serán únicamente para el administrador tecnológico o a quien este delegue, así mismo ellos tendrán la facultad y responsabilidad de limitar los perfiles de cada usuario para el acceso a la información.

t) Las contraseñas de los administradores deberán cumplir con las características indicadas en la política de autenticación de personal indicada en el numeral 5.2 del presente documento.

u) Cuando se requiera re iniciar el Servidor deberá hacerlo únicamente la persona responsable de este.

3.11 Política de seguridad a través de las herramientas de office

Para VEHÍCULOS DEL LLANO SAS es fundamental contar con herramientas de office que garanticen legalmente adquiridas para el adecuado funcionamiento y tratamiento de datos o información relevante para el análisis o funcionamiento de los procesos.
Es por lo anterior que se establecen las siguientes directrices frente al uso de estas herramientas:

Para la instalación

La instalación del paquete office se debe garantizar al momento de asignar el equipo de cómputo al colaborador.

A través del administrador de tecnología se debe contar con las licencias necesarias para el adecuado funcionamiento de las herramientas office.

No está permitido el uso de software gratuito o de licencias no oficiales

Cuando se presenten inconvenientes con las herramientas office el usuario es responsable de informar mediante la mesa de ayuda para la respectiva gestión.

El uso de las licencias es exclusivamente laboral, ningún colaborador deberá tener conocimiento ni disponer de manera propia dichas licencias. Solo el área de tecnología y el administrador tecnológico realizaran la administración de las mismas.

De los correos electrónicos:

El concesionario establece sus controles y genera las siguientes directrices para garantizar la seguridad de la información a través de los correos electrónicos:

Se conocen, pero no se limitan a posibles amenazas a las cuales puede estar expuesta la información tratada por correo electrónico del concesionario los siguientes:

Spam, aquellos enviados a un gran número de destinatarios con fines comerciales o publicitarios.

Phishing, método fraudulento para captar la información sensible, intento de engaño a través de mensajes que se pueden considerar oficiales emitidos por entidades financieras, de empresa o de nuestra confianza.

Estafas, posible venta de productos falsos o inexistente, información falsa.

Es prohibición que los usuarios o colaboradores falsifiquen mensajes de correo electrónico en nombre de la empresa o de cualquier otro fin.

No se permite leer, borrar, copiar o modificar mensajes de correo electrónico de otras personas, sin su autorización.

Correos con ficheros adjuntos maliciosos, Esos ficheros adjuntos contienen virus, gusanos, troyanos, etc. Actualmente es uno de los peligros más extendidos. Recibimos un mensaje (de un remitente no necesariamente desconocido ya que puede estar falsificado) con un fichero adjunto que nos invita a abrirlo.

Hoax o cadenas de mensajes falsos, generalmente se trata de mensajes variados acerca de hechos o falsas alarmas de cualquier tipo. En los que se nos pide que reenviemos y difundamos el mensaje entre nuestros conocidos.

Se limita la capacidad de los archivos adjuntos que se envían a través del correo electrónico máximo de 35MB.

Los siguientes serán responsabilidades de los usuarios de correo electrónico:

Los lideres o jefes de proceso serán los encargados de asignar el personal o cargo que estará en la facultad de recepcionar o remitir correspondencia electrónica de externos o proveedores.

La Información que se considere sensible o critica únicamente será compartida a los interesados, así mismo se implementan mecanismos de restricción del acceso a la información según su criticidad o riesgo hacia la organización o el titular frente a la divulgación o publicación de la misma.

Cuando se efectúen envíos de correo electrónico y se requieran incluir otros destinatarios, en lo posible se deberá utilizar la opción “correos ocultos” con el fin de evitar en lo posible que los receptores conozcan los demás usuarios copiados.

Todos los administradores de correo electrónico deberán ser prudentes a la hora de enviar información a externos, deberá validar la información que remite y sus destinatarios antes de efectuar el envío.

Las siguientes serán responsabilidades del administrador tecnológico:

A través del administrador tecnológico se dispondrán de herramientas de filtrado de correo las cuales mediante sus algoritmos intercepta todos los correos que a su criterio sean catalogados spam y los direcciona a verificación por parte de la herramienta, todos aquellos correos que logren evadir el antispam deben ser enviados por los usuarios a la opción Spam del correo personal para que estos quede bloqueados.

Implementar enlace con el antivirus en la puerta de correo electrónico con el fin de analizar la información para su posterior tratamiento y evitar una infección de virus.

El administrador tecnológico dispondrá de una herramienta de archivado de correo la cual intercepta todos los correos que salen y entran guardándolos por un periodo de retención establecido.

Los usuarios no pueden utilizar la funcionalidad O365 o Outlook para reenviar correos electrónicos de manera masiva fuera de la compñia. Esta configuración es administrada por el proveedor tecnológico.

SPF, DKIM y DMARC están configurados para mejorar la seguridad del correo electrónico. Esta configuración es administrada por el proveedor tecnológico.

Se realiza configuración para bloquear o interrumpir el tráfico a direcciones IP, dominios, archivos o contenidos de comunicación maliciosos conocidos. Esta configuración es administrada por el proveedor tecnológico.

Los usuarios no pueden realizar el reenvío de correos masivos a usuarios con destino fuera de la organización, para esto el proveedor tecnológico deberá aplicar los controles necesarios.

Así mismo, el administrador tecnológico y el área de tecnología realizara campañas, envío de boletines, sensibilización y capacitación para el reconocimiento o incentivación de amenazas a través de la administración del correo corporativo o envío de información externa.

Del acceso a los servicios de la web o internet:

Todos los colaboradores que tengan acceso a las redes de navegación directa o por wifi deberán cumplir con lo indicado en los numerales de la SIS-PS-013 Política para la administración y uso adecuado de la red local y red wifi, lo anterior con el fin de garantizar el no acceso o restricción a sitios web maliciosos o no autorizados.

3.12 Política para el manejo de material confidencial dentro y fuera de las instalaciones.

VEHÍCULOS DEL LLANO S.A.S a través de las directrices garantiza la NO fuga de información a través de las plataformas de navegación o dispositivos de extracción de la información y así mismo limita el acceso a la información a través de los dispositivos corporativos.

