1. **OBJETIVO**
   Implementar normas, políticas y protocolos relacionados con la seguridad informática de AERCARGO SERVICES S.A.S

2. **ALCANCE**
   Aplica a todos los procesos de la empresa.

3. **DEFINICIONES**

- **Cuentas de Servicio informáticos o cuentas de usuario:** Registro electrónico individual para un usuario de los servicios informáticos institucionales los cuales cuentan con los siguientes datos, un nombre (ID usuario) una contraseña (pasword).
- **Infraestructura para el procesamiento de datos:** Es un conjunto de recursos tecnológicos y de infraestructura física que se combina de forma integral para tratar de manera adecuada la información que los usuarios requieren para el desempeño de funciones.
- **Infraestructura tecnológica:** La infraestructura tecnológica se encuentra integrada por un conjunto de elementos como lo es el hardware (servidores, puestos de trabajo, redes, enlaces de telecomunicaciones, etc) software (sistemas operativos, bases de datos, lenguajes de programación, herramientas de administración) servicios (soporte técnico, seguros, comunicaciones).
- **Licencia de Software:** Es un contrato donde se establecen normas y clausulas que rigen el uso de un determinado programa por parte de usuarios o licenciatarios. Principalmente se estipulan los alcances de uso, instalación, reproducción y número de copias de estos productos.
- **Recursos tecnológicos:** Elementos de tecnología que pueden ser hardware y/o software, tales como equipos de computo, servidores, impresoras, teléfonos, fax, programas y aplicativos de software, dispositivos USB, entre otros.
- **Sistema de información:** Conjunto independiente de recursos de información organizados para recopilación, procesamiento, mantenimiento, transmisión y difusión de datos.

4. **RESPONSABLE**
   Gerencia, Dpto. de tecnología, Administrativo y Financiero

5. DESARROLLO

POLITICA DE SEGURIDAD DE LA INFORMACION

AERCARGO SERVICES S.A.S se compromete a administrar los riesgos de seguridad de la información para generar, implementar y monitorear los controles que permitan garantizar, mantener la confidencialidad, integridad y disponibilidad de sus activos de información en cumplimiento de los requisitos aplicables. De igual manera, promueve una cultura en seguridad para evitar incidentes que afecten a la mejora continua del Sistema de Gestión de Seguridad de la Información.

Esta política abarca todos los procesos y procedimientos de AERCARGO SERVICES S.A.Sque tenga presencial o desarrolle su acompañamiento a través de la recolección, procesamiento, almacenamiento, recuperación, intercambio, transferencia y consulta de información, en el desarrollo de su misión. Es responsabilidad de cada usuario interno o externo que utilice los recursos de cómputo de AERCARGO SERVICES S.A.S en forma, profesional, ética y legal.

Para asegurar la dirección estratégica del AERCARGO SERVICES S.A.S y la implementación de la presente política de seguridad y manejo de la información, AERCARGO SERVICES S.A.S, establece las siguientes directrices:

- ✓ Proteger los activos de información, preservando su integridad, confidencialidad y disponibilidad.
- ✓ Gestionar la integridad de la información que ha sido solicitada, creada, procesada resguardada por los procesos de la organización.
- ✓ Cumplir las disposiciones legales, regulatorias y contractuales relacionadas con la seguridad de la información.
- ✓ Garantizar la continuidad del negocio frente a la seguridad y privacidad de la información a través de las plataformas tecnológicas.
- ✓ Fortalecer la cultura de seguridad y privacidad de la información en los funcionarios, personal interno y externo que manipule los recursos de la organización
- ✓ Establecer los mecanismos de monitoreo de la seguridad sobre las vulnerabilidades en la infraestructura tecnológica, los sistemas de información

- ✓ Garantizar la optimización de los recursos tecnológicos para la eficiencia de los procesos de la organización

