POLÍTICA SEGURIDAD DE LA INFORMACIÓN

Comercializadora de Vehículos Importados S.A

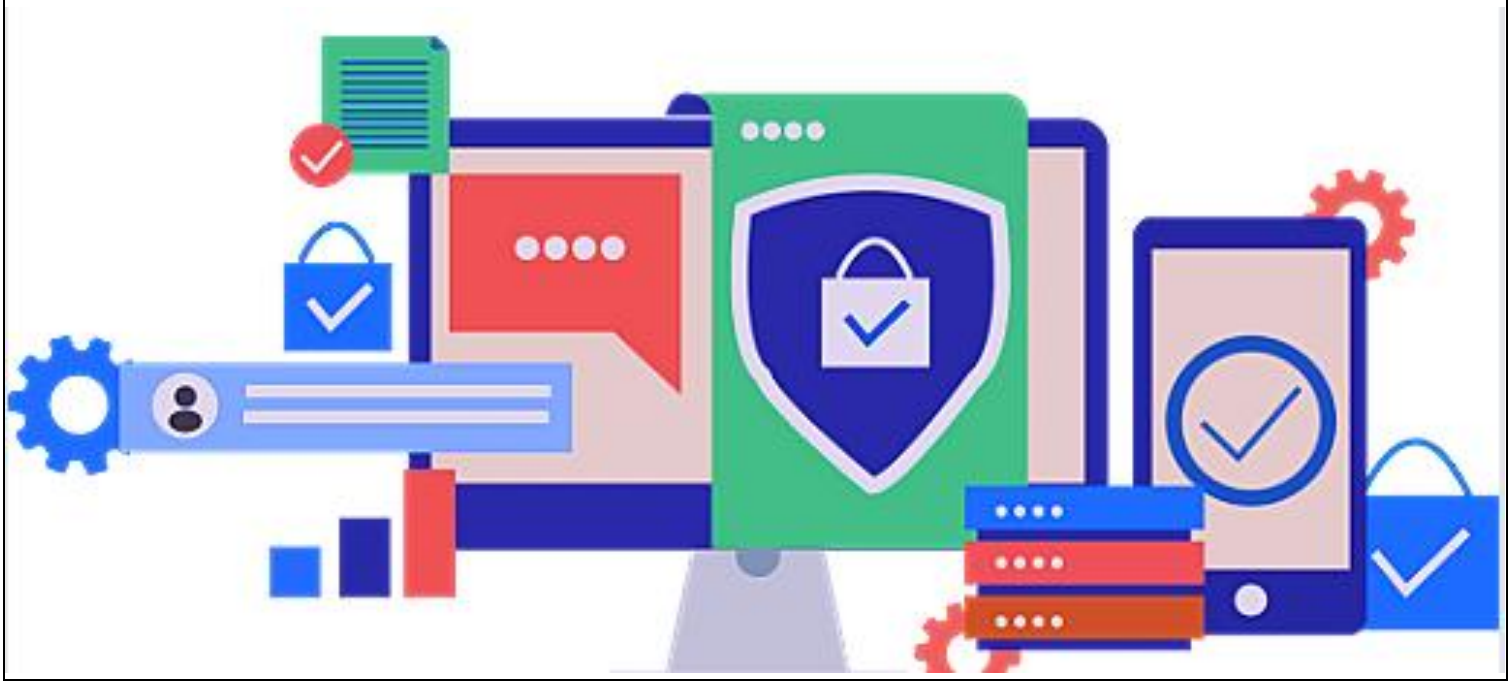


Tabla de Contenido

1. OBJETIVO GENERAL. 3
2. ALCANCE. 3
3. RESPONSABILIDADES. 3
4. CONDICIONES GENERALES. 4
4.1. TERMINOS Y DEFINICIONES. 4
4.2. PRESTACIÓN DE SERVICIOS TÉCNOLOGIA. 5
5. NIVELES DE CONFIDENCIALIDAD. 5
6. USO GENERAL Y PROPIEDAD DE LA INFORMACIÓN. 7
7. CLASIFICACIÓN DE FALTAS POR INCUMPLIMIENTO. 8
8. FUNCIONES SEGREGACIÓN DE FUNCIONES. 9
9. USO DE REDES DE DATOS. 10
10. CONTROL BIOMETRICO. 12
11. ACCESO A WIFI. 12
12. USO DE EQUIPOS DE COMPUTO Y DISPOSITIVOS MÓVILES. 13
13. ASIGNACIÓN Y USO DE USUARIOS Y CONTRASEÑAS. 15
14. ACCESO Y USO DE APLICACIONES. 15
15. MANTENIMIENTOS DE EQUIPOS. 16
16. TRABAJO EN CASA. 16
17. ESCRITORIO DESPEJADO Y PANTALLA DESPEJADA 17
18. POLÍTICA PARA INTERCAMBIO DE INFORMACIÓN. 18
19. PROTECCIÓN CONTRA CÓDIGOS MÓVILES O MALICIOSOS. 18
20. ALMACENAMIENTO DE INFORMACIÓN. 20
21. RESPALDO DE INFORMACIÓN. 20
22. POLITICA PARA INFORMACIÓN DISPONIBLE AL PUBLICO. 21
23. USO DE INTERNET. 21
24. USO DE CORREO ELECTRÓNICO - MENSAJERÍA ELECTRÓNICA. 22

Este documento es propiedad de Comercializadora de Vehículos Importados S.A. es para consulta y uso de sus procesos.

25. POLITICA DERECHOS DE AUTOR. 23
26. POLITICA DE INSTALACIÓN DE SOFTWARE. 23
27. POLITICA DE ELIMINACIÓN DE INFORMACIÓN Y BORRADO SEGURO. 24
28. POLÍTICA DE INTELIGENCIA DE AMENAZAS. 25
29. GESTIÓN DE INCIDENTES DE SEGURIDAD. 25

Este documento es propiedad de Comercializadora de Vehículos Importados S.A. es para consulta y uso de sus procesos.

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN
COMERCIALIZADORA DE VEHÍCULOS IMPORTADOS S.A.

Comercializadora de Vehículos Importados S.A – CVI S.A. es una Organización dedicada a:

- ✓ Comercialización de vehículos automotores nuevos y usados;
- ✓ Comercialización de partes, piezas (autopartes) y accesorios (lujos) de vehículos automotores;
- ✓ Prestación de servicios de mantenimiento y reparación de vehículos automotores

Como parte de su planeación estratégica establece como prioridad la mejora continua de sus procesos obteniendo beneficios de productividad, eficiencia y eficacia en su operación, para esto se establecen el siguiente compromiso con alcance a sus colaboradores, contratistas, visitantes y demás partes interesadas:

1. OBJETIVO GENERAL.

Establecer los lineamientos para la administración y control de la seguridad informática teniendo en cuenta que la administración de los servicios tecnológicos es subcontratada con un Proveedor (Gestión Franca) y su finalidad es salvaguardar la información o capital intelectual de la Organización en caso de materializarse un riesgo que ataque una amenaza o vulnerabilidad por causa de un ciberataque sin importar la naturaleza de su fuente, para esto se implementan controles, optimizando el uso eficiente de los sistemas de información, correo electrónico, redes de datos, Internet y demás recursos informáticos, asegurando calidad en el desarrollo de las responsabilidades y funciones de los Colaboradores de la Organización Comercializadora de Vehículos Importados S.A.- CVI S.A, dentro de un marco de seguridad informática.

