1 OBJETIVO

Establecer los lineamientos necesarios para la protección de la información propia de Comunicaciones Empresariales de Colombia SAS (**CEM**) que es transferida al interior o al exterior de la compañía.

2 ALCANCE

Las reglas contenidas en este estándar aplican para todos los empleados, sistemas de información, procesos o terceros de Comunicaciones Empresariales de Colombia SAS

Este estándar complementa la **SIGO-SI-10.0-GSI-POL Política de Transferencia de Información**

3 DEFINICIONES

Activo de información: Según la Norma ISO/IEC 27000 un activo es cualquier cosa que tiene valor para la organización. Es información de diferentes tipos, registrada o almacenada en diferentes medios, con la que una organización desarrolla su actividad y que suele ser vital para el desarrollo del negocio de la organización.

Clasificación de la Información: Es el ejercicio por medio del cual se determina que la información pertenece a uno de los niveles de clasificación estipulado por la entidad. Tiene como objetivo asegurar que la información tenga el nivel de protección adecuado. La información debe clasificarse en términos de sensibilidad e importancia para la organización.

Cifrado: Método que permite aumentar la seguridad de un mensaje o de un archivo mediante la codificación del contenido a una forma ilegible, de manera que sólo pueda leerlo la persona que cuente con la clave de descifrado adecuada para decodificarlo (descifrarlo).

Información Confidencial: Esta clasificación se asigna a la información más sensible de la compañía, destinada estrictamente para manejo de un grupo reducido de personas definido por el responsable de la información. La revelación no

autorizada de la información de este tipo podría tener impactos negativos a niveles económicos, misionales, reputaciones o legales para Comunicaciones Empresariales de Colombia SAS, sus accionistas, socios o clientes.

Información Restringida: Información que únicamente debe ser conocida por personas que lo requirieren para el cumplimiento de sus funciones o proceso, sólo debe tener acceso un departamento, miembros de un proyecto, un comité, etc. pero no toda la empresa.

4 INTERCAMBIO DE INFORMACIÓN

Cuando se realicen acuerdos con terceras partes para el intercambio de información, se deben especificar en un capítulo de Seguridad de la Información anexo en el contrato o acuerdo de transmisión de datos y se firmarán por las partes interesadas, teniendo siempre en cuenta los aspectos necesarios para la transferencia segura de dicha información propia o de los clientes de Comunicaciones Empresariales de Colombia SAS.

Para asegurar la transferencia de información digital al interior y exterior de Comunicaciones Empresariales de Colombia SAS, contra interceptación, copiado, modificación o destrucción; el Área de Tecnología debe implementar las herramientas necesarias para asegurar su transferencia.

4.1. Transferencia de Archivos

- Compartir carpetas directamente desde los equipos de cómputo de los usuarios NO está permitido para el intercambio de información. En su lugar, el intercambio de información debe realizarse a través del servidor de archivos destinado para tal fin.
- Los servidores de archivos, a nivel interno y externo, deben contar con métodos de autenticación y cifrado de la comunicación (en este sentido debe evitarse el uso de protocolos inseguros como FTP, http, POP3, etc.).
- Para la transferencia de archivos con terceras partes o equipos fuera del dominio de red de Comunicaciones Empresariales de Colombia SAS, se deben utilizar canales y protocolos seguros de transferencia de archivos (por ejemplo, SFTP o FTPS).
- Si se han de transmitir datos sensibles a través de cualquier canal de comunicación externo, dichos datos deben ser enviados en forma cifrada, siempre y cuando el receptor tenga los recursos necesarios y acepte el intercambio de datos cifrados.

4.2. Correo Electrónico Corporativo

- En el caso de intercambio de información confidencial tanto interna como con terceros, los archivos adjuntos deben ir cifrados con la herramienta definida por la compañía o por la definida contractualmente con el tercero.
- Todo correo debe incluir en la firma una advertencia de seguridad.
- El Área de Tecnología, deberá controlar las acciones para reenvío automático de correo electrónico a direcciones de correo externo.
- Periódicamente los usuarios deben limpiar el buzón de correo, borrando mensajes antiguos que ya no son necesarios y los mensajes que se requieran guardar deben archivarse en carpetas.
- El intercambio de información a través de correos electrónicos corporativos a cuentas personales (Gmail, Hotmail, Yahoo, etc.) sólo está permitido hacia cuentas autorizadas, propiedad de clientes o proveedores.
- Se debe confirmar el destinatario del mensaje de correo electrónico antes de su envío.

