1. OBJETIVO

El objetivo de esta política es proteger la integridad, confidencialidad y disponibilidad de la información y los sistemas informáticos de **COORDINADORA COMERCIAL DE CARGAS S.A.S.** para asegurar el funcionamiento continuo y proteger los activos de la empresa contra accesos no autorizados, daño o pérdida.

2. ALCANCE

Esta política se aplica a todos los empleados, contratistas y terceros que tengan acceso a los sistemas y datos de **COORIDNADORA COMERCIAL DE CARGAS S.A.S**.

3. RESPONSABILIDADES

Es responsabilidad de **COORDINADORA COMERCIAL DE CARGAS S.A.S** y **SOLUCIONES** asegurar que los derechos de acceso de sus empleados a los sistemas de información y recursos informáticos estén alineados y actualizados según el nivel de autorización correspondiente. Esto debe permitir a los empleados realizar sus funciones de manera adecuada, garantizando que los accesos se concedan, mantengan o revoquen conforme a las necesidades operativas y las políticas de seguridad establecidas.

Proceso de Tecnologia- TI: Es responsable de implementar y mantener las medidas de seguridad necesarias, así como de proporcionar formación sobre seguridad informática.

Líderes: Es responsabilidad de **COORDINADORA COMERCIAL DE CARGAS S.A.S.**, a través de los líderes de los procesos de la información, garantizar una correcta administración de las herramientas tecnológicas e informáticas dentro de su estructura organizacional. Los líderes deben asegurarse de que las responsabilidades y funciones estén claramente definidas y que las herramientas tecnológicas sean asignadas al personal calificado, asegurando así su uso adecuado y eficiente en el cumplimiento de los objetivos organizacionales.

Usuarios: Todos los usuarios de **COORIDNADORA COMERCIAL DE CARGAS S.A.S**., son responsables de seguir las directrices establecidas en esta política y de proteger la información a la que tienen acceso.

4. POLÍTICA GENERAL

- Toda persona que para el desempeño de sus funciones utilice o tenga acceso a los bienes o servicios informáticos que ofrece de **COORIDNADORA COMERCIAL DE CARGAS S.A.S**., deberá observar lo prescrito en la presente política. La ignorancia del mismo no lo exonera de las responsabilidades asociadas con su incumplimiento.

- El proceso de Gerencia Administrativa y financiera, Tecnologia, junto con el sistema integrado de Gestion de **CORIDNADORA COMERCIAL DE CARGAS S.A.S**., vigilarán que se acaten las Políticas Informáticas vigentes.

- Toda adquisición de cualquier bien o servicio informático deberá ser considerada y aprobada por la alta Gerencia, proceso de Gerencia Administrativa y financiera y subproceso de Tecnologia quién evaluará la necesidad, conveniencia de dicha adquisición, especificando las características y configuración mínimas del bien o servicio a adquirir. Dichas características deberán detallarse en la solicitud de cotización/términos de referencia/pliego de condiciones respectiva, efectuará la evaluación técnica de las propuestas presentadas para la adquisición de bienes y/o servicios informáticos.

- La versión vigente y reglamentada de los procedimientos del **CORIDNADORA COMERCIAL DE CARGAS S.A.S**., se encontrará publicada en la página de la entidad, una vez se cuente con ella.

- Toda solicitud de servicio informático referente a: Creación de identificación o nombre de usuario, acceso a navegar en Internet, asignación o cambio del perfil de un usuario para acceder a los sistemas de información, acceso a trabajar en horas no hábiles, cambios o modificaciones a los sistemas de información (soporte legal para el caso en el que aplique); debe ser presentada al jefe administrativo por escrito (vía e-mail institucional) y deben estar firmadas por el jefe del proceso.

- Los accesos a los sistemas y datos estarán limitados y se otorgarán basados en el principio de mínimo privilegio. Solo se concederá acceso a la información necesaria para que cada usuario realice su trabajo.