2. ALCANCE.

Estas políticas son aplicables a todos los Colaborades de la Organización tales como empleados directos, temporales, aprendices, contratistas, prove edores tecnológicos y su incumplimiento es considerada como una falta grave de conformidad con las políticas de la Organización.

3. RESPONSABILIDADES.

Todos los niveles de la Organización incluyendo Gestión Franca como proveedor tecnológico de Comercializadora de Vehículos Importados S.A.- CVI S.A. deben cumplir con los lineamientos establecidos en el presente documento.

Este documento es propiedad de Comercializadora de Vehículos Importados S.A. es para consulta y uso de sus procesos.

4. CONDICIONES GENERALES.

4.1. TERMINOS Y DEFINICIONES.

Antivirus: Programas especializados en la detección y, si es posible, en la destrucción de virus informáticos.

Certificado: Un certificado es una declaración que garantiza la identidad del emisor, así como la integridad y confidencialidad de la información del documento firmado digitalmente, el certificado declara que un determinado servidor web es seguro, genuino y asegura que ningún otro sitio web puede suplantar la identidad del servidor original.

Contraseña de Acceso: Una clave de acceso compuesta de letras, números y signos que debe teclearse para obtener acceso a un programa, partes de un programa o equipo determinado.

Correo Electrónico: También conocido como e-mail, permite el intercambio de mensajes, archivos, imágenes, etc. aparte del texto.

Encriptación en un Sitio Seguro: Los servidores y clientes de Internet utilizan un sistema de criptografía basado en claves públicas para obtener un sistema seguro de envío y recepción de información. Solo el servidor y el navegador pueden encriptar y desencriptar su información. Durante el tránsito por Internet, la información es un conjunto de datos sin sentido e indescifrable. Un tercero puede hipotéticamente llegar a ver los datos, pero no podrá interpretarlos. La información permanece Segura y privada.

Doble Factor de Autenticación (2FA): El doble factor de autenticación (en ingles Two Factor Authentication o 2FA), también llamado autenticación de dos pasos, es una medida de seguridad que sirve para verificar la identidad de la persona que quiere ingresar a una cuenta.

Internet: Red informática de comunicación internacional que permite el intercambio de todo tipo de información entre sus usuarios. El nombre proviene del acrónimo de las palabras inglesas International Network (red internacional).

Mensajería electrónica: Sistema de intercambio de mensajes sin soporte papel, es decir, de ordenador a ordenador. Puede operarse en cualquiera de los sistemas de red de comunicaciones, respetando determinados protocolos.

Nombre de usuario: Nombre que identifica el usuario dentro del sistema de información.

SPAM: Se denomina con este término al correo electrónico que se recibe de forma indeseada, generalmente con carácter comercial.

Este documento es propiedad de Comercializadora de Vehículos Importados S.A. es para consulta y uso de sus procesos.

Servidor Seguro: Es un servidor Web que utiliza protocolos de seguridad (por ej.: SSL, HTTPS) al ejecutar transacciones. Los protocolos de seguridad utilizan técnicas de cifrado y autenticación como medios para incrementar la confidencialidad y la fiabilidad de las transacciones.

Servicios en la Nube: cualquier servicio de computación proporcionado a través de internet, incluyendo almacenamiento, bases de datos, servidores y software.

Sitio seguro: Un sitio seguro se instala sobre un servidor que dispone de los programas necesarios para implementar el protocolo de seguridad, que permitirá que toda la información viaje encriptada desde el cliente al servidor o viceversa. Con el fin de asegurar que ese sitio es realmente seguro, determinadas empresas de consultoría emiten certificados que se integran en la instalación del servidor seguro, para garantizar al usuario la autenticidad de las páginas que visita.

Sistemas ofimáticos: Conjunto de aplicaciones integradas destinadas al tratamiento más común de la información, con unas características que la hacen especialmente valiosa para el usuario, dentro de estos tenemos: office, entre otros.

Virus: Un virus es un programa informático que se ejecuta en la máquina de cómputo sin previo aviso y que puede corromper el resto de los programas, archivos de datos e, incluso el mismo sistema operativo.

4.2. PRESTACIÓN DE SERVICIOS TÉCNOLOGIA.

La Organización cuenta con un contrato con el proveedor de tecnología Gestión Franca el cual:

1. Contiene un acuerdo de confidencialidad antes de iniciar la prestación del servicio.

2. Se especifica claramente las condiciones las condiciones del contrato.

3. Cuando existan cambios en los servicios que prestan, estos deben ser documentados e incluidos en los acuerdos de servicios o contratos.

4. Aclara que se deberán ejecutar auditorías para evaluar la seguridad de la información evaluando como mínimo la integridad, disponibilidad, confidencialidad y calidad del servicio.

5. NIVELES DE CONFIDENCIALIDAD.

La Organización define las siguientes categorías de confidencialidad:

Este documento es propiedad de Comercializadora de Vehículos Importados S.A. es para consulta y uso de sus procesos.

- ✓ Altamente Confidencial: Información sensible para la Organización que no se ha puesto a disposición de los Colaboradores, para poder ser consultada se requiere de autorización por parte del Líder del Proceso o Gerencia General.

- ✓ Confidencial: son documentos con acceso restringido a diferentes niveles de la Organización, debido a su contenido sensible.

La Organización define como información reservada (confidencial) para protección, toda información que contenga la Operación de la Organización en especial la relacionada con los procesos y procedimientos a las que se tenga acceso de acuerdo a las funciones a realizar dentro de los roles y responsabilidades de los Colaboradores, para esto toda contratación que tenga la Organización debe tener un acuerdo de Confidencialidad donde se define que la información reservada (confidencial) es:

- Cifras.
- Procesos.
- Listados.
- Planes de negocio.
- Información relacionada con la estructura corporativa.
- Servicios de la compañía.
- Productos.
- Servicios suministrados y ofrecidos.
- Procedimientos internos relacionados con el desarrollo del objeto social de la compañía.
- Formatos desarrollados por la compañía tanto para procesos internos como externos.
- Información técnica sobre la operación de la compañía.
- Toda aquella información que pueda guardar relación con el objeto social de la compañía y los servicios y productos ofrecidos.
- Información contenida en las hojas de vida de colaboradores.
- Resultados de pruebas psicotécnicas.
- Memorandos de recomendaciones.
- Bases de datos (clientes), colaboradores, presupuestos, etc.

Quien tenga acceso a la información se compromete a suscribir nuevas cláusulas de confidencialidad o a modificar las existentes, en la medida la Organización declare como tal, nueva información de carácter reservado y que éste deba conocer con ocasión de la ejecución del contrato de trabajo o del vínculo comercial.

Este documento es propiedad de Comercializadora de Vehículos Importados S.A. es para consulta y uso de sus procesos.

El receptor de la información asume la obligación de no usar, explotar, divulgar, revelar, exhibir o adquirir sin autorización la Organización, en beneficio propio o de un tercero, la información o documentación reservada a la que tenga acceso. En consecuencia, reconoce y acepta que Comercializadora de Vehículos Importados S.A. – CVI S.A. es titular exclusivo de cualquier derecho sobre la información y documentación a la que tenga acceso con ocasión del contrato de trabajo o el vínculo comercial que tenga con la Organización. Igualmente, reconoce y acepta que respecto de la información mencionada no tiene derecho alguno, obligándose a no copiarla, a no duplicarla, a no sustraerla y a no comunicarla, en favor de terceros, ni a usarla para sí, durante el tiempo que dure la relación laboral o comercial ni en momento posterior a la terminación esta.

