CONTROL DE CAMBIOS		
VERSIÓN VIGENTE	**FECHA DE ACTUALIZACIÓN**	**DESCRIPCIÓN CAMBIO**
00	Abril de 2022	Versión Inicial
01	Mayo de 2023	Inclusión de políticas alineadas con el proveedor de servicios tecnológicos
02	Agosto de 2025	Complemento a las políticas
		Estrategias de prevención, respuesta a incidentes y controles específicos para incidentes de seguridad. incumplimientos relacionados con la seguridad de la información Respaldo de información

Aprobó:			
Bernardo Tobón **Representante legal**			
Versión: 02	**Fecha: 12/08/2025**	**Área: SGI**	

Para CARCO S.A, la Información es uno de los activos más importantes y valiosos en los procesos, por tanto, es necesario mantenerla protegida ante diferentes amenazas a las que pueda estar expuesta.

Con el establecimiento de la presente política, se busca minimizar o eliminar los riesgos que pueden afectar la información em cualquiera de las formas que está representada, teniendo como finalidad mantener en todo momento su integridad, disponibilidad y confidencialidad.

ALCANCE

La política es de obligatorio conocimiento y aplicación de todo el personal de CARCO S.A, incluyendo el personal de las empresas contratistas independiente de su labor.

OBJETIVO

- Informar y comprender la importancia de proteger y preservar la información.
- Establecer las directrices para el correcto tratamiento de la información.
- Garantizar la integridad disponibilidad y confidencialidad de la información propiedad de CARCO S.A.

GLOSARIO

ACTIVO: cualquier cosa que tiene valor para la organización.

ACTIVO DE INFORMACIÓN: cualquier cosa que tiene valor para la organización y que contiene información.

CONFIDENCIALIDAD: Propiedad que determina que la información no esté disponible ni sea revelada a individuos, entidades o procesos no autorizados.

DISPONIBILIDAD: propiedad de que la información sea accesible y utilizable por solicitud de una entidad autorizada.

ERP: (Customer Relationship Management) Planificación de Recursos Empresariales, utilizado para centralizar y administrar la información y los procesos de los diferentes departamentos (Ejemplo: Ofima).

FORMATEAR: En informática, borrado o eliminación de la información de un dispositivo, dejándolo preparado para un nuevo uso.

GESTION FRANCA: Proveedor y administrador de servicios tecnológicos.

INTEGRIDAD: propiedad de salvaguardar la exactitud y estado completo de los activos.

IT (Information Technology): Tecnologías de la información y la comunicación.

LA ORGANIZACIÓN: Hace referencia a Carco S.A.

PROPIEDAD DE LOS ACTIVOS: Toda la información y los activos asociados con los servicios de procesamiento de información deben ser "propiedad" de una parte designada de la organización.

PROPIETARIO: Identifica a un individuo o una entidad que tiene responsabilidad aprobada de la dirección por el control de la producción, el desarrollo, el mantenimiento, el uso y la seguridad de los activos. El término "propietario" no implica que la persona tenga realmente los derechos de propiedad de los activos.

SEGURIDAD DE LA INFORMACIÓN: Preservación de la confidencialidad, la integridad y la disponibilidad de la información.

SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN SGSI: Tiene como fin establecer, implementar, operar, hacer seguimiento, revisar, mantener y mejorar la seguridad de la información.

RESPONSABILIDAD

Gerente general de CARCO S.A: revisará y aprobará la política establecida, de igual forma garantizará los recursos necesarios para su implementación y cumplimiento.

Recursos Humanos: Responsable de divulgar la política de seguridad de la información.

Gerentes: responsables de garantizar que las personas a su cargo cumplen con los requerimientos establecidos para proteger la información.

Encargado del sistema de seguridad de información, líder Kaisen: deben proporcionar capacitación, soporte y asegurarse del cumplimiento de esta política.

Colaboradores de CARCO S.A: Responsables de velar por el cumplimiento de la política de seguridad de la información.