Para garantizar el cumplimiento de las directrices establecidas anteriormente, la alta dirección pone a disposición recursos humanos, financieros, tecnológicos y de infraestructura, que permitan la ejecución de buenas prácticas descritas en la presente política, como en los documentos de la organización que afecten de manera directa o indirecta la seguridad de la información.
Además, se compromete con mantener actualizada, aprobada y divulgada dicha política, a fin de comunicar a las partes interesadas los mecanismos para proteger el patrimonio informático y garantizar la protección de su información

Nota: La presente política se encuentra aprobada y divulgada

5.1 Política de Recursos Informáticos

Establecer una política que asegure de manera eficiente el control, manejo y asignación de los recursos tecnológicos mediante la entrega, custodia. Por tanto, se describe los siguientes lineamientos:

- ✓ Cumplir con las políticas, normas, procedimientos y estándares referentes a la política de recursos informáticos.
- ✓ Los Recursos informáticos, deben ser operados y utilizados solamente por el personal que tiene el equipo bajo custodia o se encuentre autorizado para ellos.
- ✓ El uso de los recursos informáticos ofrecidos por la empresa, deben ser utilizados únicamente con fines laborales no personales.
- ✓ Notificar al departamento de sistemas sobre cualquier eventualidad que ocurra sobre dichos equipos.
- ✓ No uutilizar el equipo en condiciones de daño parcial detectado.
- ✓ La instalación de hardware o software, la reparación o retiro de cualquier parte o elemento en los computadores de escritorio, computadores portátiles y demás recursos informáticos propiedad de la compañía, solo puede ser realizado por los funcionarios autorizados por el departamento de tecnología. Por ningún motivo los usuarios podrán abrir o desarmar los equipos de cómputo.
- ✓ Ante el requerimiento de cambio de ubicación o puesto de trabajo El jefe de cada dependencia deberá informar los cambios de puestos de trabajo vía mail.
- ✓ El Departamento de sistemas es el único autorizado para realizar movimientos y entrega de recursos informáticos, por lo que está totalmente prohibida la disposición de éstos por parte de los empleados, aún así a este se le haya asignado el recurso.

- ✓ Todos los recursos tecnológicos deben ser apagados al finalizar la jornada laboral. salvo que la Compañía disponga expresamente lo contrario por medio escrito vía mail.
- ✓ Responder por las consecuencias por pérdidas o daños cuando se compruebe negligencia y falta de cuidado.
- ✓ Está prohibido el ingreso a las instalaciones de recursos informáticos que no sean propiedad de la compañía, salvo aquellos que estén relacionados en los acuerdos de conexión a la red por parte de empleados o terceros y sean usados para cumplir el objeto de algún contrato vigente entre el tercero y la compañía. Por ningún motivo se permite el ingreso a las instalaciones de la compañía, recursos informáticos que sean propiedad de los empleados.

5.2 Política de control de acceso

Establecer una política que asegure de manera eficiente el control y manejo de los accesos a redes, aplicativos, sistemas de información y inicios de sesión equipos de cómputo, y de esta forma garantizar la seguridad de la información e impedir el acceso no autorizado a los sistemas.

La política y directrices establecidas para el control de acceso a los recursos informáticos, aplican para todos los usuarios que le sean asignados o tengan manipulación sobre el activo y sistemas de información, se establece las siguientes directrices

- ✓ Cambiar la contraseña provisional inicial en el primer inicio de sesión y colocar contraseña segura según parámetros
- ✓ El préstamo de códigos de identificación y/o cuentas de usuarios y contraseñas para el ingreso a los servicios informáticos está totalmente prohibido.
- ✓ Salvaguardar, no publicar ni compartir los datos asignados para inicio de sesión de las aplicaciones o los servicios informáticos a los cuales se le hayan dado privilegios de acceso.
- ✓ Las contraseñas no deben ser divulgadas a ningún otro usuario, salvo pedido de un empleado de mayor jerarquía, autorizado para tal fin. Se debe informar por correo vía mail a gerencia con conocimiento del dpto. de tecnología.
- ✓ Informar al área de sistemas ante la pérdida o sospecha de divulgación asignados para inicio de sesión de las aplicaciones o recursos informáticos.
- ✓ Todos los usuarios deben, al momento de abandonar su puesto de trabajo, bloquear el acceso al computador de escritorio o portátil.
- ✓ Cada usuario autorizado es responsable por todas las acciones realizadas dentro de los distintos Sistemas de Información, por cualquier otra persona a quien haya divulgado su contraseña. Se debe recordar que el código de