- Para el retiro de bienes informáticos como portátiles, de la entidad, en calidad de préstamo, por motivos de capacitaciones, charlas, cursos y Teletrabajo, fuera de las instalaciones de **CORIDNADORA COMERCIAL DE CARGAS S.A.S**, deberá ser registrada, por el personal encargado de Tecnologia, quien a su vez deberá tener los bienes informáticos guardados en el almacén de la entidad.

- Los recursos tecnológicos deben ser utilizados de manera ética, legal y en beneficio de los objetivos organizacionales. Está prohibido el uso para fines personales que puedan interferir con el trabajo o poner en riesgo la seguridad.

- Se debe proteger el hardware, software y demás recursos tecnológicos contra robos, daños y accesos no autorizados. Todos los usuarios deben manejar los equipos con cuidado y reportar cualquier problema o incidente al subproceso de TI.

- Al momento de desvinculación de un empleado de la entidad, la Oficina Administrativa y Financiera, deberá verificar que los bienes informáticos entregados al funcionario se encuentren completos.

5. DIRECTRICES PARA EL ACCESO Y CONTROL DE RECURSOS INFORMÁTICOS

Dado que los administradores de sistemas de información tienen acceso a los archivos, mensajes de correo electrónico de los usuarios y cierta información confidencial, es necesario establecer límites en las atribuciones conferidas.

Por otra parte, es necesario identificar sus responsabilidades y comportamiento esperado en el cumplimiento de su deber, para asegurar la protección apropiada de los sistemas de información.

Los administradores de sistemas tienen las mismas responsabilidades que tienen los usuarios más las responsabilidades adicionales, deberes y derechos que surgen por la naturaleza de su trabajo.

5.1 Entre otros, son deberes o responsabilidades de los administradores de sistemas:

- Actuar con ética y profesionalismo, protegiendo la privacidad y confidencialidad de la información.
- Mejorar continuamente la seguridad de los sistemas, resolviendo brechas lo antes posible.
- Configurar y orientar los sistemas para identificar a los usuarios y sus accesos.
- Implementar medidas de seguridad sin afectar innecesariamente el trabajo de los usuarios.
- Proteger los recursos contra corrupción, pérdida, fallos y destrucción.
- Configurar accesos y permisos para que solo personas autorizadas usen los recursos.
- Evaluar y ajustar medidas de seguridad según sea necesario para reducir riesgos.
- Informar sobre interrupciones o cambios que puedan afectar los datos.
- Incorporar la seguridad informática en las labores diarias y documentar el trabajo.
- Desarrollar procedimientos para recuperación ante contingencias informáticas.
- Capacitarse en seguridad informática y participar en actividades institucionales.
- Aplicar y divulgar políticas de seguridad y cumplir las directrices institucionales.
- Mantener copias de respaldo y aplicar parches de seguridad según la criticidad.
- Revisar archivos de registro para detectar accesos o usos no autorizados.
- Verificar el software legal y el uso adecuado de los equipos.
- Tratar como confidenciales los contenidos de archivos de usuario.
- Gestionar incidentes de seguridad con sentido común y sensibilidad, escalando solo si es necesario.

5.2 Limitaciones en el Uso de Recursos Informáticos:

No leerán el correo o archivos de uso restringido de los usuarios a menos que para el cumplimiento de sus deberes sea realmente necesario. En tales casos el acceso se hará al nivel menos invasivo, tratando dichos archivos como si fuese información privada o confidencial.

No deben borrar ningún archivo de usuario que se encuentre almacenado en los sistemas de cómputo al servicio de **CCCARGAS S.A.S**. sin el permiso de su propietario, a menos que la presencia del archivo interfiera con la operación del sistema.

Pueden suspender temporalmente el acceso a Internet a computadores desde los cuales se observe usos inaceptables, no acordes a las políticas y fines institucionales.

Pueden por razones de seguridad o por usos inaceptables, deshabilitar temporalmente las cuentas de correo de los usuarios.

Pueden contribuir, y están invitados, a la revisión y mejoramiento de las políticas institucionales de seguridad informática.