DIRECTRICES DE LA POLÍTICA

POLITICA DE PROPIEDAD DE LA INFORMACIÓN

- Carco S.A es propietario de toda la información que se genere o se adquiera y que esté almacenada en computadores, dispositivos tecnológicos o archivos impresos. La información propiedad de Carco S.A almacenada física o electrónicamente en computadores o dispositivos propios, alquilados o de terceros seguirá siendo propiedad únicamente de Carco S.A o de las empresas a las cuales se les prestan o se adquieren servicios (en adelante Empresas) de acuerdo a las leyes de derechos de autor y protección de datos vigentes.

  Toda la información que se maneja en los diferentes medios se considera de carácter confidencial, por tanto, solo puede ser accedida por personal autorizado en cada área

de trabajo limitando su acceso y haciendo responsable a cada propietario por la información que genera o accede en cumplimiento de sus funciones.

Los empleados o terceros con accesos a esta información deben reportar de inmediato al jefe inmediato o al área IT el robo, pérdida o divulgación no autorizada de información de propiedad de Carco S.A o de las Empresas.

Los empleados o terceros pueden acceder, usar o compartir la información de Carco S.A o de las Empresas, solo cuando se encuentren debidamente autorizados y sea necesario para cumplir con las funciones asignadas a su trabajo.

Los empleados son responsables de ejercer un buen juicio sobre el uso personal de los computadores y dispositivos electrónicos suministrados por Carco S.A.

Por razones de seguridad, propósitos de supervisión y mantenimiento de la red, personas autorizadas por Carco S.A podrán monitorear los equipos, sistemas y tráfico de la red en cualquier momento.

Carco S.A se reserva el derecho a auditar las redes, dispositivos y sistemas de manera periódica para asegurar el cumplimiento de esta política, bien sea por personal interno autorizado o por el proveedor de servicios tecnológicos.

La autorización para el uso de dispositivos de la empresa a favor de los empleados o terceros conlleva la aceptación de la obligación de confidencialidad sobre la información a la que puedan tener acceso, la cual es de naturaleza reservada y constituye un activo intangible de vital importancia para Carco S.A, por lo que los empleados o terceros que accedan a ella se obligan a poner todas sus capacidades personales y profesionales para prestar una protección efectiva. El incumplimiento de dicha obligación constituye según el numeral 6° del literal a) del artículo 62 del C.S.T, una justa causa para dar por terminado de manera unilateral el contrato de trabajo.

Para efectos de lo anterior, constituye información reservada de Carco S.A sometida a especial protección, toda la información relacionada con la operación de Carco S.A y sus clientes, en especial la relacionada con los procesos y procedimientos a los que tenga acceso en desarrollo de su cargo o su posición en la empresa. Adicionalmente se considera información confidencial o bajo reserva, sin limitarse a este listado, la información que a continuación se relaciona:

- Procesos.
- Cifras.
- 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.
- Software (programas, bases de datos, sistemas operativos, interfaces de diagnóstico entre otros.)

Quien tenga acceso a la información se compromete a suscribir nuevas cláusulas de confidencialidad o a modificar las existentes, en la medida en que Carco S.A 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.

El receptor de la información asume la obligación de no usar, explotar, divulgar, revelar, exhibir o adquirir sin autorización de Carco S.A, en beneficio propio o de un tercero, la información o documentación reservada a la que tenga acceso. En consecuencia, reconoce y acepta que Carco 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 Carco S.A. 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 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.

El incumplimiento por parte de los trabajadores de Carco S.A de cualquiera de las obligaciones de confidencialidad mencionadas, se considerará como una falta grave que dará lugar a la terminación inmediata y con justa causa del contrato de trabajo existente con Carco S.A, de acuerdo con lo establecido en el contrato de trabajo y/o el código sustantivo del trabajo (C.S.T).

POLÍTICA DE SEGREGACIÓN DE FUNCIONES

Toda tarea en la cual los empleados tengan 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 Carco S.A.

En concordancia:
Todos los sistemas de disponibilidad crítica o media de Carco S.A, deben implementar las reglas de acceso de tal forma que haya segregación de tareas entre quien administre, opere, mantenga, audite y en general, tenga la posibilidad de acceder a los sistemas de información, así como entre quien otorga el privilegio y quien lo utiliza.