identificación y/o cuenta de usuario es único, al igual que la contraseña de acceso a los servicios informáticos es individual e intransferible.

✓ Bajo ninguna circunstancia, se debe escribir las contraseñas en papel, archivos electrónicos o almacenarlas en medios digitales no encriptados.

✓ Ningún usuario está autorizado para conectar computadores de escritorio, computadores portátiles u otros dispositivos de tecnología que no sean propiedad la compañía, de manera cableada o inalámbrica. Dpto. de tecnología es el único autorizado para gestionar la conexión de dispositivos con previa autorización escrita de gerencia.

✓ Se prohíbe la instalación de cables, derivaciones a través de conectores en "T" o cualquier tipo de derivación de voz o datos por parte de los usuarios. Así mismo, no se permite la instalación de ningún servicio que intervenga directamente sobre el cableado de voz y/o datos corporativos. Sin excepción, las conexiones deberán ser realizadas por el personal autorizado del Dpto. de tecnología.

✓ El Uso de los Servicios es personal e intransferible. La seguridad de las Cuentas asignadas al usuario depende de la privacidad con que él le dé su clave de acceso. Es responsabilidad exclusiva del usuario preservar cuidadosamente su clave de acceso.

✓ El dpto. de tecnología debe procesar y auditar el cambio de contraseñas de acceso a los distintos Sistemas de Información que administran de manera regular, para evitar que ésta sea conocida y utilizada por otras personas

✓ Cuando se solicite por medio escrito cambio de contraseña por incidencia, perdida u olvido, se debe realizar por medio escrito a recursos humanos con conocimiento de gerencia y dpto. de tecnología.

5.3 Política de uso de activos de información

Establecer una política que asegure de manera eficiente el control y manejo de los activos de información mediante a asignación entrega, custodia del recurso. La política y directrices establecidas para el uso activos de información en el presente documento aplican para todos los usuarios que le sean asignados o tengan manipulación sobre el mismo, por tanto, se describe los siguientes lineamientos:

- ✓ Cumplir con las políticas, normas, procedimientos y estándares referentes a la Asignación, custodia y cuidado de la informacion.
- ✓ El empleado entiende y acepta que no es propietario de la información, datos entregados o generada en el tiempo de contrato con la compañía.
- ✓ Se contará con un sistema de información de carpetas compartidas con restricción de permisos, centralizadas en la nube ubicadas en un repositorio de archivos, donde el acceso será controlado y únicamente el

personal identificado y autenticado como titular de esta carpeta podrá acceder.