Adicionalmente, el receptor de la información se obliga, a que, una vez terminada la relación laboral o comercial existente con la Organización, devolverá toda la documentación, que se le haya dado en ejecución del mismo.

Para el cumplimiento de estas obligaciones todo Colaborador de la Organización debe firmar un acuerdo de confidencialidad el cual con lleva que la información a la que puedan tener acceso, la cual es de naturaleza reservada y constituye un activo intangible de vital importancia para la Organización

- ✓ Interno y/o Protegida: son documentos a los cuales tienen acceso de todos los niveles de la Organización.

- ✓ Público: son documentos que pueden ser conocidos por las partes interesadas externas de la Organización.

6. USO GENERAL Y PROPIEDAD DE LA INFORMACIÓN.

Comercializadora de Vehículos Importados S.A. – CVI S.A. es propietario de toda la información generada y capital intelectual de la Organización de acuerdo al **AD-PR-01 Procedimiento para el manejo de la Información Documentada**, sin embargo, el Proveedor Tecnológico Gestión Franca es administrador de toda información generada o adquirida por bases de datos, servidores y computadores de propiedad de la Organización.

- ✓ En caso de que la Organización perciba robo, perdida o divulgación no autorizada de la Información, debe reportar directamente al proveedor tecnológico.

Este documento es propiedad de Comercializadora de Vehículos Importados S.A. es para consulta y uso de sus procesos.

- ✓ Los Colaboradores de la Organización pueden acceder, usar o compartir la información solicitado por tercero siempre y cuando se encuentren debidamente autorizados y sea necesaria para el cumplimiento de funciones y responsabilidades.

- ✓ Los Colaboradores de la Organización son responsables de ejercer un buen uso de los recursos tecnológicos a su cargo como lo son Computadores y Dispositivos Móviles.

- ✓ Por razones de Seguridad los únicos autorizados para ingreso al DataCenter para monitoreo de equipos, sistemas y tráfico de la red, son los Proveedores Tecnológicos como se define en el **AD-PR-02 Procedimiento para la Gestión de Visitantes**.

- ✓ De acuerdo a la política de seguridad de la Información del Proveedor Tecnológico, ***"Gestión Franca se reserva el derecho de auditar las redes, dispositivos y sistemas de manera periódica validando cumplimento de sus políticas".***

7. CLASIFICACIÓN DE FALTAS POR INCUMPLIMIENTO.

La organización define las siguientes faltas por incumplimiento en materia de ciberseguridad:

Faltas Leves: Se consideran faltas leves siempre y cuando sean notificadas por primera vez y no hayan generado perjuicio alguno a la Organización:

a) No utilizar el celular corporativo en caso de ser asignado,
b) No utilizar la guaya del equipo asignado y dejarlo a la vista del público.
c) No reportar incidentes de ciberseguridad de manera inmediata.
d) Incumplimiento de procedimientos internos para áreas restringidas.
e) Utilizar el celular corporativo de manera inadecuada para fines personales.
f) Utilizar el celular corporativo sin clave de acceso ni biométrico.
g) Realizar cambios en la configuración inicial del celular corporativo.
h) Descarga de aplicativos no autorizados por la Organización tanto para celulares como para equipos de cómputo.
i) Compartir usuarios y claves de acceso de equipos y/o aplicativos manejados por cada área.
j) Solicitar modificación de perfil de usuario a Mesa de Ayuda sin la debida autorización del área administrativa.

Faltas Graves:

a) No acatar las recomendaciones notificadas por primera vez sobre incumplimiento de las políticas establecidas en ciberseguridad.

Este documento es propiedad de Comercializadora de Vehículos Importados S.A. es para consulta y uso de sus procesos.

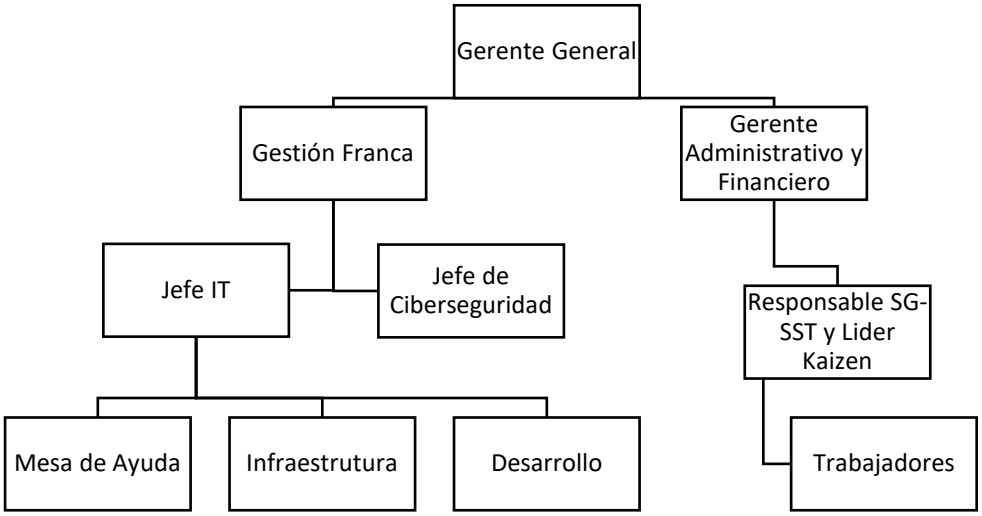
b) Permitir el acceso a áreas restringidas sin solicitar autorización al área administrativa.
c) No cumplir con los compromisos de confidencialidad, exclusividad y permanencia establecidos en contrato y en el reglamento interno de trabajo.
d) Suministrar a terceras personas, sin autorización expresa de la empresa, datos relacionados con la organización o sus sistemas, servicios o procedimientos.
e) Crear o alterar documentos que tengan poder representativo o probatorio en su relación laboral para utilizarlos en su beneficio personal.
f) Divulgar, publicar o comunicar a terceros, por cualquier medio y de utilizar para fines distintos a los propios del contrato, cualquier información que sea catalogada como importante y confidencial por la empresa y que conozca en virtud de la ejecución de su contrato o por cualquier otra causa.
g) El incumplimiento por parte de los Colaboradores de la Organización en cualquiera de las obligaciones de confidencialidad, se considerará como una falta grave que dará lugar a la terminación inmediata y con justa causa del contrato de trabajo existente, Lo anterior, sin perjuicio de las acciones que tiene la Organización tanto si por dicha violación tiene que asumir responsabilidad de cualquier índole, o si se ve de algún modo perjudicado, de acuerdo a como lo establece el código de comercio en el Títulos II, III, IV; V, VI, VII, VIII, IX X, XI, XII, Y XII del libro Tercero y el artículo 238 y siguientes de la decisión Andina 486 de 2000.

8. FUNCIONES SEGREGACIÓN DE FUNCIONES.

Todo Colaborador que en su tarea tenga acceso a la infraestructura tecnológica y a los sistemas de información, debe contar con una definición clara de los roles y responsabilidades, así como del nivel de acceso y los privilegios correspondientes, con el fin de reducir y evitar el uso no autorizado o modificación sobre los activos de información de la Organización.

Este documento es propiedad de Comercializadora de Vehículos Importados S.A. es para consulta y uso de sus procesos.

Para cumplimiento y control la organización junto con el proveedor tecnológico define la siguiente estructura Organizacional para manejo de la política de seguridad de la información:



9. USO DE REDES DE DATOS.

La Organización implementa las siguientes medidas de control para uso de redes de datos:

- ✓ Es responsabilidad del Proveedor Tecnológico Gestión Franca el buen uso y la manipulación de las redes de datos de la Organización, y según sus Políticas Internas:

  "La manipulación de los puntos de red, puntos de Switches y panel de cableado deben ser autorizados por ellos.

