1. OBJETIVO.

Establecer los lineamientos generales para el uso, protección y gestión segura de los recursos informáticos y la información de Papeles y Corrugados Andina S.A.S, con el fin de garantizar su confidencialidad, integridad y disponibilidad, así como mitigar los riesgos que puedan afectar la operación de la organización.

2. ALCANCE.

Esta política aplica a todos los empleados, contratistas, proveedores y terceros que accedan a la infraestructura tecnológica o a la información de la organización.

3. RESPONSABILIDADES.

- Gestión Sistemas: Implementar los controles técnicos y administrativos necesarios para garantizar la seguridad de la información.
- Usuarios (Todos los trabajadores): Cumplir con las disposiciones de esta política, usar los recursos tecnológicos de manera adecuada y reportar incidentes o sospechas de vulnerabilidades.

4. LINEAMIENTOS.

La política de seguridad de la información de Papeles y corrugados Andina S.A.S, busca promover a través de una gestión de riesgos, la adopción de controles, por parte de todos los trabajadores, sobre las fuentes de información operativas, tácticas y/o estratégicas que se utilicen para el logro de los objetivos estratégicos de la organización.

Esta política pretende preservar la confidencialidad, integridad y disponibilidad de la información mediante lineamientos y controles adoptados según los requisitos exigidos por las buenas prácticas y que, con su adopción desde la Presidencia, se establece el cumplimiento de éstas para garantizar la seguridad y privacidad de los activos de información, minimizando posibles impactos no deseados que comprometan los principios esenciales de la seguridad de la información.

4.1. LINEAMIENTOS GENERALES.

- Todo trabajador de Papeles y Corrugados Andina S.A.S, debe asegurar los activos de información bajo su gestión.
- Los trabajadores serán los directamente responsables de proteger la información a la cual accedan y procesen, para evitar su pérdida, alteración, destrucción o uso indebido.

- Está restringido el acceso a personal no autorizado a la información y a los medios para su procesamiento manual o automatizado.
- El proceso de Gestión Sistemas apoyará la gestión de aseguramiento de la información durante todo su ciclo de vida utilizando herramientas tecnológicas especializadas en el tema.
- Es requerido definir acuerdos de interacción con terceros para preservar la confidencialidad, integridad y disponibilidad de la información compartida y/o transmitida.
- Todos los trabajadores deben reportar con diligencia, prontitud y responsabilidad, presuntas violaciones de seguridad, eventos sospechosos y el mal uso de los recursos de información o comunicaciones.
- Papeles y Corrugados Andina S.A.S, solo permitirá el uso de software autorizado que haya sido adquirido legalmente por la organización y autorizado explícitamente por el Proceso de Sistemas.
- Se mantendrá acceso controlado y restringido a los cuartos de servidores principales.
- Todos los trabajadores deben firmar un acuerdo de confidencialidad.
- El incumpliendo o violación de la Política de Seguridad de la Información será sancionado según, lo establecido en el reglamento interno de trabajo de Papeles y Corrugados Andina S.A.S.
- Anualmente se debe actualizar la matriz integral de riesgos, con los riesgos y/o controles asociados a seguridad de la información.
- Todo acceso remoto de un trabajador a la infraestructura de Papeles y Corrugados Andina S.A.S, debe ser debidamente autorizado por la Presidencia y generado por el proceso de Gestión Sistemas para asegurar la confidencialidad de la información.
- Se deben mantener prácticas de mejora continua para la gestión de seguridad de la información.
- Todo equipo corporativo debe contar con un antivirus debidamente instalado y actualizado.

4.1. Uso de los equipos de cómputo.

- Los bienes y recursos TIC corporativos se emplearán de manera exclusiva por el usuario al cual han sido asignados y únicamente para el correcto desempeño de su cargo o función, por lo tanto, no deben ser utilizados con fines personales o por terceros no autorizados.

- Durante la jornada laboral y en todo tiempo de uso, corresponde al usuario prestar la debida custodia y cuidado a los equipos de cómputo asignados, así como impedir su sustracción, destrucción, ocultamiento o utilización indebida.
- Las credenciales de acceso a los servicios TIC (nombre de usuario y contraseña) son de carácter estrictamente personal e intransferible, por lo tanto, los usuarios no deben revelarlas a terceros ni utilizar credenciales ajenas a las asignadas.
- Todo usuario debe verificar que los equipos de cómputo asignados se encuentren debidamente conectados a fuentes de corriente reguladas.
- Los usuarios deben bloquear su computador cuando no están utilizando el equipo o no está presente en su puesto de trabajo.
- Los únicos autorizados para realizar modificaciones a la configuración original de los equipos, así como para destapar, agregar, desconectar, retirar, revisar y/o reparar sus componentes, es le proceso de Gestión Sistemas y/o las personas por ellos autorizadas.
- Toda pérdida de equipos de cómputo o de alguno de sus componentes debe ser informada de inmediato Gestión Sistemas.
- Todos los equipos de cómputo se deben apagar correctamente en ausencias prolongadas y en lo posible al final de la jornada laboral. No se debe dejar hibernando el equipo por un periodo prolongado de tiempo, se debe reiniciar para que se realicen las actualizaciones de seguridad.
- Todo problema de orden técnico con los equipos de cómputo o con el software que en ellos se ejecuta, debe ser reportado a Gestión Sistemas.