- ✓ Notificar al departamento de sistemas sobre cualquier eventualidad daño opérdida que ocurra con los activos de información.
- ✓ El usuarios es responsable del buen uso y gestion documental de la infromacion, por esta razon tiene total responsabilidad por pérdidas, divulgación y daños, cuando se compruebe negligencia y falta de cuidado.
- ✓ Son responsabilidad del empleado la información almacenada en cada una de las estaciones de trabajo. En las cuales deben abstenerse de almacenar información no perteneciente a la compañía, el uso y almacenamiento de información personal está totalmente prohibida.
- ✓ El uso de dispositivos de almacenamiento externo (dispositivos móviles, DVD, CD, memorias USB, etc.) son considerados riesgos potenciales que afectan la seguridad de la información de la compañía por tal razón están prohibidos.
- ✓ Esta totalmente prohibido utilizar plataformas web o accesos externos para la transferencia de información.
- ✓ En las excepciones que se presenten autorizadas por gerencia referente al uso de medios extraíbles el usuario entiende que es responsable del uso y manejo de la información almacenada en estos medios.
- ✓ Los empleados de acuerdo con lo establecido en el procedimiento de backup, deberán guardar en la ubicación asignada una copia de la información considerada como elemental para el desarrollo de sus actividades al finalizar la jornada laboral.
- ✓ Los usuarios aceptan y entienden que la información generada debe quedar almacenada en las carpetas asignadas según perfil o cargo para una correcta gestión documental, debe ser únicamente información empresarial, cualquier otro tipo de información que se encuentre allí almacenada, será eliminada, está totalmente prohibido almacenar información personal o que no esté relacionada con la actividad de la empresa.
- ✓ Ante cualquier solicitud por parte de los usuarios de recuperación de un activo de información parcial o completa, se debe notificar y pedir autorización a gerencia, y copiar para su conocimiento a jefe de área y Dpto. de tecnología justificando el porqué del proceso vía mail**.**

5.4. Uso del correo corporativo

Definir el procedimiento mediante el cual se describa el uso correo La política y directrices establecidas en el presente documento aplican para todos los usuarios que le sean asignados o tengan manipulación sobre el correo. por tanto, se describe las siguientes directrices:

✓ Al momento de recibir su cuenta de correo asignada el usuario debe cambiar la contraseña temporal inicial en el primer inicio de sesión y colocar contraseña segura según parámetros establecida en la política control de acceso a recursos.
✓ Utilizar su cuenta corporativa únicamente para fines relacionados con las actividades propias de su trabajo. No se permite la utilización del buzón de correo electrónico para fines comerciales, religiosos, pornográficos, de prostituciones infantiles, políticas, personales y en general diferentes a los que sean relativos al interés de La Compañía
✓ El Trabajador podrá recibir y enviar mensajes desde programas (clientes) de correo que utilicen los protocolos SMTP, POP e IMAP o a través del servidor Microsoft suscrito a la Compañía.
✓ El usuario deberá informar al personal de soporte cualquier advertencia o sospecha de un correo sospechoso que pueda contener virus o publicidad engañosa.
✓ El usuario debe informar a personal de soporte de manera inmediata, de las fallas en el transporte de los mensajes, para que el departamento de tecnología tome las medidas adecuadas para dar continuidad al servicio.
✓ Esta totalmente prohibido enviar, contestar o redirigir mensajes de correo que constituyan cadenas.
✓ No enviar, contestar o redirigir mensajes de correo sin verificar el remitente y su firma corporativa esto con el fin de proteger la cuenta antes spam
✓ No descargar archivos adjuntos ni abrir enlaces sin verificar la autenticidad de la cuenta de correo del remitente, y ante cualquier sospecha el usuario deberá pedir asesoría al área de tecnología para descartar cualquier elemento peligroso que contenga el cuerpo del correo.
✓ No abrir o reenviar correos que sean catalogados como mensajes SPAM.
✓ No enviar desde su buzón, documentos (textos, software, música, imágenes o cualquier otro) que contravengan lo dispuesto en la legislación vigente y en los reglamentos internos, sobre propiedad intelectual y derechos de autor. En especial debe evitar la distribución que requiera licencia, claves ilegales de software, programas para romper licencias (crackers), y en general cualquier elemento u objeto de datos sin permiso específico del autor cuando dicho permiso sea requerido. La violación de esta obligación origina automáticamente la terminación del servicio y puede ser causa de sanciones al usuario responsable, sin perjuicio de las responsabilidades que eventualmente puedan surgir ante la ley.
✓ No Utilizar identidades ficticias o pertenecientes a otros usuarios para el envío de mensajes.
✓ Evitar el envío de respuestas con copia A TODOS los destinatarios de un mensaje recibido, y en particular cuando se trata de mensajes que originalmente hayan sido dirigidos a un grupo grande de usuarios salvo cuando se trate de una

respuesta que por su naturaleza y/o contenido, necesariamente requiera ser conocida por todos ellos.

