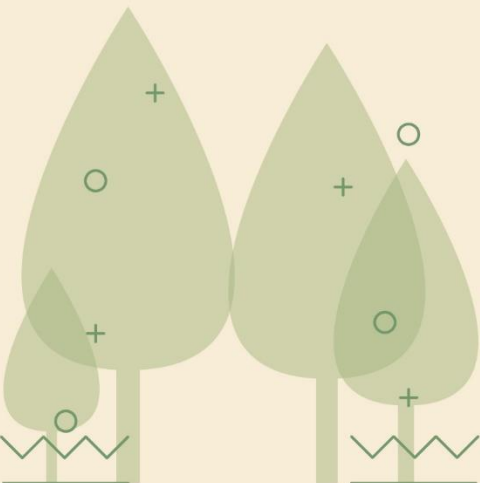




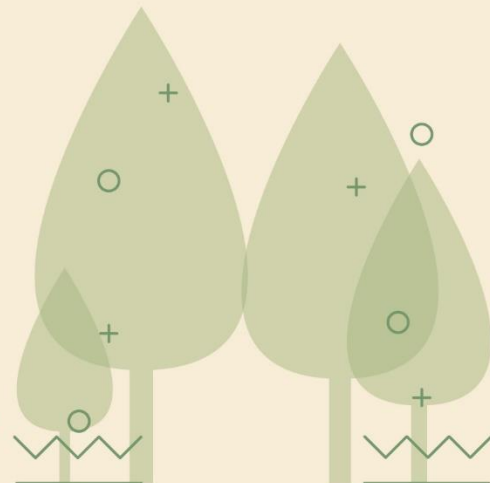
# Plan de Seguridad y Privacidad de la Información

# CORTOLIMA



Corporación Autónoma Regional del Tolima  
*¡Siembra Tu Futuro!*

# SIEMBRA TU FUTURO



## TABLA DE CONTENIDO

INTRODUCCION.....	3
1. OBJETIVOS .....	4
1.1. OBJETIVO GENERAL.....	4
1.2. OBJETIVOS ESPECÍFICOS.....	4
2. ALCANCE.....	4
3. POLITICA DE SEGURIDAD DE LA INFORMACION .....	4
4. MARCO NORMATIVO.....	6
5. COMITÉ DE SEGURIDAD DE LA INFORMACION.....	10
6. IMPLEMENTACIÓN DEL PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN .....	11

## INTRODUCCIÓN

El Plan de seguridad y privacidad de la información, debido a los múltiples riesgos y amenazas que hoy en día atentan contra la seguridad de la información, la protección y privacidad de los datos, es fundamental que las entidades implementen, conserven y optimicen de manera continua un sistema de gestión de seguridad de la información basado en los riesgos. La información es el activo más importante en todos los contextos, de igual manera es un recurso indispensable para el desarrollo, la toma de decisiones y el cumplimiento de la misionalidad de las organizaciones. La finalidad del presente documento es presentar el plan de seguridad y privacidad de la información con el fin de entender los pasos a realizar para la implementación de un modelo de seguridad y privacidad de la información (MSPI), su gestión a través del SGSI y que la corporación tenga una postura de seguridad.

## 1. OBJETIVOS

### 1.1. OBJETIVO GENERAL

Actualizar y ejecutar las directrices, políticas y estándares de seguridad de la información que permitan asegurar la protección constante y adecuada de los activos de información de la Corporación Autónoma Regional del Tolima – CORTOLIMA, a través de la comprensión de los objetivos de seguridad de la información y el soporte a las políticas presentadas en el presente documento, por parte de todos los funcionarios

### 1.2. OBJETIVOS ESPECÍFICOS

Realizar seguimiento al Modelo de Seguridad y Privacidad de la Información – MSPI, con el objetivo de garantizar la privacidad, confiabilidad e integridad de la información de la entidad.