5.3 Supervisión Y Uso Responsable De Recursos Informáticos:

CCCARGAS S.A.S., se reserva el derecho a supervisar, duplicar o registrar todo el uso que los funcionarios y otros usuarios autorizados le den a los recursos informáticos de **COORDINADORA COEMRCIAL DE CARGAS S.A.S.,** con o sin aviso. Esto incluye pero no está limitado al uso del correo electrónico, uso de Internet, inicios de sesión de trabajo, accesos a archivos y pulsaciones de teclas.

Más aún, es un deber de todo funcionario público vigilar y salvaguardar los recursos informáticos al servicio de **CCCARGAS S.A.S.,** para que se usen debida y racionalmente, de conformidad con los fines institucionales para los cuales han sido destinados.

Para facilitar su cumplimiento **CCCARGAS S.A.S.,** dispondrá de controles que permitan cuantificar al máximo posible el uso de los recursos de tal forma que se facilite el autocontrol y sea posible un control mutuo del uso racional y transparente que debe darse a los recursos de **COORDINADORA COMERCIAL DE CARGAS S.A.S.**

Las responsabilidades y deberes de los administradores de sistemas informáticos de CCCARGAS están detalladas en la Política de Administración de Sistemas. En particular, las siguientes están directamente relacionadas con el cumplimiento de las políticas institucionales de seguridad informática:

* Orientar y configurar los sistemas que administran de tal forma que en cualquier momento se pueda identificar a los usuarios que acceden o usan un determinado recurso informático.

* Realizar revisiones periódicas a los computadores personales y estaciones de trabajo de los usuarios que se encuentren bajo su cuidado, para verificar que solamente se esté utilizando en ellos software legal autorizado y que el uso que se les da a estos equipos esté acorde a las políticas institucionales.

Usuarios Son responsabilidades de los usuarios:

* Utilizar los recursos informáticos observando y cumpliendo las políticas y directrices Institucionales.

6. USO APROPIADO

El estándar de conducta para el uso de los recursos informáticos debe alinearse con el estándar general de comportamiento esperado de los funcionarios y otros usuarios autorizados en el manejo de cualquier recurso institucional.

El uso de estos recursos debe ser ético, legal, honesto, racional, eficiente, responsable, respetuoso de los derechos de autor y acorde con los mecanismos de seguridad y control establecidos.

Se espera que todos los usuarios actúen con responsabilidad al acceder o transmitir información a través de las redes de cómputo de **CCCARGAS S.A.S.** Los usuarios son responsables de sus acciones en estos entornos digitales, de la misma manera que lo serían al utilizar otros medios tradicionales.

6.1 Ejemplos de usos inaceptables/inapropiados

- Realizar actividades ilegales con los recursos institucionales.
- Usar los recursos para fines personales durante el horario laboral.
- Compartir datos o información sin autorización.
- Ignorar leyes de derechos de autor en textos, multimedia y software.
- Violar políticas, reglamentos o directrices institucionales.
- Usar los recursos para actividades no relacionadas con la misión de la empresa.
- Realizar negocios personales o comerciales con los recursos institucionales.
- Poner en riesgo la información, los recursos o los intereses de la empresa.
- Interferir con sistemas de cómputo y telecomunicaciones.
- Permitir el acceso a usuarios no autorizados o usar contraseñas ajenas.
- Difamar a personas a través de correo electrónico u otros medios.
- Alterar configuraciones de software o hardware sin autorización.
- Acceder a datos o archivos de otros usuarios sin permiso.
- Leer correspondencia electrónica ajena sin autorización.
- Compartir contraseñas o datos personales.
- Hacer parecer que se representa a la empresa sin autorización.
- Suplantar identidades o usar cuentas ajenas.

- Realizar actividades no institucionales como ver contenido pornográfico o almacenar música.
- Evitar mecanismos de seguridad o interferir con la red.
- Ayudar a otros a violar reglas o políticas.
- Interceptar o alterar información transmitida.
- Tomar prestados recursos sin autorización.
- Usar software sin respetar derechos de autor o licencias.
- Establecer conexiones no autorizadas con otras redes.
- Cargar excesivamente sistemas o ejecutar códigos dañinos.
- Crear o reenviar cadenas de mensajes no relacionadas con la empresa.
- Escribir o almacenar contraseñas sin protección.
- Instalar software sin autorización.
- Realizar actividades ilegales, inapropiadas u ofensivas.
- Crear o transmitir material sexualmente explícito.
- Usar recursos informáticos para juegos.