- No se tiene permitido la extracción o conexión de dispositivos externos como: USB, Disco externo, DVD, CD, entre otros, todos los equipos deberán tener los puertos bloqueados y no reconocerán este tipo de dispositivos a fin de garantizar la seguridad de la información.

NOTA: únicamente se permitirá el uso de estos, bajo autorización de Gerencia, se enviará la solicitud por correo de desbloqueo de puertos o dispositivos al proveedor tecnológico y el realizará el proceso acorde a procedimientos estipulados por el proveedor.

- Los equipos, la información o software, independientemente de su formato o soporte de almacenamiento, no pueden ser retirados de las instalaciones sin el permiso escrito previo autorizado por el jefe de Gestión IT y/o Gerencia General. (Se realiza solicitud de retiro del equipo por medio del formulario del SharePoint y se retorna la aprobación por correo.)

Mientras los activos en cuestión permanecen fuera de la organización, deben ser controlados por la persona a la que se le concedió el permiso para retirarlo.

NOTA: únicamente el personal del proceso comercial o a quien Gerencia autorice puede trasladar los equipos (teléfono corporativo) de manera externa.

- Mientras los activos en cuestión permanecen fuera de la organización, deben ser controlados por la persona a la que se le concedió el permiso para retirarlo.

- Todos los equipos deberán estar cifrados.

- El proceso de cifrado lo realiza el proveedor tecnológico acorde a sus procedimientos establecidos de cifrado. La solicitud de cifrado se realiza por medio de una solicitud de correo electrónico por parte del área de tecnología de la empresa. La información de cifrado quedara en el share point del área de sistemas. De igual manera queda en un disco externo el cual es almacenado en caja fuerte dentro del data center el cual tiene acceso limitado y restringido.

- En lo posible, todos los colaboradores deberán utilizar las rutas de acceso compartido con el fin de disminuir el riesgo de pérdida o daños de la información a través de los escritorios o discos locales de los equipos de cómputo.

- El acceso a la información digital únicamente tendrá acceso el trabajador de acuerdo a su rol o perfil dentro de la empresa.

- Ningún colaborador podrá revelar por ningún motivo información que no este permitida o se considere sensible.

Con el material físico:

- Está prohibido evidenciar tachones y enmendaduras en los documentos o registros de las operaciones.

- No se podrá extraer registros, información, hojas de vida y material sensible del concesionario sin previa autorización de Gerencia.

- Se considera una falta grave la perdida de información que este a cargo o bajo la responsabilidad de un colaborador sin importar su nivel de autoridad o jerarquía.

- Únicamente estará disponible a consulta la información que por ley o por políticas internas del concesionario se debe transmitir o socializar a sus partes interesadas.

3.13 Política para la administración y uso adecuado de la red local y red wifi.

VEHÍCULOS DEL LLANO S.A.S implementa las siguientes directrices para la administración y buen uso de la red loca y red wifi.:

3.13.1 Red local

- No se permite el ingreso a la red local a personal no autorizado o ajeno a la compañía.
- Los permisos o perfiles otorgados para el acceso a la red local deberán ser solicitados y administrados por el administrador tecnológico.
- No se tiene permitido la conexión hacia la red local de equipos personales o ajenos al concesionario, en caso de que se requiera conectar a una red, se dará acceso a la de invitados.
- Los colaboradores no podrán conectar dispositivos o equipos que se consideren personales a la red local.
- Únicamente el personal del concesionario y que por sus funciones requieren la conexión a la red local tienen permitido el acceso.
- El administrador tecnológico por sus funciones y contrato de concesión contara con el acceso a la red local.
- El acceso a la red local será a través de puntos de red establecidos en las instalaciones del concesionario y avalados por un proveedor externo.
- En los casos donde la operación o mantenimiento requiera que el personal ajeno al concesionario ingrese a la red local, deberán ser autorizados por Gerencia y el administrador tecnológico, lo anterior con el fin de identificar los dispositivos externo en caso de incidentes frente a la seguridad de la información.
- Los usuarios externos como lo pueden ser proveedores, clientes o cualquier otro tipo de visitantes podrán acceder de wifi cumpliendo con las directrices de la Política para la Administración y Uso Adecuado de las redes WIFI V1
- El administrador tecnológico controlara y efectuara seguimiento de los dispositivos conectados a la red local con el fin de responder de manera rápida cuando se pueda presentar algún incidente de seguridad.

3.13.2 Red Wifi

Todo usuario que requiera tener acceso o conexión a la red WIFI deberá cumplir con el siguiente procedimiento:

- Solicitar el acceso al responsable de la administración de la misma.

- Para los clientes, proveedores o contratistas que necesiten el acceso, se dará el ingreso a la red wifi de Invitados. Solo se ingresará la contraseña al equipo, pero no se revelará esta.
- Para el acceso a los colaboradores, el jefe de tecnología junto con el jefe de cada parea validara quien debe contar con conexión a red wifi acorde a la necesidad de sus operaciones.
- La contraseña cambiara acorde a las políticas del proveedor tecnológico. Cuando se considere el cambio de la misma se debe garantizar la salida de todos los usuarios temporales.
- El administrador de la contraseña WIFI cuenta con la autorización y responsabilidad de validar junto con el administrador tecnológico el correcto y uso adecuado de la navegación o control de la misma.
- Todos los usuarios de vehillanos a los que se les de acceso a través de la red wifi corporativo deberá autenticarse en la plataforma de portal cautivo con su usuario y contraseña. De lo contrario no tendrá acceso a internet.
- Cuando se evidencie el inadecuado uso de la red WIFI se le informará al líder del proceso y se procederá a tomar acciones con el proceso de Gestión Humana.
- El administrador tecnológico controlara y efectuara seguimiento de los dispositivos conectados a la red wifi con el fin de responder de manera rápida cuando se pueda presentar algún incidente de seguridad.

Tener en cuenta:

- La red se encuentra separa por VLANS lo que permite segmentar el tráfico en diferentes dominios lógicos, mejorando la seguridad y reduciendo la congestión, ya que cada VLAN actúa como una red independiente dentro de la misma infraestructura física. Esta segmentación y administración de las VLANS las realiza el proveedor tecnológico.