  El acceso lógico y físico a los equipos especializados de cómputo como servidores, router etc., deberá ser exclusivo y administrado por Gestión Franca. Para el caso especial de terceros y proveedores de servicios especializados la Organización debe solicitar autorización.

  Por lo menos una vez al año Gestión Franca valida la viabilidad de realizar mantenimiento preventivo y peinado de los Datacenter y centros de cableado.

  La instalación de canales dedicados y conexiones con redes externas se debe solicitar por la dirección del área a utilizar y la debe autorizar Gestión Franca.

Este documento es propiedad de Comercializadora de Vehículos Importados S.A. es para consulta y uso de sus procesos.

La Organización cuenta con un diagrama actualizado de las redes lógicas que se tienen en la Organización y de los Datacenter.

La creación de nuevas redes lógicas o reconfiguración de las existentes, solo ser adelantada por el personal autorizado por Gestión Franca.

- ✓ Los puntos de red que se encuentren libres en la canaleta se deben deshabilitar en el centro de cableado y únicamente deben ser habilitados por el personal autorizado.

- ✓ Los servidores son dedicados, por lo que se prohíbe los accesos a cualquiera de ellos con cualquier tipo de herramienta o software diferente a los sistemas de información de la compañía excepto para el personal de Gestión Franca.

- ✓ Todos los dispositivos electrónicos y computadores que se conecten a la red de datos deben cumplir con los requisitos mínimos establecidos en el registro del **Proveedor Procedimiento general de infraestructura.**

- ✓ El acceso a los computadores, servidores y aplicaciones de la red interna desde redes externas no se encuentra permitido de acuerdo a lo establecido en el registro del **Proveedor Procedimiento general de infraestructura.**

- ✓ El acceso a la red a través del servicio VPN solo está permitido para el personal de Gestión Franca y es exclusivamente para labores técnicas. Por ningún motivo podrán utilizarse herramientas de software diferentes para establecer conexión a estos desde redes externas.

- ✓ El acceso a VPN está permitido para el trabajo en casa.

- ✓ Todos los accesos desde y hacia redes externas como internet son protegidos y monitoreados por medio de Firewall de seguridad para garantizar la seguridad de la información.

- ✓ No está permitido intervenir las redes de cableado, instalando cables, cortando o empalmando cables, desprendiendo marcaciones de tomas, puertas o productos, golpeando o forzando tubos y/o canaletas.

- ✓ La solicitud de creación o modificación de accesos a las redes, se debe hacer utilizando el sistema de gestión de solicitudes (Mesa de Ayuda) de Gestión Franca.

- ✓ El acceso a las redes se realiza de acuerdo con las funciones del cargo que desempeña el usuario.

Este documento es propiedad de Comercializadora de Vehículos Importados S.A. es para consulta y uso de sus procesos.

- ✓ Está prohibido conectar dispositivos personales a la red local para esto debe utilizarse el acceso a WI-FI para clientes como red alterna implementada en la empresa y en caso de identificar que un tercero no autorizado está utilizando la red local, debe realizar el reporte inmediato a la Gerencia Administrativa y Financiera.

10. CONTROL BIOMETRICO.

La Organización cuenta con control biométrico por huella el cual permite monitorear el reporte del ingreso y salida de los Colaboradores (Empleados y Terceros), en las instalaciones.

Su control en el manejo de inclusión y retiro de los Colaboradores debe realizarlo la Coordinadora de Gestión Humana una vez sea notificada o se presente la novedad de retiro o ingreso de Colaboradores a la Organización.

11. ACCESO A WIFI.

La Organización implementa las siguientes medidas de control para el acceso a WiFi:

- ✓ El acceso a las redes Wifi de la Organización se debe realizar por autenticación Radius con su respectivo usuario y contraseña.

- ✓ La navegación de las redes corporativas está controlada por perfiles de navegación web y tienen protección de seguridad.

- ✓ Las redes Wifi para clientes o visitantes se debe realizar mediante accesos independientes a las corporativas por lo que está segmentada de la red corporativa, esta red debe contar con contraseña de ingreso, estar configurada bajo el firewall con protección de seguridad y contar con restricciones de navegación a listas negras y direccionamiento IP bloqueado en el firewall, en caso de que se presente inconvenientes de conexión se debe solicitar apoyo a Gestión Franca.

- ✓ La Organización establece que está prohibido:

  - Conectar los computadores corporativos a redes Wifi Publicas o desconocidas.

  - La conexión a internet mediante las redes de Wifi para clientes o invitados, salvo a excepciones de fuerza mayor por continuidad de la operación.

  - Transmisión de Contenido fraudulento, difamatorio, obsceno, ofensivo o de vandalismo, insultante o acosador, sea este material o mensajes.

Este documento es propiedad de Comercializadora de Vehículos Importados S.A. es para consulta y uso de sus procesos.

- Interceptar, recopilar o almacenar datos sobre terceros sin su conocimiento o consentimiento. Escanear o probar la vulnerabilidad de equipos, sistemas o segmentos de red. Enviar mensajes no solicitados (spam), virus, o ataques internos o externos.

- Enviar mensajes no solicitados (spam), virus, o ataques internos o externos.

- Obtener acceso no autorizado a equipos, sistemas o programas tanto al interior de la red como fuera de ella. Tampoco podrá utilizar la red WIFI para obtener, manipular y compartir cualquier archivo de tipo musical o filmográfico, sin tener los derechos de propiedad intelectual.

- Dañar equipos, sistemas informáticos o redes y/o perturbar el normal funcionamiento de la red y sea usada con fines de lucro, actividades comerciales o ilegales, por ejemplo, hacking. Ser utilizada para crear y/o la colocar un virus informático o malware en la red.

- Transmitir, copiar y/o descargar cualquier material que viole cualquier ley. Esto incluye entre otros: material con derecho de autor, pornografía infantil, material amenazante u obsceno, o material protegido por secreto comercial o patentes.

12. USO DE EQUIPOS DE COMPUTO Y DISPOSITIVOS MÓVILES.

La Organización implementa las siguientes medidas para el uso de equipos de cómputo y dispositivos móviles:

✓ Todos los equipos conectados a la red de la Organización deberán hacerlo utilizando una cuenta valida registrada en el Directorio Activo del proveedor de tecnología Gestión Franca.

✓ Ningún usuario debe tener permisos de administrador sobre los computadores de la Organización con el propósito de proteger los equipos contra virus y evitar la instalación de software no licenciado o autorizado.

✓ Los equipos se encuentras con restricción de acceso a internet, a las unidades CD/DVC y puertos Usb.

✓ Los equipos están protegidos de descargas eléctricas, se debe realizar conexión siempre a la corriente regulada y deberá estar alejado de fuentes de calor.

Este documento es propiedad de Comercializadora de Vehículos Importados S.A. es para consulta y uso de sus procesos.

- ✓ Los equipos están configurados con acceso a internet de acuerdo al Registro del Proveedor Tecnológico Procedimiento gestión de usuarios.

- ✓ Todo el personal comercial debe utilizar un dispositivo móvil asignado directamente por la Organización y debe realizarse su solicitud por correo electrónico a la Coordinadora de Gestión Humana.

- ✓ No está permitido el uso de computadores personales o ajenos al asignado para la ejecución de las funciones.

- ✓ No esta permitido el uso de celulares personales dentro de las áreas sensibles o criticas como lo son Datacenter y centros de cableado.