Incrementar el nivel de madurez en la corporación frente a la gestión de la seguridad y privacidad de la información.

Garantizar la actualización en la Infraestructura Tecnológica de la Corporación con el ánimo de ajustar las necesidades en cuanto a capacidades, anchos de banda, tecnologías y soluciones que optimicen el acceso a los sistemas de información, servicios de red e internet de la Infraestructura de TI.

Ejecutar Gestión y Control sobre los incidentes de seguridad que se presenten a nivel del uso de los servicios de red e internet de la infraestructura de TI de la Corporación.

Garantizar la disponibilidad de la información crítica de la Corporación con respaldos eficientes en la Nube, que permitan mantener la continuidad de la información y el acceso a la misma de forma íntegra, veraz y actualizada.

Adoptar elementos de buenas prácticas que permitan mejorar los servicios y la atención de requerimientos y necesidades de TI a nivel de usuarios y la interacción con los entes gubernamentales externos, que garanticen la estabilidad y funcionalidad de los servicios de red e internet en la Corporación y la actualización de los marcos normativos que nos rigen, dentro del Sistema de Gestión de la Seguridad de la Información.

## 2. POLITICA DE SEGURIDAD DE LA INFORMACION

La corporación cuenta con la política de seguridad de la información aprobado por la Dirección General de la Corporación fue elaborado y revisado por los funcionarios que conforman el Comité de Seguridad de la Información. Los principios, políticas, estándares y demás lineamientos se evidencian a través del manual de seguridad de la información, se presentan mandatorios y de estricto cumplimiento como directriz de la Dirección General y se encuentra basadas en la Norma NTC/ISO IEC 17799 con su equivalente NTC/ISO/ IEC 27001,27002 como un marco de referencia para la gestión de la seguridad de la información en la corporación. La Norma ISO/IEC 27001 avala la adecuada implantación, gestión y operación de todo lo relacionado con un SGSI, siendo la norma más completa que existe en la implantación de controles, métricas e indicadores que permiten establecer un marco adecuado de gestión de la seguridad de la información para las organizaciones.

### TERMINOS Y DEFINICIONES

**Administración de Riesgos:** Se entiende por administración de riesgos al proceso de identificación, control y minimización o eliminación, a un costo aceptable, de los riesgos de seguridad que podría afectar a la información.

**Auditabilidad:** Define que todos los eventos de un sistema deben poder ser registrados para su control posterior

**Autenticidad:** Busca asegurar la validez de la información en tiempo, forma y distribución. Asimismo, se garantiza el origen de la información, validando el emisor para evitar suplantación de identidades.

**Confiability de la Información:** Es decir, que la información generada sea adecuada para sustentar la toma de decisiones y la ejecución de la misiones y funciones.

**Confidencialidad:** Se garantiza que la información se accesible solo a aquellas personas autorizadas a tener accesos a la misma.

**Disponibilidad:** Se garantiza que los usuarios autorizados tengan acceso a la información y a los recursos relacionados con la misma, toda vez que requieran.

**Evaluación de Riesgos:** Se entiende a la amenazas y vulnerabilidades relativas a la información y a las instalaciones de procesamiento de la misma. La probabilidad de que ocurran y su potencial impacto en la operatoria de la corporación.

**Información:** Se refiere a toda comunicación o representación de conocimiento como datos, en cualquier forma, con inclusión de formas textuales, numéricas, graficas cartográficas, narrativas o audiovisuales, y en cualquier medio, ya sea magnético, en pape, en pantallas de computadoras, audiovisual u otro.

**Incidente de Seguridad:** Un incidente de seguridad es un evento adverso en un sistema de computadoras, o red de computadoras, que compromete la confidencialidad, la integridad o disponibilidad, la legalidad y confiabilidad de la información. Puede ser causado mediante la explotación de alguna vulnerabilidad o un intento o amenazas de romper los mecanismos de seguridad existentes.