- El diagrama de red se realiza y es administrado por el proveedor tecnológico.

3.14 Política para el control, respuesta y prevención ante incidentes y eventos. (borrar, perder, ingresar, entre otros) así como la prevención ante ciberataques.

En **VEHÍCULOS DEL LLANO S.A.S** estamos comprometidos con la seguridad de la información que se pueda generar debido a la explotación de vulnerabilidades, es por ellos que nos apoyamos a través de nuestro administrador tecnológico y de su procedimiento **GF-P-GIT-15** se adopta la metodología para la prevención y respuesta de ciberataques.

Sin embargo, el concesionario será responsable de informar de manera inmediata al administrador tecnológico cualquier ataque, acción o situación que se considere amenaza para la seguridad de la información con el fin de que este las evalué e implemente controles para la prevención de próximos posibles ataques o intentos de violación de la información.

Así mismo el administrador tecnológico es responsable de informar a **VEHÍCULOS DEL LLANO S.A.S** de cualquier creación, modificación o eliminación de los procedimientos, políticas y demás directrices necesarias para el control y respuesta ante incidentes de seguridad de la información.

Estas directrices serán de carácter obligatorio para todos nuestros colaboradores y demás partes interesadas que visiten nuestras instalaciones o tengan algún vínculo comercial con el concesionario.

Como concesionario nos comprometemos adoptar y mantener actualizada nuestra **SIS-MT-02** Matriz de estrategias de prevención, respuesta a incidentes y controles específicos para incidentes de seguridad de la información o ciberseguridad y nuestro **SIS-PO-04** procedimiento para el manejo de incidentes de seguridad de la información e informática. Así mismo identificamos e implementaremos controles asociados a sus riesgos con el fin de prevenir o reducir al máximo todo tipo de fugas o ataques.

Cualquier violación o no cumplimiento a la política generara sanciones acordes al Reglamento interno de trabajo.

3.15 Política de seguridad interna (fotografías y grabaciones de video).

En **VEHÍCULOS DEL LLANO S.A.S** estamos comprometidos con salvaguardar o cuidar de nuestras operaciones y a nuestros colaboradores, es por ello que únicamente se permite la grabación de videos o toma de fotografías de los vehículos en exhibición, siempre y cuando se encuentren únicamente en las zonas de vitrina o sala de ventas.

Ningún colaborador podrá tomar fotografías o videos de los procesos u operaciones del concesionario sin la debida autorización de su jefe directo o Gerencia y cuando se permita, únicamente esta información podrá ser utilizada con fines laborales, en favor del concesionario o cuando este lo autorice.

Los asesores de servicio están autorizados para efectuar videos en la recepción del vehículo a través de los dispositivos corporativos y con fines laborales.

El concesionario cuenta con CCTV con el fin de garantizar la seguridad en sus instalaciones y así mismo da a conocer a todos sus visitantes o partes interesadas que al ingreso de nuestras instalaciones se someterán y aprueban que la empresa efectué grabaciones de seguridad de manera regular y que además de lo anterior, estas evidencias o grabaciones serán utilizadas únicamente acorde a las necesidades de la empresa y serán respetados los derechos del visitante de manera confidencial.

Estas grabaciones se realizarán en los periodos o tiempos requeridos por la dirección y se realizara monitoreo, inspección y mantenimiento con el fin de verificar el correcto o adecuado funcionamiento.

El concesionario cuenta con la implementación de las directrices dadas en el SIS-PO-003 Procedimiento para la Gestión de CCTV para garantizar la instalación, el monitoreo y la administración de cámaras de video.

3.16 Política para la identificación y señalización de áreas o acceso restringido

El concesionario se compromete a la demarcación e identificación de todas las áreas de acceso restringido, así como las áreas de circulación libre para terceros garantizando que para todas sus partes interesadas sean visibles y legibles, así mismo cada que se evidencie el deterioro de alguna se procederá a efectuar el respectivo proceso para su posterior cambio.

Así mismo, toda persona que requiera acceder a las áreas restringidas deberá contar con el respectivo permiso y acompañamiento del colaborador asignado o responsable del visitante, cuando se considere el acceso, este deberá ser registrado en la planilla de ingreso al concesionario.

El acceso a las áreas restringidas deberá ser monitoreado a través de los CCTV las cuales grabarán durante las 24 horas del día y serán inspeccionadas de manera periódica por el responsable asignado.

Para las áreas con acceso restringido debido a la presencia de información documental, el ingreso estará permitido únicamente a los colaboradores responsables asignados. En caso de que un tercero o un colaborador de otra área requiera acceder a dicha información, se deberá aplicar el procedimiento establecido para el préstamo de documentos, facilitando la documentación mas no generando ingreso a las áreas.

3.17 política para la Gestión del Riesgo

El objetivo de la presente política es establecer un enfoque sistemático para identificar, evaluar, tratar y monitorear los riesgos que puedan afectar los procesos, activos e información de **VEHÍCULOS DEL LLANO S.A.S.**

Aplica a todas las áreas, procesos, activos y personal de VEHÍCULOS DEL LLANO S.A.S involucrados en la identificación y gestión de riesgos operativos, tecnológicos y de seguridad de la información.

VEHÍCULOS DEL LLANO S.A.S identifica sus activos de información, controla y mitiga los riesgos asociados a la seguridad de la información a través de la SIS-MT-03 Matriz de

Inventario y Gestión del Riesgo en Activos de Información así mismo evalúa y valida la eficacia de sus controles a través del SIS-PO-02 Procedimiento para la Gestión del Riesgo.

En dicha matriz se enumeran todos los activos de la compañía incluyendo físicos, tecnológicos, de infraestructura, personas, entre otros. De igual manera se identifican riesgos, estado, descripción, controles, valoración y planes de acción de dicho activo acorde al riesgo identificado.

Dado a que contamos con un administrador de tecnología externo, este también identifica y controla a través del GF-O-GIT-03 Matriz de Gestión de Riesgos alineado a nuestro concesionario y así mismo ambos cuentan con la facultad de auditar o validar el grado de confiabilidad esperado para eliminar o mitigar la materialización de los riesgos.