POLÍTICA DE USO DE LAS REDES DE DATOS

Es responsabilidad de Carco S.A a través del área encargada de IT o su proveedor de tecnología externo velar por el buen uso y la manipulación de las redes de datos, para esto debe tener en cuenta lo siguiente:

La manipulación de los puntos de red, puntos de Switches, panel de cableado, acceso lógico y físico a los equipos especializados de cómputo deberá ser exclusivo y administrado por el encargado del área de IT. Para el caso especial de terceros y proveedores de servicios especializados estos deberán estar autorizados y supervisados por el jefe de área de IT de Carco S.A.

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

Todos los accesos desde y hacia redes externas 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, desprender marcaciones de tomas, puertas o productos, golpear o dañar tubos o canaletas.

La solicitud de creación, modificación, desactivación o eliminación de accesos a la red de Carco S.A, se debe hacer a través de la mesa de ayuda de nuestro proveedor de servicios tecnológicos utilizando los formatos de creación, modificación, desactivación, eliminación, o el formato de solicitudes especiales según el requerimiento.

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

POLÍTICA SOBRE LA ASIGNACIÓN Y USO DE USUARIOS Y CONTRASEÑAS

La asignación de usuarios y contraseñas se realiza de acuerdo con lo establecido por el proveedor de servicios tecnológicos.

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 de cada 30 días.

Las contraseñas de los sistemas deben cumplir con la directiva de complejidad de contraseñas la cual establece 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.
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)
Caracteres no alfanuméricos (por ejemplo: $, #, %, *)

Estos requisitos de complejidad se exigen al cambiar o crear contraseñas de red.

El usuario no debe conservar registros de las contraseñas en papel o en archivos digitales.

- No se pueden utilizar contraseñas estáticas para el acceso a scripts o aplicaciones.
- No se deben guardar contraseñas en los navegadores.
- No se deben incluir contraseñas en procedimientos automáticos de conexión.
- No asignar claves que ya hayan sido utilizadas.

Las contraseñas asignadas a un nuevo usuario no deberán entregarse por medio de WhatsApp ni por medio del ticket solucionado. Deberán comunicarse directamente al funcionario por medio telefónico.

El usuario deberá cambiar la contraseña en el primer inicio

Las llaves/claves de administración de los directorios activos, accesos a los dispositivos de comunicaciones y de todos los servicios de informática y tecnología cubiertos por esta política deben ser protegidas para evitar su divulgación no autorizada y su posible uso fraudulento posterior.

Las llaves o claves de administración de los servicios adquiridos al proveedor tecnológico se encuentran en medio lógico en un archivo protegido por contraseña y en medio físico en las cajas de seguridad de sus Datacenter.

POLÍTICA DE ACCESO Y USO DE LAS APLICACIONES

El ingreso a las aplicaciones debe ser con el usuario y clave asignados.

No está permitido la suplantación de usuarios para el ingreso a las aplicaciones.

La información ingresada a las aplicaciones debe ser la real.

No se debe acceder a los aplicativos y/o herramientas utilizadas en la organización desde lugares públicos de internet.

El acceso al ERP (Ofima) de Carco S.A se encuentra limitado por roles, los cuales son definidos por el responsable del módulo o jefe de área junto con las áreas de Contabilidad, y Gestión IT.

El acceso a las bases de datos desde las aplicaciones o cualquier ambiente que requiera consultar la información de las mismas debe realizarse de acuerdo a la política de seguridad de bases de datos.

POLÍTICA DE USO DE ACTIVOS FUERA DE LAS INSTALACIONES

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 encargada.

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

ACCESO A LAS REDES WIFI

Las redes Wifi para clientes o visitantes se debe realizar mediante accesos independientes y por redes lógicas independientes a las redes corporativas

No está permitido:

- Transmisión de contenido fraudulento, difamatorio, obsceno, ofensivo o de vandalismo, insultante o acosador, sea este material o mensajes.
- 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.
- Obtener acceso no autorizado a equipos, sistemas o programas tanto al interior de la red como fuera de ella.
- No 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, por tanto, tampoco puede ser usada con fines de lucro, actividades comerciales o ilegales, por ejemplo, hacking, ser utilizada para crear y/o subir virus informáticos o malware en la red.
- No se podrá 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.