**Integridad:** Se salvaguarda la exactitud y totalidad de la información y los métodos de procesamiento.

**Legalidad:** Referido al cumplimiento de las leyes, normas, reglamentaciones o disposiciones a la que está sujeta la corporación.

**No repudio:** Se refiere a evitar que una entidad que haya enviado o recibido información alegue ante terceros que no la envió o recibió.

**Protección a la Duplicación:** Consiste en asegurar que una transacción solo se realiza una vez, a menos que se especifique lo contrario. Impedir que se grave una transacción para luego reproducirla, con el objeto de simular múltiples peticiones del mismo remitente original.

**Sistema de Información:** se refiere al Hardware y Software operado por la corporación o por terceros que procese información en su nombre, para llevar a cabo una función propia de la corporación, sin tener en cuenta la tecnología utilizada, ya se trate de computación de datos, telecomunicaciones u otro tipo.



Corporación Autónoma  
Regional del Tolima  
¡Siembra Tu Futuro!



### 3. MARCO NORMATIVO

TIPO DE NORMA	NUMERO	FECHA	TEMA RELACIONADO	TITULO	EXPEDIDO POR
Constitución Política		1991		Constitución Política de Colombia	Asamblea Nacional Constituyente
Ley	23	1982	Derechos de Autor	Sobre derechos de autor	Congreso de la Republica
Ley	44	1993	Derechos de Autor	por la cual se modifica y adiciona la Ley 23 de 1982 y se modifica la Ley 29 de 1944.	Congreso de la Republica
Ley	545	1999	Derechos de Autor	Por medio de la cual se aprueba el "Tratado de la OMPI - Organización Mundial de la Propiedad Intelectual- sobre Interpretación o Ejecución y Fonogramas (WPPT)", adoptado en Ginebra el veinte (20) de diciembre de mil novecientos noventa y seis (1996).	Congreso de la Republica
Ley	463	1998	Propiedad Industrial	Por medio de la cual se aprueba el "Tratado de cooperación en materia de patentes (PCT)", elaborado en Washington el 19 de junio de 1970, enmendado el 28 de septiembre de 1979 y modificado el 3 de febrero de 1984, y el reglamento del tratado de cooperación en materia de patentes.	Congreso de la Republica
Ley	527	1999	Comercio electrónico y firmas digitales	por medio de la cual se define y reglamenta el acceso y uso de	Congreso de la Republica



Corporación Autónoma  
Regional del Tolima  
¡Siembra Tu Futuro!

# SIEMBRA  
TU FUTURO

				los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones.	
Ley	565	2000	Derechos de Autor	por medio de la cual se aprueba el "Tratado de la OMPI – Organización Mundial de la Propiedad Intelectual– sobre Derechos de Autor (WCT)", adoptado en Ginebra, el veinte (20) de diciembre de mil novecientos noventa y seis (1996).	Congreso de la Republica
Ley	599	2000	Derechos de Autor	Por el cual se expide el código penal. Art. 199. Espionaje Art. 258. Utilización indebida de información, Art. 418. Revelación de Secreto, Art. 419. Utilización de asunto sometido a secreto o reserva, Art. 420. Utilización indebida de información oficial, Artículo 431. Utilización indebida de información obtenida en el ejercicio de la función pública, Artículo 463. Espionaje	Congreso de la Republica
Ley	603	2000	Derechos de Autor	Protección de los derechos de autor en Colombia.	Congreso de la Republica
Ley	1266	2008	Protección de los datos personales	Por la cual se dictan las disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y	Congreso de la Republica