La eficacia de los controles y la mejora continúa dado a los cambios que se pueden presentar en el contexto de la organización se evaluaran por medio de auditorías por lo menos una vez al año.

3.18 Política para el intercambio de información

- No está permitido entregar información de la Empresa sin autorización.
- A cada Empresa únicamente se le entrega la información que le corresponde.
- La información únicamente puede ser entregada por los funcionarios autorizados.
- Cuando se envié información sensible por correo electrónico, se debe asignar clave a los archivos adjuntos y está debe ser informada al destinatario por un medio diferente al correo electrónico.
- Los empleados de **VEHÍCULOS DEL LLANO S.A.S** están obligados a cumplir los acuerdos de confidencialidad y por lo tanto serán responsables de la entrega de información no autorizada.
- La información sensible disponible al público a través de sitios web debe estar protegida por sitios seguros y adicionalmente con usuario y clave de acceso.
- La comunicación con entidades externas para el intercambio de información crítica se debe hacer a través de canales dedicados, con mecanismos de seguridad, como son VPN o web services y debe ser configurado por personal de infraestructura IT.

- Es responsabilidad de los dueños de la información crítica no dejar copias impresas o documentos físicos en lugares de fácil acceso a personal no autorizado.

- No realizar conversaciones confidenciales en lugares públicos, oficinas abiertas o lugares de reunión sin paredes a prueba de sonido.

- En los contratos o acuerdos de servicios se incluyen los requisitos y condiciones requeridas para el intercambio de información.

3.19 Política manejo adecuado del correo electrónico corporativo

La organización asignará una cuenta de correo electrónico y/o una cuenta, de mensajería instantánea tipo chat, a empleados que según las actividades de su cargo lo requiera; Dicha cuenta es personal e intransferible y se deberán cumplir las siguientes directrices:

a) Cada usuario es el único responsable de la administración de su correo electrónico y de la manera que se utilice.

b) El envío de correos electrónicos implica el consumo de recursos tecnológicos y demanda tiempo a la persona receptora, por tal razón se debe evitar el envío de correos innecesarios y que no guarden relación con el desempeño de las funciones asignadas.

c) Todos los usuarios del correo institucional deben unificar y utilizar la firma del correo electrónico utilizando el modelo asignado por **VEHÍCULOS DEL LLANO S.A.S.**

d) Todo correo de procedencia desconocida, correo basura, SPAM, correo no deseado, etc. que sea recibido en la los buzones de correo electrónico de la **VEHÍCULOS DEL LLANO S.A.S**, debe ser ignorado, eliminado inmediatamente y reportado a la ZONA FRANCA con el fin de evitar posibles infecciones por código malicioso o virus.

e) Antes de responder o reenviar un correo, el usuario debe validar si se requiere incluir todos los destinatarios, el historial y la información que posee el mismo.

f) Será una herramienta usada únicamente con fines laborales y exclusivos de **VEHÍCULOS DEL LLANO S.A.S**, no se tendrá permitido el uso de esta herramienta con fines personales.

g) Lo usuarios se comprometen a no enviar correos o información a terceros, esto se permite únicamente cuando es requerido para la operación de las actividades en pro del funcionamiento adecuado de la empresa.

h) Todos los usuarios que cuenten con un correo asignado se comprometen a darle un uso correcto y adecuado para el desarrollo de las funciones en ejercicio de su cargo.

i) Cada usuario es el único responsable de todas las actividades realizadas con sus cuentas de correo o en el envió de la mensajería instantánea.

j) Deberán cumplir en todo momento las normas de uso y de seguridad de la red de datos de la organización.

k) Comunicar o hacer públicas únicamente las direcciones electrónicas permitidas por la empresa.

l) Siempre utilizar la firma del correo asignada en la administración del mismo.

m) Ningún colaborador podrá utilizar el correo electrónico para cualquier propósito comercial o financiero ajeno a las funciones propias de la organización.

n) Por ningún motivo se podrá enviar correo tipo SPAM, es decir correo basura, relacionado con falsos virus, con publicidad de empresas, cadenas de mensajes, etc.

o) No utilizar redes de internet públicas para él envió o remisión de correos, se podrá efectuar únicamente bajo autorización.

p) Se prohíbe borrar todo tipo de información guardada en los correos durante la vigencia de la relación laboral.

q) Se prohíbe compartir contactos o listas de distribución de **VEHÍCULOS DEL LLANO S.A.S** con personal externo, con el objetivo de propiciar el envío de propagandas, ofertas, negocios personales, avisos publicitarios, o información de otro tipo, ajena a las labores propias del cargo.

r) El envío de correos con mensajes que contravengan las normas legales, la moral, el orden público, la intimidad o el bueno nombre de las personas, que contengan contenido irrespetuoso, difamatorio, racista, religioso irrespetuoso, discriminatorio, de acoso o intimidación; así como imágenes o videos con contenidos ilegales, ofensivo, extorsivo, indecente o con material sexual.

s) Está prohibida la migración o el uso de correos personales frente a la información del concesionario.

t) **VEHÍCULOS DEL LLANO S.A.S** recomienda hacer caso omiso a los links que vengan agregados en el cuerpo del correo de cuentas externas; por lo tanto, se aconseja digitar directamente la página que deseen consultar en el navegador del equipo o informar de manera inmediata a gestión franca para el respectivo análisis.

u) Queda prohibido el envío de material que sea considerado delicado, censurado, sensible, ofensivo, sexual, privado o prohibido a través del correo asignado, será exclusión la información permitida por las políticas internas de **VEHÍCULOS DEL LLANO S.A.S**.

NOTA: Según lo establecido en la Ley 524 de 1999, los mensajes de correo electrónico revisten la misma fuerza probatoria que tienen los documentos físicos.

3.19.1 Uso de Equipos

- El colaborador debe utilizar únicamente equipos autorizados y proporcionados por la empresa para el desarrollo de sus labores.
- Queda prohibido el uso de equipos personales para acceder a información o sistemas corporativos.
- Los equipos deben contar con antivirus actualizado, firewall activo, software de seguridad aprobado, discos cifrados y demás software bases autorizados por la empresa.