POLÍTICA DE USO DE EQUIPOS DE CÓMPUTO Y DISPOSITIVOS MÓVILES

Todos los equipos conectados a la red del proveedor de servicios deberán hacerlo utilizando una cuenta valida registrada en el Directorio Activo.

Ningún usuario debe tener permisos de administrador sobre los computadores de la compañía, de acuerdo con la directiva implementada por el área de Gestión IT, esto con el propósito de proteger los equipos contra virus y evitar la instalación de software no licenciado o autorizado.

No está permitido el uso de computadores personales o ajenos al asignado por Carco S.A para el desempeño de sus funciones.

No estará permitido la configuración del correo corporativo en equipos personales que no cuenten con la autorización pertinente del jefe de área; en caso contar con este permiso el dispositivo móvil deberá contar con control de acceso con contraseña, antimalware y cifrar la información contenida. Este debe ser solicitado por el formato de solicitudes especiales con las debidas autorizaciones.

No está permitido retirar computadores o sus accesorios del área asignada o de la organización.

No está permitido comer o ingerir bebidas mientras se esté usando el computador.

No está permitido pegar calcomanías o cualquier tipo de adornos en los equipos.

No está permitido instalar cualquier tipo de software en los computadores de la Organización, esta actividad es responsabilidad del área de Gestión IT.

Los equipos deberán protegerse de descargas eléctricas, conectándolos siempre a la corriente regulada y deberán estar alejados de fuentes de calor.

No se permite la extracción o copia de archivos en medios extraíbles, tales como memorias USB, discos duros externos, CDS, DVDS, teléfonos celulares etc.

Los equipos de escritorio y portátiles que se encuentran asignados a los empleados Carco S.A tendrán restricción de acceso a las unidades de CD/DVD y puertos USB, de igual forma el acceso a internet estará restringido de acuerdo al perfil de usuario previamente solicitado. mediante el formato de creación de usuario.

Se debe permitir la adquisición de las herramientas de hardware y software que permitan realizar los controles necesarios y el cumpliendo de la política, este debe cumplir con la legalidad de licenciamiento y la autorización de la instalación por parte del administrador Gestión Franca o el área de sistemas de CARCO S.A

POLÍTICA DE MANTENIMIENTO DE EQUIPOS DE CÓMPUTO

Al área de Gestión IT le corresponde la realización del mantenimiento preventivo y correctivo de los equipos de cómputo de Carco S.A.

Los usuarios responsables de los equipos de cómputo salvo expresa autorización del área de Gestión IT no podrán realizar ningún tipo de mantenimiento preventivo, correctivo, ajustes, cambios en la configuración, instalación de software o Hardware y cualquier otra actividad que vaya en contra la integridad física de los equipos, la red de datos, la confidencialidad y disponibilidad de la información.

El área de Gestión IT no está en la obligación de realizar mantenimiento preventivo y/o correctivo a equipos instalados por terceros para proveer servicios de comunicaciones, datos o cualquier otro servicio contratado.

POLÍTICA DE CONTROLES DE ACCESO

Esta Política se aplica a todas las formas de acceso a las instalaciones de la organización y para aquellas áreas definidas como "áreas críticas", debido a su relación con datos confidenciales y de interés para el negocio.

El acceso de los colaboradores a las instalaciones se controla por medio de software de control de acceso biométrico, el cual es administrado por el área IT y Talento Humano, adicional a esto, es requerido el uso del carnet de identificación en todo momento dentro de las instalaciones de la compañía.

El acceso de todo el personal (incluyendo contratistas y visitantes) a zonas restringidas tales como Datacenter, Centros de Cableado, archivo y almacén entre otros, está restringido y sólo pueden acceder a través de la autorización correspondiente por un funcionario autorizado, adicionalmente, estas locaciones deben permanecer cerradas.

Para preservar la seguridad de los equipos de los servidores y equipos de comunicaciones y en general todos los dispositivos y centros de cableado, los armarios (Racks) deben permanecer cerrados.

Se utilizan cámaras de video (CCTV) y control de acceso biométrico para supervisar el acceso físico de personas a áreas críticas o que resguardan información confidencial.

POLÍTICA DE SEGURIDAD FLUIDO ELÉCTRICO

La conexión eléctrica de todos los equipos de cómputo se debe realizar en circuitos regulados.