- ✓ No está permitido la configuración de correo corporativo en dispositivos que no son propiedad de la Organización como se indica en el registro del proveedor Procedimiento para la Gestión de Usuarios.

- ✓ No está permitido el retiro de computadores o accesorios del puesto de trabajo sin previa autorización.

- ✓ No está permitido el consumo de bebidas ni alimentos en los sitios de trabajo.

- ✓ Todo computador portátil debe contar con guaya de seguridad mientras se encuentre en uso en la estación de trabajo y se revisara por parte del Responsable del SG-SST y Líder Kaizen que se esté cumplimiento y en caso de identificarse gestionara corrección inmediata.

- ✓ En caso de que el proveedor tecnológico determine en alguna inspección o soporte que el dispositivo utilizado por algún usuario este para baja, se debe informar a la Organización y la Organización será la encargada de realizar la solicitud por medio de Mesa de Ayuda para que realicen la gestión pertinente.

- ✓ No estar permitido pegar calcomanías o cualquier tipo de adorno en los equipos.

- ✓ La instalación de cualquier tipo de software en los computadores es responsabilidad de Gestión Franca.

- ✓ No está permitido que el usuario instale cualquier tipo de Software en los computadores de la Organización.

Este documento es propiedad de Comercializadora de Vehículos Importados S.A. es para consulta y uso de sus procesos.

13. ASIGNACIÓN Y USO DE USUARIOS Y CONTRASEÑAS.

La Organización implementa las siguientes medidas para la asignación de usuarios y contraseñas:

- ✓ El proveedor de tecnología es el encargado de realizar la activación y desactivación de usuarios de acuerdo a su registro Procedimiento de gestión de usuarios de Usuarios.

- ✓ Las contraseñas asignadas a los usuarios son personales e intransferibles.

- ✓ Las contraseñas se deben cambiar periódicamente las cuales se encuentran programadas por política del controlador de dominio y la cual se fija en un periodo cada 30 días.

- ✓ Las contraseñas deben cumplir:

  - No contener nombre de la cuenta o usuario o nombres y apellidos del usuario.
  - Tener una longitud mínima de ocho caracteres.
  - Incluir caracteres de las siguientes tres categorías.
    - Mayúsculas (de la A a la Z).
    - Minúsculas de la (A a la Z).
    - Dígitos de base 10 del (0 al 9).
    - Caracteres no alfanuméricos (por ejemplo $, #, %, *).
    - No asignar claves que ya hayan sido asignadas.

- ✓ Se debe cambiar las contraseñas de inicio asignadas durante la creación de usuarios.

- ✓ No se debe guardar registros en papel o virtual de contraseñas.

- ✓ No está permitido usar contraseñas estáticas para el acceso a scripsts o aplicaciones.

- ✓ No está permitido guardar contraseñas en navegadores e incluir contraseñas en procedimientos automáticos de conexión.

14. ACCESO Y USO DE APLICACIONES.

La Organización establece:

- ✓ El ingreso a las aplicaciones debe ser con el usuario y clave asignadas.

Este documento es propiedad de Comercializadora de Vehículos Importados S.A. es para consulta y uso de sus procesos.

- ✓ No está permitido la suplantación de usuarios para el ingreso a las aplicaciones.
- ✓ La información ingresada a las aplicaciones debe ser real.
- ✓ El acceso al ERP se encuentra limitado por roles previamente definidos.
- ✓ Las modificaciones del ERP se realizan de acuerdo a lo establecido en registro Procedimiento Marco de Referencia Desarrollo.
- ✓ El acceso a bases de datos desde las aplicaciones o cualquier ambiente que requiera consultarla información de las mismas debe realizarse de acuerdo a la política de seguridad de bases de datos.
- ✓ No se debe acceder a los aplicativos y/o herramientas utilizadas en la Organización desde lugares públicos de internet.

15. MANTENIMIENTOS DE EQUIPOS.

La Organización debe realizar mantenimientos de sus equipos para ello establece:

- ✓ Gestión Franca es el responsable del mantenimiento preventivo y correctivo de los equipos de cómputo de acuerdo al registro de mantenimiento preventivos equipos.
- ✓ Se debe solicitar autorización a Gestión Franca en caso de requerir ejecución de mantenimiento de manera externa, ajustes, cambios en configuración o cambios en el hardware y cualquier otra actividad que vaya en contra de la integridad física del equipo, de las políticas de seguridad, de los derechos de autor, de la integridad de los datos.

16. TRABAJO EN CASA.

La Organización permite que sus Colaboradores realicen su trabajo fuera de las instalaciones de la Organización. El trabajo en casa incluye el uso de teléfonos móviles, para esto la Organización establece:

- ✓ El acceso a los recursos de tecnología y al ERP, la conexión se debe realizar únicamente garantizando la conexión a través de VPN, por lo que previo al trabajo en casa se debe validar con el Proveedor Tecnológico Gestión Franca, si se cumple con el perfil requerido y con las necesidades para realizar el trabajo en casa.

Este documento es propiedad de Comercializadora de Vehículos Importados S.A. es para consulta y uso de sus procesos.

- ✓ El acceso a los recursos de tecnología disponibles se debe realizar únicamente desde computadores y equipos de la Organización. No está permitido el uso de computadores ni dispositivos personales.

- ✓ Las áreas de trabajo remoto que autorice la organización fuera de su sede deben cumplir con todas las políticas y controles del sistema de seguridad definido por la Organización.

- ✓ El usuario de servicios remotos deberá sujetarse al Reglamento de uso de la Red y en concordancia con las políticas generales de uso de Internet definidos por la Organización

- ✓ Es responsabilidad de los usuarios que trabajen desde casa reportar a través de la mesa de ayuda cualquier anormalidad que llegue a presentarse con los equipos tecnológicos que tenga a disposición fuera de la Organización.

17. ESCRITORIO DESPEJADO Y PANTALLA DESPEJADA

La Organización establece los siguientes controles alineándose a las políticas de control del proveedor Tecnológico Gestión Franca:

- ✓ Todo Colaborador está obligados a utilizar protectores de pantallas protegidos con contraseña o a dejar cerradas todas las sesiones cuando abandonan su puesto de trabajo y cuando regrese, debe introducir nuevamente la contraseña del usuario para acceder de nuevo a la información.

- ✓ En los equipos tienen configurado una política de directorio activo la cual activa automáticamente protectores de pantalla con clave como política del directorio activo. Este se debe disparar en el momento en que transcurran 45 segundos desde la última vez que se manipuló él computador.

- ✓ Se debe apagar el computador al alejarse por períodos prolongados de tiempo o al finalizar la jornada laboral.

- ✓ La información clasificada como “privada” y “confidencial” en medio físico se debe mantener bajo llave, esto incluye: documentos impresos, CDs, dispositivos de almacenamiento USB y medios removibles en general; y la magnética almacenada en las particiones del servidor designada.

- ✓ Las impresoras de uso general están protegidas con pin de seguridad asignado por usuario garantizando que el documento solo será impreso cuando el usuario este en la impresora, se debe recoger las impresiones antes de abandonar el puesto de impresión y revisar que no queden documentos en cola de impresión o documentos impresos. En el caso que se destine papel para

Este documento es propiedad de Comercializadora de Vehículos Importados S.A. es para consulta y uso de sus procesos.

reciclaje es responsabilidad del usuario garantizar que la información que se encuentra en estos documentos no contenga información sensible o confidencial, de ser así estos documentos deben ser destruidos.