3.19.2 Acceso a la Información

• El acceso remoto a los sistemas corporativos deberá realizarse únicamente mediante conexiones seguras (VPN o canales cifrados).
• Las credenciales de acceso son personales e intransferibles; no deben compartirse con ningún tercero ni almacenarse en lugares visibles o inseguros.
• El usuario debe bloquear su sesión o cerrar la sesión al ausentarse del equipo, incluso por periodos cortos.

3.19.3 Protección de Datos e Información

• Se prohíbe almacenar información confidencial o restringida en dispositivos externos o servicios en la nube no autorizados.
• Los documentos y archivos corporativos deben guardarse únicamente en las rutas seguras establecidas por la empresa (SharePoint, OneDrive corporativo, servidor interno, etc.).
• La información impresa (si se genera) debe ser custodiada de forma segura y destruida correctamente cuando deje de ser necesaria.

3.19.4 Entorno de Trabajo

• El colaborador debe garantizar un espacio de trabajo privado y libre de interrupciones donde no haya exposición visual o auditiva de información sensible.
• No se permite la grabación de reuniones o pantallas sin la autorización previa de las partes involucradas.
• Se deben evitar conversaciones sobre temas confidenciales en espacios públicos o a través de dispositivos no corporativos.

• En las reuniones virtuales se deberá solicitar al colaborador mantener la cámara encendida, con el fin de verificar su identidad y asegurar que sea efectivamente él quien participa en la sesión.

3.19.5 Conectividad y Redes

• Solo se deben usar redes Wi-Fi seguras y protegidas con contraseña.
• Está prohibido conectarse desde redes públicas (cafeterías, aeropuertos, etc.) sin el uso de VPN corporativa.
• El usuario deberá informar de inmediato cualquier anomalía o comportamiento sospechoso del equipo o red al área de tecnología.

3.19.5 Responsabilidad del Colaborador

• El colaborador es responsable del cuidado y uso adecuado de los equipos y la información a su cargo.
• En caso de pérdida, robo o daño del equipo o acceso no autorizado, debe reportarlo de inmediato al área de sistemas y/o seguridad de la información.

El incumplimiento de estas políticas podrá ser objeto de sanciones disciplinarias conforme al reglamento interno de trabajo.

3.20 Política gestión de equipos para trabajo remoto

Solicitud trabajo remoto

En caso de que el colaborador necesite retirar el equipo de cómputo de las instalaciones por motivos de trabajo remoto o teletrabajo, deberá validar inicialmente con el jefe directo y después diligenciar el formulario que se encuentra en el sharepoint del área de sistemas con el fin de generar dicha aprobación de salida por parte de la gerencia administrativa y financiera y área de tecnología.

Parámetros o políticas para el trabajo remoto

Uso de Equipos

- El colaborador debe utilizar únicamente equipos autorizados y proporcionados por la empresa para el desarrollo de sus labores.
- Queda prohibido el uso de equipos personales para acceder a información o sistemas corporativos.

- Los equipos deben contar con antivirus actualizado, firewall activo, software de seguridad aprobado, discos cifrados y demás software bases autorizados por la empresa.

Acceso a la Información

- El acceso remoto a los sistemas corporativos deberá realizarse únicamente mediante conexiones seguras (VPN o canales cifrados).

- Las credenciales de acceso son personales e intransferibles; no deben compartirse con ningún tercero ni almacenarse en lugares visibles o inseguros.

- El usuario debe bloquear su sesión o cerrar la sesión al ausentarse del equipo, incluso por periodos cortos.

Protección de Datos e Información

- Se prohíbe almacenar información confidencial o restringida en dispositivos externos o servicios en la nube no autorizados.

- Los documentos y archivos corporativos deben guardarse únicamente en las rutas seguras establecidas por la empresa (SharePoint, OneDrive corporativo, servidor interno, etc.).

- La información impresa (si se genera) debe ser custodiada de forma segura y destruida correctamente cuando deje de ser necesaria.

Entorno de Trabajo

• El colaborador debe garantizar un espacio de trabajo privado y libre de interrupciones donde no haya exposición visual o auditiva de información sensible.
• No se permite la grabación de reuniones o pantallas sin la autorización previa de las partes involucradas.
• Se deben evitar conversaciones sobre temas confidenciales en espacios públicos o a través de dispositivos no corporativos.

• En las reuniones virtuales se deberá solicitar al colaborador mantener la cámara encendida, con el fin de verificar su identidad y asegurar que sea efectivamente él quien participa en la sesión.

Conectividad y Redes

• Solo se deben usar redes Wi-Fi seguras y protegidas con contraseña.
• Está prohibido conectarse desde redes públicas (cafeterías, aeropuertos, etc.) sin el uso de VPN corporativa.
• El usuario deberá informar de inmediato cualquier anomalía o comportamiento sospechoso del equipo o red al área de tecnología.

Responsabilidad del Colaborador

• El colaborador es responsable del cuidado y uso adecuado de los equipos y la información a su cargo.
• En caso de pérdida, robo o daño del equipo o acceso no autorizado, debe reportarlo de inmediato al área de sistemas y/o seguridad de la información.

- El incumplimiento de estas políticas podrá ser objeto de sanciones disciplinarias conforme al reglamento interno de trabajo.

3.21 Política para el uso responsable de herramientas de inteligencia artificial

INTELIGENCIA ARTIFICIAL (IA)

Tecnología que permite a sistemas informáticos realizar tareas que normalmente requieren capacidades humanas, como generar contenido, responder consultas, analizar información, identificar patrones, procesar datos y asistir en diferentes actividades.

HERRAMIENTAS DE INTELIGENCIA ARTIFICIAL

Son las plataformas, aplicaciones, sistemas, asistentes virtuales o servicios basados en Inteligencia Artificial que hayan sido evaluados y expresamente autorizados por la organización para el desarrollo de actividades laborales.

La autorización de una herramienta estará sujeta a las condiciones de uso, licenciamiento, controles de seguridad, protección de datos y restricciones establecidas por la organización.