7. USO DE INTERNET

El servicio de Internet es un recurso clave para **COORDINADORA COMERCIAL DE CARGAS S.A.S.** y debe usarse para apoyar los objetivos de la empresa, maximizando beneficios y minimizando costos. Se proporciona acceso a Internet a empleados cuyo rendimiento pueda mejorar con su uso, y se fomenta el desarrollo de habilidades para su uso efectivo.

El acceso a Internet debe limitarse a actividades relacionadas con la empresa, salvo uso personal limitado fuera del horario laboral. Los usuarios deben usar Internet para ampliar conocimientos, acceder a información relevante y comunicarse en el ámbito institucional.

Al utilizar Internet con direcciones de **COORDINADORA COMERCIAL DE CARGAS S.A.S.**, los usuarios representan a la empresa y deben evitar cualquier uso que pueda perjudicar su reputación. Es fundamental usar buen juicio al acceder a sitios web, evitando aquellos no relacionados con el trabajo o que puedan comprometer la seguridad de la empresa.

El uso de Internet debe ser legal, respetando derechos de autor y sin interferir con el trabajo de otros. Los usuarios que no requieran acceso a Internet para sus funciones laborales no deben usar los equipos de la empresa para acceder a la red.

8. SEGURIDAD

El acceso y uso de Internet en **CCCARGAS S.A.S.** debe realizarse a través de una puerta de enlace segura, equipada con un firewall que controle todos los paquetes de datos entrantes y salientes, y que impida conexiones no autorizadas a las redes internas de la organización.

Los servicios de red institucionales autorizados para acceso desde Internet deben ser operados únicamente después de implementar medidas de seguridad básicas, como el uso de conexiones encriptados, para garantizar la protección de los datos y la infraestructura.

Para acceder remotamente a los equipos de **COORDINADORA COMERCIAL DE CARGAS S.A.S.**, es obligatorio utilizar conexiones seguras, evitando el uso de servicios de alto riesgo como Telnet, FTP y otros que son conocidos por sus vulnerabilidades.

Los servicios de red o conexiones autorizadas desde **COORDINADORA COMERCIAL DE CARGAS S.A.S.** hacia Internet incluyen: navegación web (HTTP y HTTPS), correo electrónico, conexiones remotas seguras (SSH), transferencia de archivos mediante FTP, consultas DNS, sincronización de tiempo y copias remotas usando rsync. Otros servicios y conexiones serán autorizados conforme a las necesidades y conveniencias institucionales.

Por razones de seguridad, se prohíbe el uso de software de mensajería instantánea, chat y similares, así como cualquier otro servicio de red o conexión a Internet que no esté explícitamente autorizado.

No está permitido conectarse a Internet utilizando equipos no oficiales, como el uso de módems en PCs personales para este propósito.

Se prohíbe el uso de contraseñas institucionales en sitios de Internet.

Recuerde que cualquier documento enviado a través de Internet puede ser interceptado por terceros. Por lo tanto, actúe siempre conforme a las políticas de confidencialidad de **CCCARGAS S.A.S.** y asegúrese de proteger la información sensible.

9. CORREO ELECTRONICO

El servicio de correo electrónico facilita la comunicación interna y externa, apoyando la misión de **COORDINADORA COMERCIAL DE CARGAS**.

- No se debe enviar información confidencial no autorizada por correo electrónico. Para enviar información confidencial, use teléfono o correo postal. Si es necesario usar correo electrónico, solicite encriptación.
- Las cuentas de correo electrónico son para uso oficial. Se permite el envío ocasional de mensajes breves y de solo texto, según la política.
- No use direcciones de correo de CCCARGAS S.A.S. para suscribirse a listas no relacionadas con la empresa (por ejemplo, redes sociales como Facebook).
- Limite la distribución de correos electrónicos al menor número posible de destinatarios para evitar congestión de red.