18. POLÍTICA PARA INTERCAMBIO DE INFORMACIÓN.

Para el intercambio de información la Organización establece:

- ✓ No está permitido realizar intercambio de información sin previa autorización de la Gerencia Administrativa y Financiera.
- ✓ Cuando se envié información sensible por correo electrónico, se debe colocar clave a los archivos adjuntos y está debe ser informada al destinatario por un medio diferente al correo electrónico.
- ✓ Todos los colaborares deben 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 webservices y debe ser configurado por Gestión Franca.
- ✓ 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.
- ✓ En los contratos o acuerdos de servicios se incluyen los requisitos y condiciones requeridas para el intercambio de información.

19. PROTECCIÓN CONTRA CÓDIGOS MÓVILES O MALICIOSOS.

La Organización establece los siguientes controles alineándose a las políticas de control del proveedor Tecnológico Gestión Franca:

- ✓ Cada equipo de la Organización cuenta con instalación de software de antivirus los cuales serán actualizados mensualmente.

Este documento es propiedad de Comercializadora de Vehículos Importados S.A. es para consulta y uso de sus procesos.

- ✓ Restringir el intercambio de CD´s, memorias tipo USB y otros medios removibles de origen desconocido o si fuere necesario, someterlos a la revisión del antivirus instalado en el disco antes de su utilización.

- ✓ Restringir el uso de los equipos por parte de personas ajenas a las actividades propias de la Organización.

- ✓ Se debe contar obligatoriamente con una copia de respaldo de los archivos que se almacenan en la red, Gestión Franca es responsable de la ejecución, custodia y almacenamientos de estas copias.

- ✓ En el caso de los archivos comprimidos bajo el formato ZIP o cualquier otro tipo de archivo que fueron descargados por Internet o por correo electrónico, deberán ser revisados por el antivirus inmediatamente después de haber sido desempaquetados y antes de ser ejecutados.

- ✓ Este mismo tratamiento se deberá dar a los archivos anexados (adjuntos), enviados por correo electrónico, cuidándose de no abrir mensajes de origen desconocido o sospechoso.

- ✓ Verificar en internet la lista de códigos maliciosos nuevos.

- ✓ No se permite la desinstalación y/o desactivación de software y herramientas de seguridad avaladas por Gestión Franca.

- ✓ Las únicas personas autorizadas para desactivar de manera temporal el sistema de antivirus, en cualquier componente de la infraestructura tecnológica de la Organización es Gestión Franca.

- ✓ No se permite utilizar medios de almacenamiento físico o virtual que no sean de carácter corporativo.

- ✓ No se permite escribir, generar, compilar, copiar, propagar, ejecutar o intentar introducir cualquier código de programación diseñado para auto replicarse, dañar o afectar la disponibilidad, integridad y confidencialidad de la información, así como el desempeño de cualquier dispositivo o infraestructura tecnológica de la Organización.

- ✓ Utilizar medios de almacenamiento físico o virtual que no sean de carácter corporativo.

Este documento es propiedad de Comercializadora de Vehículos Importados S.A. es para consulta y uso de sus procesos.

20. ALMACENAMIENTO DE INFORMACIÓN.

La Organización implementa buenas prácticas en seguridad de la información orientados a la prevención de riesgos que puedan afectar la integridad, disponibilidad y confidencialidad de la información, por lo que la Organización establece:

- ✓ Toda la información generada por Colaboradores para el desarrollo de sus funciones debe ser almacenada en las carpetas de los servidores de archivos de destinados para ello.

- ✓ Almacenar únicamente información relacionada con sus actividades laborales, en el espacio asignado.

- ✓ Se deben controlar los derechos de lectura, escritura y modificación para usuarios, preservando siempre los principios de integridad, confidencialidad y disponibilidad de la información. El acceso a la información estará basado en derechos y perfiles de usuario previamente definidos.

- ✓ La clasificación de la información, tipos de usuarios y perfiles de cada sistema debe ser controlando desde el programa de seguridad informática con el fin de mantener la seguridad de la información.

- ✓ Los servidores de archivos de Gestión Franca tienen restricciones de seguridad que no permiten el almacenamiento de archivos ejecutables (.exe , .msi, .bat), 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.

- ✓ Toda la información que sea catalogada como confidencial solo debe ser manejada en los formatos autorizados por los Sistemas de Administración y Control.

21. RESPALDO DE INFORMACIÓN.

La Organización establece que por medio del proveedor de tecnología:

- ✓ Toda información alojada en los servidores se debe realizar copia de respaldo periódicamente de acuerdo procedimientos, para ello se deben seguir con los lineamientos de los Procedimientos establecidos.

Este documento es propiedad de Comercializadora de Vehículos Importados S.A. es para consulta y uso de sus procesos.

22. POLITICA PARA INFORMACIÓN DISPONIBLE AL PUBLICO.

Toda persona natural o jurídica, sin importar o la edad o la nacionalidad, pueden ejercer el derecho de acceso a la información pública. Se puede acceder a la información pública a través de:

- ✓ Consultando directamente en la pagina web, carteleras y cualquier otro medio disponible en la entidad.
- ✓ Solicitando la información directamente a la entidad por los diferentes canales que hay disponibles.

23. USO DE INTERNET.

La Organización define que al acceso a internet de sus usuarios está definida por medio de una matriz de roles y perfiles, sin embargo, el proveedor tecnológico y la organización establecen:

- ✓ Todos los accesos desde y hacia redes externas como internet son protegidos y monitoreados por medio de Firewall de seguridad para garantizar la seguridad de la información.

- ✓ Los colaboradores de la organización se comprometerán a utilizar internet de forma responsable y productiva. El acceso a internet se limita a actividades relacionadas solo con el trabajo y no se permite su uso personal.

- ✓ Toda información de internet redactada, transmitida y/o recibida por los sistemas informáticos de la Organización se reconoce como parte de sus datos oficiales. Por lo tanto, podrá revelarse por exigencias leales o a terceros autorizados.

- ✓ El equipamiento, los servicios y la tecnología utilizados para acceder a internet pertenecen a la Organización, por lo que se reserva el derecho a supervisar el tráfico de internet y a acceder a los datos redactados, enviados o recibidos a través de sus conexiones en línea.

- ✓ Todos los sitios y descargas serán susceptibles de supervisión y/o bloqueo por parte del proveedor tecnológico, si se considerados perjudiciales y/o improductivos para el negocio.

- ✓ Se limita el acceso a sitios que contengan material obsceno, agresivo, pornográfico, ilícito, violento o ilegal en modo alguno.

- ✓ Se limita él envió o la publicación de mensajes o imágenes ofensivas, discriminatorias o amenazantes por internet o a través del servicio de correo electrónico.

Este documento es propiedad de Comercializadora de Vehículos Importados S.A. es para consulta y uso de sus procesos.

- ✓ Se prohíbe el uso de computadores para cometer cualquier tipo de fraude y/o piratear software películas o música.

- ✓ No se puede realizar robo, uso o revelación de las contraseñas de otro usuario sin la debida autorización.

- ✓ Se prohíbe la descarga, la copia o la piratería de software o archivos electrónicos con derechos de autor sin autorización.

- ✓ Se prohíbe el acceso mediante la piratería a páginas web no autorizadas.

24. USO DE CORREO ELECTRÓNICO - MENSAJERÍA ELECTRÓNICA

La Organización asignará una cuenta de correo electrónico a sus Colaboradores. La cuenta es personal e intransferible.