INFORMACIÓN CONFIDENCIAL

Toda información interna, financiera, comercial, estratégica, técnica, operativa, contractual, personal o de cualquier otra naturaleza cuya divulgación, modificación, pérdida o acceso no autorizado pueda afectar a la organización, sus clientes, proveedores, colaboradores o demás partes relacionadas.

DATOS PERSONALES

Toda información que permita identificar o hacer identificable, directa o indirectamente, a una persona natural, de acuerdo con la legislación aplicable en materia de protección de datos personales.

USUARIO

Todo colaborador, contratista, practicante, proveedor o tercero autorizado que utilice herramientas de Inteligencia Artificial en actividades relacionadas con la organización.

HERRAMIENTAS DE INTELIGENCIA ARTIFICIAL AUTORIZADAS

Para el desarrollo de actividades laborales dentro de la organización, únicamente estarán autorizadas las herramientas de Inteligencia Artificial que hayan sido previamente evaluadas y aprobadas por el área de Tecnología y/o Seguridad de la Información.

A la fecha de emisión de la presente política, las herramientas autorizadas para uso corporativo son:

MICROSOFT COPILOT

Microsoft Copilot está autorizado como herramienta de apoyo para actividades de productividad, redacción, generación de ideas, resumen de información, aprendizaje y elaboración de contenidos no confidenciales.

Su uso deberá realizarse mediante los mecanismos de acceso autorizados por la organización y respetando las restricciones establecidas en esta política.

El uso de Copilot para programación o procesamiento de información relacionada con sistemas, aplicaciones, infraestructura o procesos internos deberá contar con autorización previa del área de Tecnología y/o Seguridad de la Información.

CHATGPT

ChatGPT está autorizado únicamente mediante su **versión gratuita** como herramienta de apoyo para actividades de redacción, generación de ideas, análisis de información pública, aprendizaje, documentación y otras actividades de bajo riesgo.

No está permitido ingresar información confidencial, datos personales, credenciales, código fuente, información financiera, estratégica o cualquier otra información restringida de la organización.

El uso de ChatGPT para programación relacionada con sistemas o procesos de la organización deberá contar con autorización previa del área de Tecnología y/o Seguridad de la Información.

GOOGLE GEMINI

Google Gemini está autorizado como herramienta de apoyo para actividades de redacción, generación de ideas, análisis de información pública, aprendizaje, documentación y otras actividades de bajo riesgo.

No está permitido ingresar información confidencial, datos personales, credenciales, código fuente, información financiera, estratégica o cualquier otra información restringida de la organización.

El uso de Gemini para programación relacionada con sistemas o procesos de la organización deberá contar con autorización previa del área de Tecnología y/o Seguridad de la Información.

OTRAS HERRAMIENTAS DE INTELIGENCIA ARTIFICIAL

Cualquier otra plataforma, aplicación, asistente, extensión, servicio o solución basada en Inteligencia Artificial que no se encuentre expresamente incluida dentro del listado de herramientas autorizadas deberá contar con una evaluación y autorización previa por parte del área de Tecnología y/o Seguridad de la Información.

El uso de herramientas de Inteligencia Artificial no autorizadas para actividades laborales podrá considerarse un incumplimiento de la presente política.

La organización podrá modificar, ampliar, restringir, suspender o retirar la autorización de cualquiera de estas herramientas cuando existan cambios en los niveles de riesgo, condiciones de seguridad, licenciamiento, costos, necesidades operativas, requisitos legales o políticas corporativas.

AUTORIZACIÓN DE LA HERRAMIENTA Y AUTORIZACIÓN DE LA INFORMACIÓN

La autorización de una herramienta de Inteligencia Artificial no significa que toda la información corporativa pueda ser ingresada en ella.

Los usuarios deberán verificar previamente la clasificación de la información y cumplir las restricciones establecidas en esta política y en las demás políticas de seguridad de la información de la organización.

LINEAMIENTOS GENERALES

Los usuarios podrán utilizar herramientas de Inteligencia Artificial únicamente como apoyo para mejorar la productividad, eficiencia, aprendizaje, análisis y desarrollo de sus actividades laborales.

El uso de estas herramientas deberá realizarse respetando los siguientes principios:

- Confidencialidad.
- Integridad.
- Disponibilidad.
- Legalidad.
- Responsabilidad.
- Ética empresarial.
- Protección de datos personales.
- Seguridad de la información.
- Propiedad intelectual.

Las herramientas de Inteligencia Artificial deberán ser utilizadas como herramientas de apoyo y no como sustituto del criterio profesional, conocimiento, responsabilidad o toma de decisiones de los colaboradores.

Toda información, documento, análisis o contenido generado mediante IA deberá ser revisado, validado y, cuando corresponda, corregido por el usuario antes de ser utilizado, distribuido o incorporado a procesos de la organización.

USOS PERMITIDOS

Se permite el uso de herramientas de Inteligencia Artificial autorizadas para actividades como:

- Redacción y corrección de documentos, correos y comunicaciones.
- Generación de ideas y apoyo en procesos creativos.
- Resumen y análisis de información pública o información autorizada.
- Elaboración de borradores de procedimientos, instructivos y documentos.
- Apoyo en actividades de aprendizaje, capacitación y formación.
- Generación y revisión de código fuente, cuando corresponda y siempre que no se exponga información confidencial.
- Apoyo en actividades administrativas autorizadas.
- Análisis de información que haya sido previamente clasificada como apta para su procesamiento mediante herramientas de IA.
- Automatización de tareas administrativas previamente autorizadas.
- Generación de contenidos que no comprometan información confidencial, datos personales o propiedad intelectual de la organización.
- Apoyo en procesos de investigación y consulta sobre información pública.

Toda información generada mediante herramientas de Inteligencia Artificial deberá ser revisada y validada por el usuario antes de su utilización.

PROHIBICIONES

Queda prohibido utilizar las herramientas de Inteligencia Artificial autorizadas para fines diferentes a los establecidos en la presente política o que puedan generar riesgos para la organización.