4.2. Información contenida en los equipos de cómputo.

- Toda la información generada, almacenada o procesada en los equipos es propiedad de la organización.
- El usuario es responsable de proteger la información confidencial y respaldarla según los lineamientos internos.

4.3. Uso, instalación y desinstalación de software y hardware.

- Solo el proceso gestión sistemas está autorizada para instalar o desinstalar software y hardware.
- Está prohibido el uso de software pirata o sin licencia.
- Cualquier requerimiento debe canalizarse formalmente al proceso de Gestión Sistemas.

4.4. Correo electrónico corporativo.

- El correo electrónico corporativo es una herramienta de trabajo y debe usarse exclusivamente para actividades relacionadas con la organización.
- Está prohibido enviar o reenviar mensajes con contenido ofensivo, cadenas, publicidad personal o información no relacionada con el trabajo.
- Los correos pueden ser monitoreados por la Papeles y Corrugados Andina S.A.S, por razones de seguridad.
- El envío de mensajes de correo electrónico debe hacerse únicamente a los destinatarios a los cuales el contenido le sea de su interés y sea necesario recibirlos.
- Todo mensaje de correo electrónico sospechoso debe notificarse al proceso de Gestión Sistemas, para que se revise la procedencia del mensaje y en caso de confirmarse que es malicioso, realizar las acciones correspondientes (eliminación de correo, bloqueo de destinatario y/o IP de procedencia en caso de que aplique, etc.)
- El reenvío de mensajes sólo debe realizarse en casos estrictamente necesarios.
- Sólo deben imprimirse los mensajes importantes que así lo requieran, ya que una de las ventajas y fines del servicio de correo electrónico corporativo es la transmisión de información con ahorro de papel.
- La cuenta de correo no debe utilizarse para enviar o recibir música, programas, material pornográfico, fotos, videos o cualquier otro ajeno a los fines de la Organización.
- Se prohíbe el envío y/o reenvío de mensajes en cadena.

4.5. Uso de internet.

- El servicio de Internet Corporativo únicamente puede ser utilizado para el desarrollo de actividades directamente relacionadas con el cumplimiento de la misión de Papeles y Corrugados Andina S.A.S y las funciones asignadas a sus colaboradores Se encuentra restringido el acceso a sitios de contenido adulto, juegos, apuestas, redes sociales (salvo casos justificados), y otros sitios que puedan representar riesgo.
- Se restringe a todos los niveles el acceso a sitios clasificados con el siguiente contenido: pornografía, desnudez, juegos en línea, racismo, violencia, sitios con potencial de infección (Spyware, Malware, etc.), tráfico de armas, drogas o cualquier comercio ilícito a través de Deep WEB o cualquier plataforma.

- NOTA: Gestión Sistemas, podrá limitar el acceso a determinadas páginas de Internet, los horarios de conexión, los servicios ofrecidos por la red, la descarga de archivos y cualquier otro aspecto ajeno a los fines corporativos. El acceso a internet es permitido de acuerdo con las funciones de cada cargo.
- El tráfico es monitoreado y controlado por la Papeles y Corrugados Andina S.A.S.

4.6. Servicio telefónico.

- Las líneas telefónicas fijas o móviles asignadas por la organización deben utilizarse para comunicaciones laborales.
- No se permite su uso para llamadas personales frecuentes, nacionales o internacionales, salvo autorización expresa.

4.7. Dispositivos móviles.

- Los teléfonos móviles, tablets y otros dispositivos entregados por la organización deben utilizarse bajo criterios de seguridad definidos por gestión sistemas.
- En caso de pérdida o robo, el colaborador debe reportar inmediatamente el hecho para tomar las acciones correspondientes (bloqueo remoto, rastreo, etc.).
- Se deben activar las funciones de bloqueo por contraseña, antivirus y cifrado cuando sea posible.

4.8. Derechos de autor.

- Todos los usuarios deben respetar las licencias de software, propiedad intelectual, patentes, marcas registradas y demás derechos de autor.
- En presentaciones, documentos, informes, entre otros, que utilicen los trabajadores o contratistas para las labores de su cargo, asegúrese de mencionar la fuente de donde se extrajo la información, cuando así se requiera.
- No está permitido copiar, distribuir o modificar contenidos protegidos sin la debida autorización.
- Papeles y Corrugados Andina S.A.S, puede tomar acciones disciplinarias y legales frente al incumplimiento de esta política.

5. Vigencia.

La presente política entra en vigor a partir de la fecha de su aprobación y estará sujeta a revisiones anuales o cuando se presenten cambios significativos en los procesos tecnológicos, normativos o de negocio.

Esta política de Seguridad de la Información es responsabilidad de todos los trabajadores, empresas asociadas, de Terceros y socios y su cumplimiento es obligatorio.

Atentamente,

Presidencia.
Fecha Actualización 09 de junio de 2025.