Para ello:

- ✓ Los usuarios son los únicos responsables de todas las actividades realizadas con sus cuentas de correo y de mensajería instantánea y deberán cumplir en todo momento las normas de uso y de seguridad de la red de datos de la Organización.

- ✓ La Organización mantendrá 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 queden bloqueados o en dado caso realizar el reporte a mesa de ayuda con el fin de poder ser analizados de forma manual.

- ✓ La organización mantendrá una herramienta de archivado de correo la cual intercepta todos los correos que salen y entran guardándolos por un periodo de retención establecido.

El uso del correo electrónico no está permitido para:

- ✓ Los correos enviados a través del sistema de correo electrónico de la Organización no podrán incluir contenidos ofensivos. Se incluyen, el uso de lenguaje/imágenes vulgares u ofensivas.

- ✓ Atentar contra la integridad de la Organización.

Este documento es propiedad de Comercializadora de Vehículos Importados S.A. es para consulta y uso de sus procesos.

- ✓ Utilizar el correo electrónico para cualquier propósito comercial o financiero ajeno a las funciones propias de la Organización.
- ✓ Divulgar información que incite a la discriminación o la violencia.
- ✓ Enviar contenidos con fines personales y servicios en beneficio propio, de familiares o de terceros.
- ✓ Enviar correo tipo SPAM, es decir correo basura, relacionado con falsos virus, con publicidad de empresas, cadenas de mensajes, etc.
- ✓ Usar la cuenta de correo electrónico de otro usuario o entregar a un tercero la contraseña propia.
- ✓ Falsificar mensajes de correo electrónico.
- ✓ Leer, borrar, copiar o modificar mensajes de correo electrónico de otras personas, sin su autorización.
- ✓ Enviar mensajes de correo electrónico, alterando la dirección electrónica del remitente para suplantar a terceros; identificarse como una persona ficticia o simplemente no identificarse.
- ✓ Iniciar o continuar cadenas de mensajes pues éstas tienden a congestionar innecesariamente la red.
- ✓ La Organización no asume responsabilidad alguna por los contenidos emitidos a través del correo electrónico o por el uso ilegal y mal intencionado por parte de los usuarios.

25. POLITICA DERECHOS DE AUTOR.

- ✓ Los usuarios no deben realizar copias no autorizadas del software que pertenece a la Organización.
- ✓ Los usuarios no deben copiar software ni otros materiales originales de otras fuentes, y son responsables por todas las consecuencias que pudieran surgir bajo la ley de propiedad intelectual.

26. POLITICA DE INSTALACIÓN DE SOFTWARE.

Este documento es propiedad de Comercializadora de Vehículos Importados S.A. es para consulta y uso de sus procesos.

- ✓ La instalación de software en cada equipo de cómputo, debe ser asignado de acuerdo al procedimiento de Gestión Franca para Alistamiento de Computadores.
- ✓ Corresponde a Gestión Franca emitir normas y procedimientos para la instalación y supervisión del Software básico para cualquier tipo de equipo.
- ✓ Se cuentan con políticas en el Directorio Activo para que se prohíba la instalación de software.
- ✓ Solo se permite la instalación de software con licenciamiento.
- ✓ En caso de requerir un software se debe contar con el apoyo técnico de Gestión Franca.
- ✓ Con el propósito de proteger la integridad de los sistemas informáticos y telecomunicaciones es imprescindible que todos y cada uno de los equipos involucrados dispongan de software de seguridad (Antivirus, privilegios de acceso, y otros que se apliquen).

27. POLITICA DE ELIMINACIÓN DE INFORMACIÓN Y BORRADO SEGURO.

La Organización debe realizar solicitud de al correo electrónico servicioalcliente@gestionfranca.com.co, el cual se puede solicitar modificación o eliminación de información personal almacenada en las bases de datos de Gestión Franca.

Métodos de borrado:

Borrado Físico: Destrucción física de la información mediante la trituración de los documentos.

La eliminación y borrado de física se realizará teniendo en cuenta los tiempos de retención y disposición final de la información establecidos en los procedimientos de gestión documental.

Borrado Lógico: La eliminación de la información almacenada en diferentes dispositivos tecnológicos para cargo no críticos se debe realizar “Formateo del equipo”, en cambio para cargos críticos como lo son jefaturas o cargos donde exista manejo de información confidencial se debe utilizar métodos de sobre escritura de los datos con diversos valores , este borrado no corresponde a métodos de formateo primario sino a métodos seguros que eliminen el riesgo de reconstruir la información, por lo que se debe realizar por lo menos tres ciclos de sobreescritura de datos.

El borrado lógico seguro se debe realiza cuando el equipo se de baja.

Este documento es propiedad de Comercializadora de Vehículos Importados S.A. es para consulta y uso de sus procesos.

28. POLÍTICA DE INTELIGENCIA DE AMENAZAS.

Gestión Franca establece un método de alertamiento relacionado a inteligencia de posibles amenazas en las cuales puedan existir riesgos ante vulnerabilidades asociadas a ataques cibernéticos para esto se debe reportar por medio de Mesa de Ayuda cualquier tipo de amenaza o evento que se considere que puede afectar de forma negativa los activos o sistemas informáticos de la organización.

29. GESTIÓN DE INCIDENTES DE SEGURIDAD.

La organización define las clasifica los incidentes de seguridad en:

Externo: Eventos y/o Incidentes de seguridad que se clasifican en las siguientes categorías de que se pueden llegar a presentar dentro de las cuales se encuentran:

- ✓ **Acceso no autorizado:** Comprende todo tipo de ingreso y operación no autorizado a los sistemas, tanto exitosos como no exitosos. Son parte de esta categoría:

  - Accesos no autorizados exitosos, sin perjuicios visibles a componentes tecnológicos.
  - Robo de información.
  - Borrado de información.
  - Alteración de la información.
  - Intentos recurrentes y no recurrentes de acceso no autorizado.
  - Abuso y/o Mal uso de los servicios informáticos internos o externos que requieren autenticación.

- ✓ **Código malicioso:** Esta categoría comprende la introducción de códigos maliciosos en la infraestructura tecnológica de la Entidad Son parte de esta categoría:

  - Virus informáticos.
  - Troyanos.
  - Gusanos informáticos

- ✓ **Denegación del servicio**: Esta categoría incluye los eventos que ocasionan pérdida de un servicio en particular. Los síntomas para detectar un incidente de esta categoría son:

  - Tiempos de respuesta muy bajos sin razones aparentes.
  - Servicio(s) interno(s) inaccesibles sin razones aparentes.
  - Servicio(s) Externo(s) inaccesibles sin razones aparentes

Este documento es propiedad de Comercializadora de Vehículos Importados S.A. es para consulta y uso de sus procesos.

- ✓ **Escaneos, pruebas o intentos de obtención de información de la red o de un servidor en particular**: Esta categoría agrupa los eventos que buscan obtener información de la infraestructura tecnológica de la Organización. Comprende:

  - Sniffers (software utilizado para capturar información que viaja por la red).
  - Detección de Vulnerabilidades.

- ✓ **Mal uso de los recursos tecnológicos**: Esta categoría agrupa los eventos que atentan contra los recursos tecnológicos por el mal uso. Comprende:

  - Mal uso y/o Abuso de servicios informáticos internos o externos.
  - Violación de las normas de acceso a Internet.
  - Mal uso y/o Abuso del correo electrónico de la Organización.