En particular, se prohíbe:

- Utilizar herramientas de Inteligencia Artificial no autorizadas para actividades laborales.
- Utilizar la IA para realizar actividades ilegales, fraudulentas, discriminatorias, ofensivas o contrarias a las políticas de la organización.
- Utilizar resultados generados por IA de manera deliberada cuando se tenga conocimiento de que contienen información falsa, engañosa o perjudicial.
- Utilizar la IA para evadir controles de seguridad, obtener accesos no autorizados o realizar actividades que puedan afectar los sistemas tecnológicos de la organización.
- Utilizar la IA para generar, modificar o distribuir contenido que pueda infringir derechos de autor, propiedad intelectual o derechos de terceros.
- Utilizar herramientas de IA para tomar decisiones que correspondan exclusivamente a personal autorizado o que requieran criterio profesional especializado.
- Utilizar la IA para fines personales que impliquen el uso indebido de recursos tecnológicos, información o servicios proporcionados por la organización.
- Emplear herramientas de IA de manera que pueda afectar la reputación, operación o intereses de la organización.

Cualquier uso no contemplado en esta política deberá ser consultado previamente con el área de Tecnología y/o Seguridad de la Información.

COMPARTIR INFORMACIÓN CONFIDENCIAL

Está prohibido ingresar, cargar, copiar, transferir o proporcionar a herramientas de Inteligencia Artificial información confidencial, restringida o sensible de la organización, salvo que exista una autorización expresa y se hayan establecido los controles de seguridad correspondientes.

Entre la información restringida se encuentra:

- Datos personales de clientes.
- Datos personales de colaboradores.
- Datos personales de proveedores.
- Información financiera.
- Contraseñas.
- Credenciales de acceso.
- Tokens, claves API o secretos de sistemas.
- Información estratégica.
- Información comercial confidencial.

- Contratos.
- Información protegida por acuerdos de confidencialidad.
- Información técnica restringida.
- Información de sistemas, redes o infraestructura que pueda representar un riesgo de seguridad.
- Información relacionada con incidentes de seguridad.
- Información cuya divulgación esté restringida por la legislación, contratos o políticas internas.

ALMACENAR INFORMACIÓN CORPORATIVA

Está prohibido utilizar plataformas de Inteligencia Artificial como repositorios de documentos, sistemas de almacenamiento empresarial o mecanismos alternativos para conservar información corporativa.

Los documentos corporativos deberán permanecer almacenados en los sistemas y plataformas oficialmente establecidos por la organización.

USO DE CUENTAS PERSONALES

Cuando exista una cuenta, licencia o mecanismo corporativo habilitado para el uso de una herramienta de IA, los usuarios deberán utilizar dicho mecanismo para las actividades laborales.

No deberá utilizarse una cuenta personal para procesar información corporativa cuando la organización haya establecido un mecanismo corporativo autorizado.

TOMAR DECISIONES EXCLUSIVAMENTE CON IA

Ninguna decisión operativa, financiera, comercial, administrativa, laboral o estratégica podrá basarse exclusivamente en respuestas generadas por herramientas de Inteligencia Artificial.

Las respuestas generadas por IA deberán ser consideradas como material de apoyo y deberán ser verificadas por una persona competente antes de tomar decisiones.

GENERAR CONTENIDO ILEGAL O INAPROPIADO

No se permitirá utilizar herramientas de Inteligencia Artificial para:

- Difundir información falsa de manera intencional.
- Realizar actividades fraudulentas.
- Suplantar identidades.
- Vulnerar derechos de terceros.
- Infringir derechos de autor o propiedad intelectual.
- Generar contenido discriminatorio, ofensivo o que pueda constituir acoso.
- Realizar actividades contrarias a la legislación vigente.
- Intentar evadir controles de seguridad de los sistemas de la organización.
- Realizar actividades que puedan afectar la reputación o los intereses legítimos de la organización.

GENERACIÓN DE CÓDIGO MALICIOSO

Está prohibido utilizar herramientas de Inteligencia Artificial para generar, modificar o distribuir código destinado a causar daños, obtener acceso no autorizado, extraer información o evadir controles de seguridad.

Las actividades de análisis, pruebas de seguridad o evaluación de vulnerabilidades mediante IA deberán realizarse únicamente cuando estén autorizadas y dentro de los procedimientos establecidos por la organización.

PROTECCIÓN DE LA INFORMACIÓN

Todo usuario deberá:

- Verificar la clasificación de la información antes de ingresarla en una herramienta de IA.
- Utilizar únicamente plataformas de Inteligencia Artificial autorizadas.
- Utilizar las cuentas corporativas cuando estas hayan sido establecidas por la organización.
- Evitar proporcionar información que permita identificar directamente a clientes, colaboradores o proveedores cuando no sea estrictamente necesario.
- Anonimizar o eliminar información sensible cuando sea posible antes de utilizar herramientas de IA.
- Verificar la información generada por la herramienta antes de utilizarla.
- Mantener la información corporativa en los sistemas oficiales de almacenamiento.
- Reportar inmediatamente cualquier incidente de seguridad relacionado con el uso de herramientas de IA.

- Cumplir las políticas de seguridad de la información y protección de datos personales vigentes.

RESPONSABILIDADES DEL USUARIO

Los colaboradores, contratistas, practicantes y terceros que utilicen herramientas de Inteligencia Artificial serán responsables de:

- Utilizar únicamente herramientas autorizadas.
- Cumplir las restricciones establecidas en esta política.
- Proteger la información corporativa.
- Validar la exactitud de la información generada.
- Corregir posibles errores, sesgos o imprecisiones.
- Verificar las fuentes cuando la información generada sea utilizada para actividades que requieran precisión.
- Garantizar el cumplimiento de las políticas internas.
- Respetar los derechos de autor y propiedad intelectual.
- Utilizar la IA de manera ética, responsable y profesional.
- Reportar incidentes o usos inadecuados de las herramientas de IA.

La responsabilidad final sobre cualquier documento, análisis, contenido, código, comunicación o decisión seguirá siendo del usuario y no de la herramienta de Inteligencia Artificial.