4.3. Aplicaciones

- Las aplicaciones deben contar con roles y privilegios que limiten el acceso a la información de acuerdo a su nivel de autorización.
- La aplicación debe limitar la impresión de información y la descarga de reportes según la clasificación de la información y los roles y privilegios establecidos.
- Las aplicaciones publicadas a terceros deben cumplir con los puntos anteriores y adicionalmente:
  - ✓ Los canales de comunicación deben contar con sistemas de cifrado, teniendo en cuenta los acuerdos definidos entre las partes.
  - ✓ En el caso de necesitar interfaces de comunicación con otras aplicaciones, éstas deben ser autenticadas y autorizadas, y todas las actividades más relevantes deben ser registradas.
  - ✓ Asegurar que el servicio publicado no pueda ser consumido desde direcciones o redes no autorizadas.
  - ✓ Los motores de bases de datos no deben ser accedidos directamente desde redes externas.

- Se prohíbe la descarga de aplicaciones desde internet, que no sean autorizadas por la compañía, así como la instalación de aplicaciones gratuitas o adquiridas, por usuarios no autorizados. Toda instalación de

aplicaciones debe ser solicitada al área de Tecnología y deberá estar autorizada por la Gerencia o Dirección del área.

4.4. Medios Físicos

- El uso de medios físicos para la transferencia de información debe ser autorizado por los Gerentes o líderes de área y seguir el procedimiento **Є.GIT-NOC-6.1-GE-PR Procedimiento puertos USB** establecido por el área de Tecnología.
- Se deben utilizar sobres o embalajes con sellos de seguridad que permitan identificar la información recibida o enviada a clientes, proveedores o partes interesadas.

5 ROLES Y RESPONSABILIDADES

Gerencias, Direcciones y/o Coordinaciones:	• Asegurarse de incluir el Anexo de seguridad de la información en el contrato o el acuerdo de transmisión de datos que sea suscrito con terceros o proveedores en los que aplique. • Verificar el cumplimiento del presente estándar y de lo establecido contractualmente con terceros para el intercambio de información.
Área de Tecnología:	• Implementar las herramientas necesarias para asegurar la transferencia de información al interior y exterior de Comunicaciones Empresariales de Colombia SAS, contra interceptación, copiado, modificación, enrutado y destrucción.
Seguridad de la Información:	• Velar por el cumplimiento de este estándar y su política relacionada.

6 VERIFICACIÓN DE CUMPLIMIENTO

- El área de Seguridad de la Información realizará inspecciones como mínimo anualmente para validar el cumplimiento de los lineamientos indicados en este documento.
- La Dirección de Auditoría de la compañía deberá realizar como mínimo una auditoría en el periodo de un año y en cualquier momento podrán adelantar inspecciones sobre los servidores, dispositivos de red, aplicaciones y equipos de cómputo para corroborar el acceso de los usuarios autorizados y los lineamientos indicados en este estándar y su política relacionada.
- Durante el ciclo de Auditorías Internas del Sistema de Gestión se revisará el cumplimiento de los controles definidos en este documento.

7 ACTUALIZACIÓN

Este documento será modificado por el Oficial de Seguridad de la Información en la medida que se requiera.

La revisión de la vigencia de las directrices se realizará mínimo una vez cada año.

8 CONTROL DE INFORMACIÓN DOCUMENTADA

Documentos que permiten verificar el cumplimiento de este estándar:

- SIGO-SI-10.0-GSI-POL Política de Transferencia de Información.

Ver SIGO-GD-1.1-CID-FR Listado Maestro de Información Documentada.

El mantenimiento de registros será de suma importancia por razones de contabilidad, auditoría y otras pertinentes a gestión.