En el Datacenter y/o Centro de cableado se debe contar con UPS de respaldo que garantice la continuidad de los servicios de tecnología por un tiempo prudente para el cierre de aplicaciones y apagado correcto de los equipos en la eventualidad de ausencia de fluido eléctrico.

El mantenimiento preventivo de la UPS de Carco S.A se debe realizar mínimo una vez al año.

POLÍTICA DE TRABAJO EN CASA

Trabado en casa significa que los equipos de información y comunicación se utilizan para permitir que los empleados realicen su trabajo fuera de la organización. El trabajo en casa incluye el uso de teléfonos móviles fuera de las instalaciones de la organización.
El acceso remoto de usuarios que se encuentran fuera de las instalaciones de la organización es autorizado por el jefe de área.

El acceso a los recursos de tecnología disponibles se debe realizar únicamente desde computadores y equipos de la compañía. No está permitido el uso de computadores ni dispositivos personales salvo autorización del jefe de área.

El acceso a los recursos de tecnología y al ERP de Carco S.A se debe realizar únicamente garantizando la conexión a través de VPN.

Las áreas de trabajo remoto que autorice la organización fuera de sus instalaciones deben cumplir con todas las políticas y controles del sistema de seguridad definido por Carco S.A.

El área de IT y el proveedor de servicios tecnológicos son responsables de proporcionar el servicio de acceso remoto y las normas de acceso a los recursos informáticos disponibles.

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 al área de IT o a través de la mesa de ayuda del proveedor de servicios tecnológicos cualquier anormalidad que llegue a presentarse con los equipos tecnológicos que tenga a disposición fuera de la compañía.

POLÍTICA DE ESCRITORIO DESPEJADO Y PANTALLA DESPEJADA

Los empleados de la organización están obligados a utilizar protectores de pantallas protegidos con contraseña o a dejar cerradas todas las sesiones cuando abandonan su puesto de trabajo. Cuando regresan, deben introducir nuevamente la contraseña del usuario para acceder de nuevo a la información.

En los equipos que técnicamente sea posible se activan automáticamente protectores de pantalla con clave como política del directorio activo. Este se debe disparar en el momento en que transcurran entre tres y cinco minutos desde la última vez que se manipuló él computador.

Para mantener el escritorio despejado se ocultará mediante la activación de una imagen corporativa en todos los computadores de los usuarios activos, la cual estará sobrepuesta en el escritorio de cada computador para que los archivos o carpetas no queden expuestos.

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 como también la almacenada en las particiones del servidor designada.

Las impresoras de uso general deben estar protegidas con PIN de seguridad. En el caso de las impresoras asignadas a usuarios específicos el empleado debe recoger las impresiones antes de abandonar la jornada laboral y revisar que no queden documentos en cola de impresión o documentos impresos.

En el caso que se destine papel para 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.

POLÍTICA DE PROTECCIÓN CONTRA CÓDIGOS MALICIOSOS

Se debe mantener instalado en los equipos de la organización software antivirus los cuales serán actualizados mensualmente por el personal de Gestión IT o el proveedor de servicios tecnológicos.

Evitar o 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, el área Infraestructura IT 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 está permitido:

La desinstalación y/o desactivación de software y herramientas de seguridad avaladas por Carco S.A o el proveedor de servicios tecnológicos.

Las únicas personas autorizadas para desactivar de manera temporal el sistema de antivirus, en cualquier componente de la infraestructura tecnológica de La Compañía serán: Proveedor de servicios tecnológicos.

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.

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

POLÍTICA PARA INTERCAMBIO DE INFORMACIÓN

No está permitido entregar información a empresas o clientes 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 colocar clave a los archivos adjuntos y está debe ser informada al destinatario por un medio diferente al correo electrónico.

Los empleados de Carco S.A están obligados a cumplir los acuerdos de confidencialidad y por lo tanto serán responsables de la entrega de información no autorizada.

En caso de ser necesario el envío y la recepción de información confidencial con los terceros contratados se debe proteger con mecanismos de cifrado fuerte.
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 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.