				se dictan otras disposiciones.	
Ley	1273	2009	Protección de la información y datos personales	Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones.	Congreso de la Republica
Ley	1341	2009	Tecnologías de la información y datos personales	Por la cual se definen principios y conceptos sobre la sociedad de la información y la organización de las Tecnologías de la Información y las Comunicaciones – TIC–, se crea la Agencia Nacional de Espectro y se dictan otras disposiciones	Congreso de la Republica
Ley	1480	2011	Estatuto del consumidor	Por medio de la cual se expide el Estatuto del Consumidor y se dictan otras disposiciones.	Congreso de la Republica
Ley	1581	2012	Protección de los datos personales	Por la cual se dictan disposiciones generales para la protección de los datos personales.	Congreso de la Republica
Ley	1621	2013	Actividades de inteligencia y contrainteligencia	Por medio de la cual se expiden normas para fortalecer el marco jurídico que permite a los organismos que llevan a cabo actividades de inteligencia y contrainteligencia cumplir con su misión constitucional y legal y se dictan otras disposiciones	Congreso de la Republica
Ley	1712	2014	Ley de transparencia	Por medio de la cual se crea la ley de transparencia y del derecho de acceso a la información pública nacional y	Congreso de la Republica

				se dictan otras disposiciones	
Ley	1915	2018	Derechos de Autor	Disposiciones relativas al derecho de autor y los derechos conexos	Congreso de la República
Decreto	2591	2000	Propiedad Industrial	Por la cual se reglamenta parcialmente la Decisión 486 de la Comisión de la Comunidad Andina.	Ministerio de Desarrollo Económico
Decreto	1747	2000	Comercio electrónico y firmas digitales	por el cual se reglamenta parcialmente la Ley 527 de 1999, en lo relacionado con las entidades de certificación, los certificados y las firmas digitales.	Presidencia de la República
Decreto	2952	2000	Reglamentación parcial Ley 1266 de 2008	Por el cual se reglamentan los artículos 12 y 13 de la Ley 1266 de 2008	Presidencia de la República
Decreto	1377	2013	Datos personales	Por la cual se reglamenta parcialmente la Ley 1581 de 2012	Presidencia de la República
Decreto	886	2014	Registro nacional de base de datos	Por el cual se reglamenta el artículo 25 de la Ley 1581 de 2012	Presidencia de la República
Decreto	2573	2014	Gobierno en línea	Por el cual se establecen los lineamientos generales de la estrategia de gobierno en línea.	MINTIC
Resolución	26930	2000	Comercio electrónico y firmas digitales	"Por la cual se fijan los estándares para la autorización y funcionamiento de las entidades de certificación y sus auditores"	Superintendencia de la Industria y Comercio
Conpes	3854	2017	Política nacional de seguridad digital	Política nacional de seguridad digital	Departamento Nacional de Planeación
Conpes	3701	2011	Ciberseguridad	Lineamientos para la Política ciberseguridad y ciberdefensa	Departamento Nacional de Planeación
Decisión	486	2000	Propiedad Industrial	Régimen común sobre propiedad industrial	CAN (Comisión de la Comunidad Andina)
Circular	1	2000	Derechos de autor	Orientación para el cumplimiento de la Ley 603 del año 2000, vinculada con el derecho de autor.	Unidad Administrativa Especial Dirección Nacional de Derecho Autor.

#### 4. COMITÉ DE SEGURIDAD DE LA INFORMACION

El comité de Seguridad de la información, es un equipo de trabajo interdisciplinario que desarrolla labores de asesoría, definición de estándares, de coordinación, de control, en la formulación de políticas en materia de seguridad de la información. Creado mediante resolución 0393 del 10 de marzo de 2015 e integrado por:

Director general o su delegado, jefe de la oficina asesora de Direccionamiento Estratégico TIC o quien haga sus veces, subdirector administrativo y financiero o su delegado, subdirector de desarrollo ambiental sostenible o su delegado, subdirector de planificación ambiental y desarrollo sostenible o su delegado, subdirector de administración de recursos naturales o su delegado, subdirector jurídico o su delegado, jefe de la oficina asesora de planeación institucional y direccionamiento estratégico o su delegado y el jefe de la oficina de control interno.

