

1	OBJETIVO.....	2
2	ALCANCE.....	2
3	DESARROLLO SEGURO.....	2
4	CUMPLIMIENTO.....	3
5	ÉTICA, SOSTENIBILIDAD Y DIRECTRICES QUE SE CUMPLEN.....	3
6	ACTUALIZACIÓN.....	3
7	APROBACIÓN DE LA POLÍTICA.....	4

USO PÚBLICO

## 1 OBJETIVO

Establecer los principios de seguridad para el desarrollo de cualquier software por parte de Comunicaciones Empresariales de Colombia SAS (**CEM**), o alguno de sus terceros.

## 2 ALCANCE

Esta política aplica a todos los sistemas de información, procesos, empleados, terceros y en general a todas las partes interesadas que acceden a la información de Comunicaciones Empresariales de Colombia SAS, propia o bajo su custodia en cualquiera de sus estados.

## 3 DESARROLLO SEGURO

Las áreas de Tecnología y Desarrollo de Software desarrollarán y/o adquirirán el software y/o hardware requerido por Comunicaciones Empresariales de Colombia SAS, de manera coordinada con el área que manifieste la necesidad de dicho software y/o hardware. Las áreas de Tecnología y Desarrollo de Software establecerán claramente los requerimientos funcionales, operacionales y especificaciones técnicas para la adquisición o desarrollo de sistemas de información y/o comunicaciones, contemplando requerimientos de seguridad de la información.

El desarrollo de software debe realizarse teniendo en cuenta las siguientes condiciones de seguridad para asegurar que los sistemas de información incluyen controles de seguridad y cumplen con las políticas de seguridad de la información:

- Contar con ambientes separados de Desarrollo, Pruebas y Producción.
- Establecer e implementar lineamientos de seguridad de acuerdo con el procedimiento Lineamientos de Seguridad para Desarrollo de Software.
- Se debe ejecutar un análisis de vulnerabilidades al desarrollo de nuevas soluciones y se deben corregir las vulnerabilidades encontradas en esta antes de su salida a producción.
- Los riesgos de seguridad de la información relacionados con el desarrollo deben ser identificados incluyendo tanto los relativos a requerimientos de negocio como a tecnología.

- Las aplicaciones de administración del core de negocio (Sisred y Sisplay) deben generar logs de auditoria para trazabilidad y seguimiento de las acciones o cambios ejecutados por los usuarios y administradores de la aplicación.
- Se debe verificar que los desarrollos de la empresa estén completamente documentados, igualmente todas las versiones de los desarrollos se deben preservar adecuadamente en varios medios y guardar copia de respaldo externa; adicionalmente deben ser registrados legalmente.

#### **4 CUMPLIMIENTO**

Cualquier empleado o tercero, que incumpla esta política o las que se requieran para desarrollar el sistema de Seguridad de la Información, debe asumir las responsabilidades y sanciones a que haya lugar definidas o relacionadas con reglamentos, la normatividad interna de Comunicaciones Empresariales de Colombia SAS. y la legislación vigente en materia de Seguridad de la Información o Protección de Datos Personales.

#### **5 ÉTICA, SOSTENIBILIDAD Y DIRECTRICES QUE SE CUMPLEN**

Todas las directrices de esta política cumplen con las leyes aplicables, las cuales incluyen regulaciones de sus partes interesadas.

Además de las reglas aplicables a Comunicaciones Empresariales de Colombia SAS para el personal y el Código de Conducta y Ética, esta Política también compromete a todo el personal a respetar la conducta ética, la responsabilidad social, la transparencia, la auditabilidad, la sólida gestión de riesgos en el contexto de la misma.

#### **6 ACTUALIZACIÓN**

Este documento será modificado de acuerdo a las necesidades de la Organización y de las áreas implicadas en el momento que se requiera y será divulgado a las partes interesadas.

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

## 7 APROBACIÓN DE LA POLÍTICA

Esta política es aprobada por la alta dirección en la figura del Representante Legal

---

Representante Legal  
**Comunicaciones Empresariales de  
Colombia SAS**

USO PÚBLICO