POLÍTICA DE CLASIFICACIÓN DE LA INFORMACIÓN

El objetivo de esta política es establecer un sistema claro y uniforme para clasificar la información manejada por la empresa, con el fin de protegerla de accesos no autorizados, modificaciones indebidas, pérdidas o divulgaciones no deseadas, de acuerdo con su nivel de sensibilidad, valor y criticidad para la organización.

Esta política aplica a toda la información generada, recibida, almacenada o transmitida por la empresa, independientemente del formato (físico o digital), medio de almacenamiento o canal de comunicación utilizado, y a todos los colaboradores, contratistas, proveedores y terceros con acceso a dicha información.

Principios Generales

- Toda información debe ser protegida de acuerdo con su nivel de sensibilidad.
- La clasificación debe realizarse en el momento de la creación de la información y puede ser revisada y modificada si las circunstancias cambian.
- El nivel de protección aplicado debe estar alineado con la clasificación asignada.

Niveles de Clasificación

La información se clasificará en los siguientes niveles:

- **Confidencial**

Información crítica cuyo acceso no autorizado podría causar daños graves a la empresa, sus clientes o socios.

Ejemplos: Datos financieros no publicados, información de clientes, secretos comerciales, estrategias corporativas.

Acceso: Restringido al personal autorizado específicamente.

Protección: Cifrado obligatorio, almacenamiento seguro, acceso limitado y registrado.

- **Protegido**

Información que no es pública, pero cuyo acceso no autorizado tendría un impacto moderado.

Ejemplos: Procedimientos internos, reportes de desempeño, políticas internas.

Acceso: Personal interno autorizado.

Protección: Acceso controlado por credenciales, no debe compartirse con terceros sin aprobación.

- **Pública**

Información que puede ser divulgada libremente sin generar daño a la organización.

Ejemplos: Publicaciones oficiales, contenido del sitio web, comunicados de prensa.

Acceso: Libre.

Protección: No requiere medidas especiales, pero debe garantizarse su integridad.

Responsabilidades

- **Todos los empleados** son responsables de clasificar correctamente la información que crean o manejan.
- **Los líderes de área** deben supervisar que la información de su departamento esté adecuadamente clasificada.
- **Los responsables de Seguridad de la Información** deben proporcionar capacitación, soporte y asegurarse del cumplimiento de esta política.

POLÍTICA SOBRE EL USO DE INTERNET

El acceso a internet se encuentra restringido por perfiles asignados a cada usuario de acuerdo con lo autorizado por los jefes de cada área, estos perfiles están diseñados para permitir accesos a diferentes categorías de páginas y están definidos en el formato de Creación Modificación y Eliminación de Usuarios.

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 empleados de la empresa 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 la información de internet redactada, transmitida y/o recibida por sus sistemas informáticos se considera propiedad de Carco S.A y se reconoce como parte de sus datos oficiales; por lo tanto, podrá revelarse por exigencias legales o a terceros autorizados.

El equipamiento, los servicios y la tecnología utilizados para acceder a internet pertenecen a Carco S.A y su proveedor de servicios tecnológicos, por tanto, se reservan se reservan 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 de área de IT o el proveedor de servicios tecnológicos si se consideran perjudiciales y/o improductivos para el negocio:

El uso inaceptable de internet por parte de los empleados de Carco S.A incluye sin límite:

Acceso a sitios que contengan material obsceno, agresivo, pornográfico, ilícito, violento o ilegal en modo alguno.

El envío o la publicación de mensajes o imágenes ofensivas, discriminatorias o amenazantes por internet o a través del servicio de correo electrónico de Carco S.A.

El uso de los computadores para cometer cualquier tipo de fraude y/o piratear software, películas, música o cualquier archivo electrónico con derechos de autor.

La divulgación de material confidencial, secretos comerciales o información confidencial fuera de la organización.

El acceso mediante piratería a páginas web no autorizadas.

El envío o la publicación de información difamatoria sobre la empresa, sus productos o servicios, trabajadores y/o clientes.

La introducción de software malicioso en la red de la empresa y/o la realización de actividades que pongan en peligro la seguridad de los sistemas de comunicación electrónica de la organización.

El envío o la publicación de cartas en cadena, solicitudes o anuncios no relacionados con el objeto o la actividad del negocio.