- ✓ **Violación de las Políticas, Normas y Procedimientos de Seguridad Informática reglamentadas.**

Es deber de los usuarios reportar un incidente de seguridad tan pronto lo detecte o sospeche de ellos. Para el reporte de un incidente de seguridad por correo electrónico a mesa de ayuda con copia al Responsable del SG-SST y Líder Kaizen, el proveedor Tecnológico ejecutara activara el **Procedimiento Gestión Incidentes**.

De acuerdo a los procedimientos internos del Proveedor Tecnológico si se llegara a presentar algún incidente de seguridad detectado con el monitoreo y seguimiento en las consolas de seguridad, se activará el procedimiento de acuerdo al registro **Procedimiento Ciberataque**.

Interno: Eventos y/o Incidentes de seguridad que se clasifican en las siguientes categorías que se pueden llegar a presentar:

Categoría	Tipo	Prevención	Respuesta	Controles
Incidentes relacionados con el acceso y cuentas de usuario	**Uso indebido de credenciales privilegiadas**	Políticas claras en manejo de contraseñas Inducción Organizacional	Solicitar a mesa de ayuda des habilitación del usuario y auditoria del mismo	Validación Mensual de Usuarios Activos

Este documento es propiedad de Comercializadora de Vehículos Importados S.A. es para consulta y uso de sus procesos.

Categoría	Tipo	Prevención	Respuesta	Controles
Incidentes de manejo inadecuado de información	**Fuga de información sensible o confidencial por perdida de equipo**	Canales de reporte	Reporte inmediato a Gestión Franca	Revisión de registros de acceso y pruebas de filtrado de datos.
	Transferencia no autorizada de datos a dispositivos externos por USB	Restringir el uso de dispositivos extraíbles, cifrado obligatorio.	Reporte inmediato a Gestión Franca	Restricción total de puertos USB
	Uso de servicios en la nube no aprobados	Restricción de Perfiles de Navegación.	Identificar servicios utilizados, evaluar el riesgo y migrar datos a entornos seguros.	Políticas claras de uso de servicios cloud.
Incidentes relacionados con software malicioso y vulnerabilidades	**Instalación de software no autorizado o inseguro**	Usuario Administrador con bloqueo para instalación de Software	Desinstalación inmediata, verificación de integridad del sistema y educación del usuario.	Permisos definidos por Directorio Activo
Incidentes relacionados con la infraestructura de TI	**Caídas o interrupciones servicios**	controles de acceso estrictos	Validación con parque industrial y reporte inmediato a Proveedor	Seguimiento de disponibilidad de servicios
Amenazas internas (Insider Threats)	**Espionaje corporativo - Amenaza**	Clasificación de datos sensibles, controles de acceso estrictos y monitoreo de transferencias de información.	Aislar al sospechoso, reforzar controles y cooperar con las autoridades si corresponde.	Revisiones de integridad de sistemas y monitoreo de redes internas.
Incidentes físicos relacionados con la seguridad de TI	**Acceso físico no autorizado Acceso a áreas restringidas**	CCTV y registros de acceso.	Identificación del intruso, reforzamiento de controles físicos y reporte a seguridad física.	Auditorías periódicas de accesos físicos.
	Robo o daño físico de hardware Equipos propios	Uso de anclajes de seguridad, cifrado de discos duros y monitoreo de áreas sensibles.	Reemplazo de equipos, recuperación de datos y reporte a autoridades.	Inventarios actualizados y seguimiento de activos críticos.

Este documento es propiedad de Comercializadora de Vehículos Importados S.A. es para consulta y uso de sus procesos.

Categoría	Tipo	Prevención	Respuesta	Controles
Incidentes relacionados con terceros	**Acceso indebido de proveedores (acceso físico)**	Definición clara de roles y permisos, auditorías de terceros y acuerdos de confidencialidad.	Revocación de accesos indebidos, revisión de contratos y análisis de riesgos.	Políticas de gestión de proveedores y monitoreo de accesos de terceros.
Incumplimiento de políticas y normativas (Se encuentra incluido en el Procedimiento de Incidentes de Gestion franca)	**Violaciones de políticas internas**	Educación continua en ciberseguridad y actualización de políticas.	Investigación del incidente, refuerzo de políticas y sanciones disciplinarias.	Revisiones periódicas del cumplimiento y auditorías internas.
	Fallos en la protección de datos personales	Implementación de controles de privacidad y formación sobre normativas.	Notificación a entes reguladores, investigación de la brecha y corrección inmediata.	Procesos sistemáticos diseñados para identificar y mitigar los riesgos de privacidad asociados con el tratamiento de datos personales en proyectos, sistemas o procesos dentro de la organización.

Canales de reporte de Incidentes de Ciberseguridad Internos: Todo incidente debe ser reportado por correo electrónico al Responsable del SG-SST y Líder Kaizen, el cual será el encargado de realizar su respectiva gestión la cual se basa en:

Detección/Reporte: Verificar si es incidente o no.

Respuesta Inicial: Clasificación y manejo de acuerdo a su nivel de criticidad:

Nivel de Criticidad	Criterio	Tratamiento
Critico	✓ Alta importancia para la Organización y requiere de una toma de decisión inmediata. ✓ No existe contingencia o se violaron los controles ya sea por negligencia o desconocimiento. ✓ Interrupción de las actividades máximo por un día. ✓ Sanciones monetarias por incumplimiento repetitivo de las normas determinadas por los agentes reguladores. ✓ Imagen negativa por mal servicio. ✓ Pérdida de información que de acuerdo a la clasificación se considera Altamente Confidencial. ✓ Estafa importante y exitosa, sistemas de información Core totalmente comprometidos y/o vulnerados. ✓ Pérdida de vidas humanas.	Reporte directamente a Gestión Franca
Alta	✓ Control débil y no mitiga la probabilidad o la consecuencia convenientemente. ✓ Interrupción de las actividades.	Reporte directamente a Gestión Franca

Este documento es propiedad de Comercializadora de Vehículos Importados S.A. es para consulta y uso de sus procesos.

Nivel de Criticidad	Criterio	Tratamiento
	✓ Observaciones por desacato de las normas establecidas por los agentes reguladores que generen un plan de acción a corto plazo. ✓ Afectación de la imagen por el servicio ineficaz o inoportuno. ✓ Incongruencia de la información ocasionando retrasos en las labores de las áreas, respuesta a los agentes reguladores y a los aprendices.	
Media	✓ Evidencia de algunos controles, pero no son los suficientes. ✓ Reactivación de operaciones y crecimiento de la carga operativa entre 24 a 36 horas. ✓ Acceso fraudulento a los sistemas de información a nivel local.	Reporte directamente a Gestión Franca
Baja	✓ Se cuenta con un control actual, sin embargo, este es susceptible a mejoras. ✓ Interrupción de las actividades focalizadas entre 8 y 12 horas. ✓ Tentativas de acceso no autorizado a los sistemas de información focalizados.	Reporte directamente a Gestión Franca – Análisis y Control Interno
Insignificante	✓ No hay interrupción de las operaciones. ✓ No genera multas monetarias y/o administrativas. ✓ No perturba las relaciones con los clientes. ✓ No afecta la congruencia de la información. ✓ No existe amenaza de seguridad ante la información.	Análisis y Control Interno

Investigación/ Respuesta: de acuerdo a la clasificación y al tratamiento se realiza reporte en matriz de incidentes, dejando trazabilidad del análisis y tratamiento del incidente.

Notificación/Reporte/Divulgación: Una vez tratado el incidente se realiza divulgación.

Firmado Fisicamente

Represente Legal
19 de Agosto de 2025

Este documento es propiedad de Comercializadora de Vehículos Importados S.A. es para consulta y uso de sus procesos.