- Evite enviar información institucional a correos de servidores públicos externos que puedan comprometer la seguridad.
- No abra archivos adjuntos de remitentes desconocidos, ya que pueden contener virus o malware.
- No envíe correos no solicitados (spam), cadenas de mensajes o materiales publicitarios a personas no interesadas.
- No comparta sus contraseñas de correo electrónico.

10. PRIVACIDAD Y SUPERVISIÓN

COORDINADORA COMERCIAL DE CARGAS S.A.S., se reserva el derecho de revisar los archivos de correo electrónico de los usuarios en cualquier momento para asegurar el cumplimiento de las políticas, razones de seguridad, necesidades técnicas u otros fines legítimos.

Dado que los administradores del sistema pueden supervisar las transmisiones y revisar ocasionalmente los contenidos de los mensajes, la privacidad no está garantizada. Los usuarios no deben tener expectativas de privacidad en la información electrónica.

11. DEBERES Y RESPONSABILIDADES

- **Uso Apropiado:** Todos los usuarios deben utilizar el servicio de correo electrónico de COORDINADORA COMERCIAL DE CARGAS S.A.S. exclusivamente para fines laborales. Deben proteger sus contraseñas, cerrar sesiones de trabajo y tomar medidas para evitar accesos no autorizados.
- **Revisión y Capacitación:** Los usuarios deben revisar su correo periódicamente y responder de manera adecuada. Es importante capacitarse sobre los riesgos asociados al correo electrónico.
- **Actuar Éticamente:** Cuando se necesite revisar correos ajenos, se debe hacer de manera ética y con el menor impacto posible.
- **Respuesta Oportuna:** Los usuarios deben responder los correos de manera apropiada y dentro de los plazos establecidos.

12. PRIVACIDAD

Uso Particular: COORDINADORA COMERCIAL DE CARGAS S.A.S., permite un uso personal limitado de los recursos informáticos fuera del horario laboral, según la política de Uso Particular. Sin embargo, esto no implica derecho a privacidad, ya que estos recursos están destinados principalmente para actividades laborales.

Expectativas de Privacidad: Los empleados, contratistas y otros trabajadores no tienen expectativas de privacidad al usar los recursos informáticos, incluidos Internet y correo electrónico. Si desean mantener la privacidad, deben evitar usar los recursos de la empresa para actividades personales.

Seguridad y Supervisión: La privacidad no está garantizada debido a la naturaleza de la información electrónica. El uso de los recursos debe considerarse como no seguro ni anónimo. Al usar estos recursos, los empleados aceptan la posibilidad de supervisión y reporte de su uso. Los administradores pueden generar y compartir reportes sobre el uso de los recursos con las autoridades pertinentes.

DEBERES

Reporte de Incidentes: Todos los usuarios deben informar a los administradores o directivos sobre el uso inapropiado de los recursos. Pueden hacerlo de manera anónima si lo prefieren.

Aplicación de Políticas: Las normas y reglamentos de COORDINADORA COMERCIAL DE CARGAS S.A.S. también se aplican al entorno electrónico. En caso de conflicto entre políticas, prevalecerá la que más beneficie a los intereses de CCCARGAS.

Violaciones de Política

13. INFRACCIONES MENORES

Resolución de Infracciones Menores: Las infracciones menores, como selección inapropiada de contraseñas o sobrecarga de sistemas, generalmente se resuelven de forma informal por el Administrador del Sistema. Los usuarios también pueden intervenir y concienciar sobre estas infracciones.

Infracciones Repetidas: Infracciones menores repetidas pueden llevar a la pérdida temporal o permanente de privilegios de acceso.

Infracciones Graves: Infracciones serias, como uso no autorizado de recursos, intentos de robo de datos, o violaciones graves de las políticas, pueden resultar en acciones disciplinarias y pérdida de acceso. En casos graves, el infractor será notificado y, si es un funcionario, el caso será remitido a control interno.

Violaciones Legales: Infracciones que violen leyes locales o nacionales resultarán en la pérdida inmediata de privilegios y posibles acciones legales por parte de CCCARGAS.

14. DEFINICIONES

AMENAZA: Es un evento o actividad, intencional o no intencional, con el potencial de causar daño a un sistema o actividad informática.