La presentación de opiniones personales como si representaran las de la organización.

El acceso y participación en redes sociales utilizando los recursos y dispositivos de la compañía, a menos que esto se encuentre dentro de las funciones del empleado.

Crear o participar en blogs o foros mientras se utilizan los equipos y recursos de la compañía, a menos que esto se encuentre dentro de las funciones del empleado.

Divulgar o revelar a través de blogs o foros información confidencial, secretos comerciales o cualquier otra información cubierta por esta política.

Los empleados no deben atribuir declaraciones personales, opiniones o creencias a nombre de la empresa cuando participen en blogs, foros o redes sociales.

Utilizar cuentas de correo personal (Gmail, Hotmail, Yahoo, etc.) para fines laborales en representación de la empresa o para trasferir cualquier tipo de información a través de estas.

Si un empleado no está seguro de qué constituye un uso aceptable de internet, deberá consultar a su jefe y pedirle más información y asesoramiento al respecto.

POLÍTICA PARA EL RESPALDO DE LA INFORMACIÓN

Toda la información que se encuentra alojada en los servidores o equipos críticos se le debe realizar copia de respaldo periódicamente de acuerdo con los procedimientos establecidos, con el fin de contar con la información en caso de ser requerida por alguna eventualidad.

Procedimiento de respaldo de información

POLÍTICA DE SOFTWARE INSTALADO

El software adquirido por la organización sea por compra, donación o cesión es propiedad de Carco S.A y mantendrá los derechos que la ley de propiedad intelectual le confiera.

En los equipos de cómputo, de telecomunicaciones y en dispositivos basados en sistemas de cómputo, únicamente se permitirá la instalación de software con licenciamiento apropiado y de acorde a la propiedad intelectual.

El área de Gestión IT de Carco S.A o el proveedor de servicios tecnológico es responsable de brindar asesoría y supervisión para la instalación de software informático, así mismo para el software de telecomunicaciones.

No está permitida la instalación de software que desde el punto de vista del área de Gestión IT pudiera poner en riesgo los recursos de la organización.

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 (antivirus, privilegios de acceso, y otros que se apliquen).

El área de Gestión IT administrará los diferentes tipos de licencias de software y vigila su vigencia en concordancia con la política de la organización.

Cualquier software que requiera ser instalado para trabajar deberá ser evaluado por la Gerencia y/o quien este delegue.

Corresponde al área de Gestión IT y el proveedor de servicios tecnológicos, apoyar los procesos de auditoría de software requeridas por entidades del gobierno o empresas que lo soliciten de acuerdo a la propiedad del software.

POLÍTICA DE BORRADO SEGURO

Todos los dispositivos de almacenamiento de información utilizados para la operación de Carco S.A incluyendo papel, que ya no se encuentren en uso o que por razones del negocio ya no deban ser utilizados, deben ser destruidos adecuadamente con el fin de evitar fugas de información confidencial.

El material impreso que ya no se requiera para ningún fin en la empresa y a menos que por razones del negocio deba ser archivado, debe ser destruido por método manual garantizando que no se pueda recuperar. De ninguna forma estos documentos deben ser depositados en canecas o bolsas de basura sin destruirlos previamente.

Los métodos de borrado son:

Borrado Físico: Destrucción Física de la información mediante la trituración de los documentos de forma manual.

Borrado Lógico: La eliminación de la información almacenada en los diferentes dispositivos tecnológicos se debe realizar dependiendo el rol del funcionario, para los empleados en general se deben realizar un "formateo del equipo o dispositivo de almacenamiento (Computadores, Discos duros, tableta, teléfonos etc.), en cambio sí es un jefe de área o un colaborar que manipule información confidencial de Carco S.A, se deben 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 cual se deberán realizar por lo menos tres ciclos de sobre escritura de datos.

Antes de ejecutar el borrado seguro de la información lógica se debe garantizar el backup de la información.

POLÍTICA DE GESTIÓN DE INCIDENTES DE SEGURIDAD

Un incidente de Seguridad Informática está definido como un evento que atente contra la Confidencialidad, Integridad y/o Disponibilidad de la información y los recursos tecnológicos de la organización.