Responsable de la seguridad Informática. Es el Servidor público que cumple las funciones de supervisar el cumplimiento de la presente Política y de asesorar en materia de seguridad de la información a los integrantes de la corporación que así lo requieran. Esta labor está a cargo del comité de seguridad de la información. Tanto el director como los subdirectores y jefes de oficina, son responsables de la implementación de esta política de seguridad de la información dentro de sus áreas de responsabilidad, así como del cumplimiento de dicha Política por parte de su equipo de trabajo. La política de Seguridad de la información es de aplicación obligatoria para todo el personal de la corporación, cualquiera que sea su vinculación, el área de trabajo y el nivel de las tareas que desempeñe.

Comité de Seguridad de la información. Procederá a revisar y proponer para su aprobación la política de Seguridad de la Información y las funciones generales en materia de seguridad de la información; monitorear cambios significativos en los riesgos que afectan a los recursos de información frente a las amenazas más importantes; tomar conocimiento y supervisar la investigación y monitoreo de los incidentes relativos a la seguridad.

## 5. IMPLEMENTACIÓN DEL PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Las acciones a realizar estarán enmarcadas en los siguientes elementos para garantizar la actualización y ejecución de las directrices, políticas y estándares de seguridad de la información que permitan asegurar la protección constante y adecuada de los activos de información de la Corporación Autónoma Regional del Tolima – CORTOLIMA, a través de la comprensión de los objetivos de seguridad de la información y el soporte a las políticas presentadas en el presente documento, por parte de todos los funcionarios:

- Infraestructura de Red a Nivel Físico
  - Documentación Infraestructura Tecnológica con el ánimo de garantizar procesos de administración, gestión y crecimiento de la misma, contando con elementos claros sobre la distribución, configuración y seguridad de los sistemas de información y servicios de red e internet para la Corporación.
  - Supervisar el adecuado funcionamiento de la Infraestructura de Interconexión e Internet de la Corporación; teniendo en cuenta procesos de actualización y estabilización de la conectividad y el acceso a los sistemas de información y los servicios de red e internet a cada una de las sedes y territoriales.
  - Actualizar Plan de Continuidad de la Infraestructura Tecnológica para contar con las mejores tecnologías y seguridad al momento del acceso e intercambio de información entre sedes y territoriales.
  
- Infraestructura de Red a Nivel Lógico
  - Documentación requerida para la continuidad de la Infraestructura Tecnológica a nivel Lógico, garantizando que en el futuro el crecimiento o cambios en la estructura de la corporación a nivel organizacional se actualicen bajo los mismos parámetros de confidenciales, privacidad y seguridad acorde a las Subdirecciones y áreas de la Corporación en la infraestructura de Red que se implementó.

- Análisis de Información Crítica para continuidad almacenada en las NAS (Almacenamiento en Red a nivel Local) que requiera Respaldo en la Nube, con el objetivo de optimizar el recurso de almacenamiento local y para garantizar el respaldo seguro y actualizado de la información de forma externa mediante soluciones de Respaldo en la Nube.
  - Implementación proyecto de Respaldo de la Información Crítica en la Nube consolidando un esquema de almacenamiento externo y seguro de la información más crítica de la Corporación basados en los objetivos misionales de la misma y garantizando procesos de continuidad y respaldo de la información institucional soportada en los sistemas de información, servicios de red e Internet.
  - Aseguramiento de la Integridad, Privacidad, Acceso, Consistencia y Seguridad de la Información Almacenada en la Nube para garantizar el acceso a la misma en momentos de requerirse ya sea por pérdidas de información o algún evento o incidente físico o de seguridad en la infraestructura de TI de la Corporación.
- Infraestructura de Seguridad
    - Aprobación de las Políticas para la Utilización de Servicios a nivel de Red e Internet, para la optimización del recurso de ancho de banda y rendimiento de los sistemas de información y el aseguramiento de los activos de información de la Corporación para prevenir compromisos en la información o indisponibilidad de los servicios de red e internet.
    - Implementar las Políticas para la Utilización de Servicios a nivel de Servicios de Red e Internet para regular el acceso a los servicios, aplicaciones y funcionalidades que los usuarios de la infraestructura de TI de la Corporación requieren con base a las funciones que cada uno desarrolla que apoyen los procesos misionales y operativos de la Corporación.
    - Actualización continua de las Políticas de Seguridad a Nivel de Servicios de Red e Internet como un proceso continuo de mejoramiento y con el ánimo de ser proactivos en la actualización y modificación de las políticas de acuerdo a los eventos o incidentes que se puedan presentar y como un proceso normal de actualización tecnológica en cuanto a servicios, posibles ataques e incidentes que se puedan presentar y que requieran de cambios en las políticas.