CUENTA DE CORREO: Identificador único con una contraseña asociada, que se asigna a un usuario para que pueda utilizar el servicio de correo electrónico.

DATOS PERSONALES: Información que identifica o describe a un individuo.

INTEGRIDAD: Característica de los datos y la información de ser y permanecer exactos y completos.

MENSAJE EN CADENA: Mensaje de correo que intenta inducir al destinatario a reenviar ese mensaje a dos o más destinatarios nuevos.

POLÍTICA: Es una declaración formal de las reglas o normas que los usuarios de los recursos tecnológicos y de información de una organización deben acatar.

PRIVADO: Particular y personal de cada uno.

PRIVACIDAD: Libertad de intrusión no autorizada (2) calidad o estado de estar apartado de observación o compañía.

RECURSOS INFORMÁTICOS: Hardware, software, datos e información, incluyendo equipos de cómputo y telecomunicaciones.

RIESGO: Es una pérdida o daño futuro potencial que puede surgir por alguna acción presente.

SEGURIDAD: Medidas tomadas para reducir el riesgo de 1) acceso y uso no autorizado 2) daño o pérdida de los recursos, por algún desastre, error humano, fallo en los sistemas, o acción maliciosa.

SEGURIDAD FÍSICA: Medidas de protección para controlar el acceso a los recursos de información electrónica por medios físicos.

SEGURIDAD LÓGICA: Medidas de protección para controlar el acceso a los recursos de información electrónica por medios lógicos (por ejemplo mediante controles de software).

SENSIBILIDAD: Grado de confidencialidad de la información.

SERVIDOR: Computador no necesariamente multiusuario/multitarea que desempeña una función específica, generalmente en forma dedicada y desatendida. En un servidor no trabajan los usuarios.

SERVIDOR INTERMEDIARIO: Es un servidor que actúa como intermediario entre una estación de trabajo de un usuario y el Internet, que se instala por seguridad, control administrativo y servicio de caché, disminuyendo el tráfico de Internet e incrementando la velocidad de acceso.

SERVIDOR PROXY: Véase Servidor intermediario.

SISTEMA: Término genérico utilizado por brevedad para hacer referencia a sistema de información.

SISTEMA DE INFORMACIÓN: Personas, equipos informáticos, software, métodos y procedimientos de operación, utilizados para colectar, almacenar, procesar, recuperar o transmitir datos e información de los usuarios.

SITIO: Es cualquier organización que posee computadores o recursos relacionados con redes de cómputo.

USO ACEPTABLE: Uso adecuado, uso tolerable.

USO APROPIADO: Uso correcto.

USO NO ACEPTABLE: Uso inadecuado que no se puede tolerar.

USO PARTICULAR: No laboral. Es el uso eventual de los recursos para fines no laborales, no relacionados con Coordinadora Comercial De Cargas.

USO PERSONAL: Uso para fines individuales. El uso individual puede ser laboral o no laboral.

USUARIO: Término utilizado por brevedad para referirse a usuario autorizado.

USUARIO AUTORIZADO: Persona que mantiene alguna relación oficial o formal con CCCARGAS, a quien se le ha concedido una debida autorización para acceder a un recurso informático con el propósito de desempeñar sus deberes laborales u otras gestiones relacionadas directamente con los intereses de CCCARGAS.

VULNERABILIDAD: Es un desperfecto o debilidad que permite que ocurra un daño a un sistema o actividad informática.

15. CUMPLIMIENTO

COORDINADORA COMERCIAL DE CARGAS S.A.S. puede realizar auditorías periódicas al proceso de TI para asegurar el cumplimiento de esta política.

Esta política será revisada anualmente y actualizada según sea necesario.

Los usuarios que violen esta política podrán enfrentar medidas disciplinarias.

CESAR JAVIER ORJUELA AVELLA
REPRESENTANTE LEGAL

CONTROL DE CAMBIO		
VERSIÓN	**DESCRIPCIÓN DEL CAMBIO**	**FECHA**
2	Se realizan modificaciones del documento	30-05-2018
3	Se realizan modificaciones del documento	22/08/2024