RESPONSABILIDADES DEL ÁREA DE TECNOLOGÍA Y/O SEGURIDAD DE LA INFORMACIÓN

El área de Tecnología y/o Seguridad de la Información será responsable, dentro del alcance de sus funciones, de:

- Evaluar las herramientas de Inteligencia Artificial que sean propuestas para uso corporativo.
- Determinar los riesgos asociados con su utilización.
- Establecer controles de seguridad cuando sean necesarios.
- Definir y mantener actualizado el listado de herramientas autorizadas.
- Establecer restricciones de acceso cuando corresponda.
- Promover buenas prácticas de seguridad relacionadas con el uso de IA.
- Atender y gestionar incidentes relacionados con herramientas de Inteligencia Artificial.
- Revisar periódicamente la pertinencia de las herramientas autorizadas.

La autorización de nuevas herramientas estará sujeta a criterios técnicos, de seguridad, protección de datos, cumplimiento legal, licenciamiento y necesidades de la organización.

VALIDACIÓN DE INFORMACIÓN GENERADA POR IA

Las herramientas de Inteligencia Artificial pueden generar información incorrecta, incompleta, desactualizada o imprecisa.

Por lo tanto, ningún usuario deberá asumir que una respuesta generada por IA es correcta únicamente por haber sido producida por una herramienta tecnológica.

Antes de utilizar información generada mediante IA, el usuario deberá:

- Revisar su contenido.
- Validar datos relevantes.
- Verificar información crítica mediante fuentes confiables.
- Corregir errores o inconsistencias.
- Confirmar que el contenido sea apropiado para el propósito para el cual será utilizado.

En procesos que involucren decisiones críticas, información financiera, aspectos legales, seguridad, recursos humanos o información de clientes, deberá existir revisión humana por parte del personal competente.

PROPIEDAD INTELECTUAL Y DERECHOS DE AUTOR

Los usuarios deberán respetar la legislación aplicable y las políticas internas relacionadas con derechos de autor, propiedad intelectual y uso de información de terceros.

No deberá utilizarse una herramienta de Inteligencia Artificial para reproducir, transformar, distribuir o utilizar material protegido sin contar con las autorizaciones correspondientes.

Cuando el contenido generado mediante IA vaya a ser utilizado en documentos, publicaciones, productos, servicios o materiales corporativos, el usuario deberá verificar que su utilización no infrinja derechos de terceros.

INCIDENTES DE SEGURIDAD RELACIONADOS CON IA

Cualquier incidente o sospecha de incidente relacionado con el uso de herramientas de Inteligencia Artificial deberá ser reportado inmediatamente al área correspondiente.

Se consideran, entre otros, posibles incidentes:

- Ingreso accidental de información confidencial en una herramienta no autorizada.
- Exposición de datos personales.
- Divulgación accidental de información corporativa.
- Uso de una herramienta de IA no autorizada.
- Pérdida o exposición de credenciales utilizadas para acceder a una herramienta de IA.
- Generación o distribución accidental de información incorrecta que pueda afectar un proceso corporativo.
- Identificación de comportamientos o respuestas que puedan representar un riesgo para la seguridad de la información.

Los incidentes serán gestionados de acuerdo con los procedimientos internos de gestión de incidentes de seguridad de la información.

MONITOREO Y CUMPLIMIENTO

La organización podrá realizar las actividades de seguimiento y verificación que considere necesarias para evaluar el cumplimiento de la presente política, de acuerdo con sus procedimientos internos y la normatividad aplicable.

El incumplimiento de los lineamientos establecidos podrá ser revisado por las áreas correspondientes y dar lugar a las acciones definidas en la presente política y demás disposiciones internas de la organización.

ACTUALIZACIÓN DEL LISTADO DE HERRAMIENTAS AUTORIZADAS

El listado de herramientas de Inteligencia Artificial autorizadas deberá ser revisado periódicamente por el área de Tecnología y/o Seguridad de la Información.

La organización podrá:

- Autorizar nuevas herramientas.
- Restringir funcionalidades.
- Modificar las condiciones de uso.
- Suspender temporalmente una herramienta.
- Retirar una herramienta del listado de autorizadas.
- Establecer diferentes niveles de acceso según el tipo de usuario o información.

Cualquier modificación al listado oficial deberá ser comunicada a los usuarios cuando corresponda.

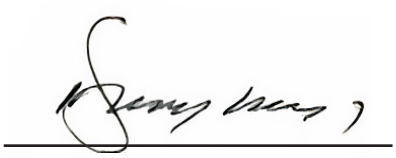
INCUMPLIMIENTO

El incumplimiento de esta política podrá dar lugar a medidas disciplinarias de acuerdo con el Reglamento Interno de Trabajo, las políticas corporativas, los acuerdos contractuales y la legislación vigente.

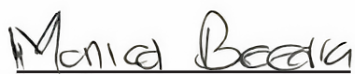
Cuando el incumplimiento pueda constituir un incidente de seguridad de la información, protección de datos, propiedad intelectual o cualquier otra situación de carácter legal, la organización podrá realizar las investigaciones y acciones correspondientes.

4. CONTROL DE CAMBIOS

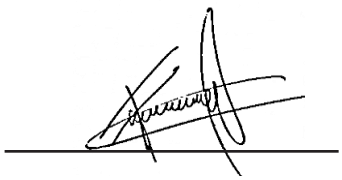
VERSION	FECHA	DESCRIPCIÓN DEL CAMBIO
1	15/10/2024	Se crea el manual de políticas de seguridad de la información.
1	08/10/2025	Se realiza revisión del manual y no presenta cambios.
2	08/10/2026	Se actualiza el Manual de Políticas de Seguridad de la Información mediante la incorporación de nuevas políticas.



DIVA LANDINEZ BAQUERO
Representante Legal



MONICA BECERRA LUNA
Jefe de Calidad



JUAN FELIPE RODIRGUEZ
Aux. Sistemas

ELABORÓ	Monica Becerra – Jefe de Calidad y Tecnología (IT)
REVISÓ	Monica Becerra – Jefe de Calidad y Tecnología (IT)
APROBÓ	Diva Landinez – Gerente General
FECHA DE APROBACIÓN 15/10/2024	