Existen varias categorías de incidentes de seguridad 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.

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:
Comprende la introducción de códigos maliciosos en la infraestructura tecnológica de la organización.

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

Escaneos, pruebas o intentos de obtención de información de la red o de un servidor en particular:

Esta categoría los eventos que buscan obtener información de la infraestructura tecnológica de la Entidad.
Comprende:

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

Mal uso de los recursos tecnológicos:
Son eventos que atentan contra los recursos tecnológicos por el mal uso.

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 Entidad.
Violación de las Políticas, Normas y Procedimientos de Seguridad Informática reglamentadas.

Es deber de los usuarios reportar un incidente de seguridad tan pronto se detecte o sospeche de ellos.

Documentos relacionados:
ESTRATEGIAS DE PREVENCIÓN, RESPUESTA A INCIDENTES Y CONTROLES ESPECÍFICOS PARA INCIDENTES DE SEGURIDAD

INCUMPLIMIENTOS RELACIONADOS CON LA SEGURIDAD DE LA INFORMACIÓN

Con el fin de proteger los activos de información de Carco S.A, todos los colaboradores están obligados a cumplir con las políticas, normas y procedimientos establecidos en materia de seguridad de la información. Cualquier acción u omisión que vulnere estas disposiciones será considerada una falta, la cual podrá clasificarse como leve o grave dependiendo de su naturaleza y del impacto que genere en la confidencialidad, integridad o disponibilidad de la información. Entre estas faltas se incluyen, pero no se limitan a: compartir contraseñas, utilizar dispositivos no autorizados, divulgar información sensible sin autorización, no reportar incidentes de seguridad, o instalar software sin aprobación. El incumplimiento de estas obligaciones podrá dar lugar a medidas disciplinarias conforme a la normativa interna vigente, sin perjuicio de las acciones legales que pudieran corresponder.

- **Faltas Leves (Seguridad de la Información)**

Estas son acciones u omisiones que, aunque no generen consecuencias inmediatas o graves, van en contra de las buenas prácticas de seguridad de la información.

1. No bloquear el equipo al ausentarse del puesto de trabajo.
2. Uso de contraseñas débiles o fáciles de adivinar.
3. Compartir dispositivos electrónicos sin supervisión o sin autorización previa.
4. Dejar documentos impresos con información interna sin resguardo.
5. No tomar las capacitaciones o inducciones de ciberseguridad, estas son obligatorios.
6. Uso ocasional de correos personales desde el equipo corporativo.
7. Utilización de la red corporativa para navegar en sitios no relacionados con el trabajo.
8. No reportar incidentes menores de seguridad (por ejemplo, correos sospechosos no abiertos).
9. No cambiar las contraseñas periódicamente.

- **Faltas Graves (Seguridad de la Información)**

Estas acciones pueden comprometer directamente la seguridad de los sistemas, los datos sensibles o la reputación de la empresa.

1. Compartir credenciales de acceso con otras personas (internas o externas).
2. Acceder o intentar acceder a sistemas o información sin autorización.
3. Instalar software no autorizado en dispositivos corporativos.
4. Enviar información confidencial o sensible a través de medios no seguros.
5. Pérdida o robo de dispositivos corporativos sin reporte inmediato.
6. Modificar o deshabilitar medidas de seguridad en el equipo (antivirus, firewall, etc.).
7. Eliminar o cambiar información sin autorización.
8. Compartir información interna en redes sociales o medios públicos.
9. Negarse a colaborar en una investigación relacionada con un incidente de seguridad.
10. Reincidencia en faltas leves relacionadas con seguridad.

Nota: Todos los términos y condiciones afirmados en este documento reflejan un acuerdo de todas las partes y debe gobernarse e interpretarse de acuerdo con las directivas y procedimientos mencionados anteriormente.

La violación de cualquiera de estas normas podrá ser causa de sanciones al usuario contempladas en el reglamento interno de trabajo o código sustantivo del trabajo.

Elaboró:	Revisó	Aprobó:
ALFREDO LIZARAZO. **Analista de sistemas**	**Jennifer Cortés** **Jefe de planeación y desarrollo**	**BERNARDO TOBÓN** **Representante Legal**