✓ El buen uso de correo corporativo depende del usuario, y se estipula que solo se debe utilizar para procesos laborales, con el fin de mitigar suplantaciones de identidad de dominio y que clasificación en listas negras, así mismo prevenir que el dominio corporativo sea utilizado para realizar ciberataques.

5.5. Política de escritorio y pantalla limpia

Definir la política y condiciones generales que permitan mitigar el riesgo de acceso no permitido, daño y perdida de la información, durante la ejecución de actividades dentro y fuera del horario regular de trabajo de los usuarios. por tanto, se describe los siguientes lineamientos:

✓ Es obligación de los usuarios al ausentarse de su estación de trabajo bloquear la sesión de su equipo de forma manual, la cual estará protegida por las credenciales asignadas.

✓ Los usuarios al ausentarse de su estación de trabajo deberán guardar cambios en los documentos y sistemas de información que contengan información pública de uso interno, pública clasificada o pública reservada.

✓ Es obligación de los usuarios mantener la pantalla de computador (escritorio) libre de archivos o enlaces de acceso a archivos, estos deben ubicarse en las debidas carpetas de almacenamiento.

✓ El escritorio del equipo de cómputo no debe tener información sensible o confidencial que pueda ser de fácil acceso.

✓ Los equipos de reproducción de información (impresoras, fotocopiadoras, escáneres, etc.), deben estar ubicados en lugares de acceso controlado y cualquier documentación con información pública clasificada o pública reservada se debe retirar inmediatamente del equipo y ser puesta en un lugar seguro.

5.6. Uso del internet y Seguridad conectividad

NIVEL DE CUMPLIMIENTO

Establecer una política que asegure de manera eficiente el control y manejo del tráfico de internet, su buen uso y controles para optimizar la seguridad que ayudan a mitigar el riesgo ante ciberataques aplican para todos los empleados que le sean asignados o tengan manipulación sobre el activo de información. por tanto, se describe las siguientes directrices:

✓ Es responsabilidad del usuario el buen uso del servicio de internet y estipula que la descarga de archivos de sitios no seguros y que no tengan certificado de seguridad están totalmente prohibidos, esto con el fin de mitigar los ciberataques o suplantación de identidadLos usuarios no deben guardar contraseñas en los

navegadores ni en archivos ya que coloca en riesgo la seguridad de los activos de información.

✓ El usuario entiende que el acceso a plataformas de correos de uso gratuito o personal, redes sociales esta prohibido.

✓ En las excepciones que se presenten autorizadas por gerencia referente a redes sociales u otras plataformas que presenten vulnerabilidad. el usuario entiende que es responsable del uso de este medio.

✓ Los usuarios solo podrán conectarse a internet usando los medios dispuestos por la compañía y no podrán acceder a treves de otros canales de proveedores de servicios de internet externos.

✓ Solo se podrá utilizar el navegador o browser asignados e instalados por el dpto de tecnología.

6 REFERENCIAS

✓ SARLAFT

_____

Representante Legal
HERIZ KINLEINER ZUÑIGA CELIZ
AERCARGO SERVICES SAS

AERCARGO SERVICES S.A.S
Nuestro Objetivo es Cumplir
NIT: 901.201.525-6

TABLA DE CONTROL DE CAMBIO

NÚMERO DE VERSIÓN	FECHA	DESCRIPCIÓN DEL CAMBIO
1	01/08/2026	Creación de documento

AERCARGO SERVICES S.A.S
Nuestro Objetivo es Cumplir
NIT: 901.201.525-6

ELABORO	REVISO	APROBÓ
Yurvis Jerez	**Cindi Madrid**	Heriz Kinleiner Zúñiga