- Infraestructura de Gestión y Monitoreo de Red e Incidentes
  - Documentación de eventos ocurridos dentro del uso de la infraestructura de TI del Sistema Gestión y Monitoreo de Red
  - Documentación de Incidentes ocurridos dentro del uso de la infraestructura de TI del Sistema de Incidentes
  - Análisis y Evaluación de las causas generadoras de los Eventos e Incidentes
  - Actualización Políticas de Seguridad, Servicios de Red e Internet acorde a los requerimientos analizados
  - Proyección de Cambios en Infraestructura o Políticas de Seguridad con base a la base de Conocimiento generada por eventos e incidentes contenidos
  
- Infraestructura Sistema de Gestión de la Seguridad de la Información
  - Actualizar políticas de la Seguridad de la Información ISO 27002 garantizando optimización a las políticas actuales implementadas frente a nuevas disposiciones en el ámbito legal y normativo para los entes gubernamentales.
  - Adoptar y Documentar las buenas prácticas de Seguridad ISO/COBIT como estrategia en la implementación y optimización de los servicios ofrecidos en la infraestructura de TI, Red e Internet.
  - Análisis, Evaluación y Adopción de ITIL como guía de buenas prácticas para la gestión de servicios de tecnologías de la información (TI) como proceso de mejoramiento continuo y con el ánimo de articular los servicios tecnológicos con herramientas y estrategias actualizadas en el ámbito de las TICs.

## 6. IMPLEMENTACIÓN DEL PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION 2023						
GESTION	Nombre actividad	Fecha inicio	Duracion en días	Fecha final		
Optimización Infraestructura de Red y Seguridad de la Información	Infraestructura de Red a Nivel Físico	Documentación Infraestructura Tecnológica	1/02/2023	90	3/04/2023	
		Supervisar el adecuado funcionamiento de la Infraestructura de Interconexión e Internet de la Corporación	1/02/2023	330	31/12/2023	
		Actualizar Plan de Continuidad de la Infraestructura Tecnológica	1/02/2023	330	31/12/2023	
	Infraestructura de Red a Nivel Lógico	Documentación requerida para la continuidad de la Infraestructura Tecnológica a nivel Lógico	1/04/2023	90	30/06/2023	
		Análisis de Información Crítica para continuidad almacenada en las NAS (Almacenamiento en Red a nivel Local) que requiera Respaldo en la Nube	1/04/2023	90	30/06/2023	
		Implementación proyecto de Respaldo de la Información Crítica en la Nube	1/04/2023	90	30/06/2023	
		Aseguramiento de la Integridad, Privacidad, Acceso, Consistencia y Seguridad de la Información	1/04/2023	90	30/06/2023	
	Infraestructura de Seguridad	Aprobación de las Políticas para la Utilización de Servicios a nivel de Red e Internet	1/02/2023	330	30/03/2023	
		Implementar las Políticas para la Utilización de Servicios a nivel de Servicios de Red e Internet	1/04/2023	270	31/12/2023	
		Actualización continua de las Políticas de Seguridad a Nivel de Servicios de Red e Internet	1/04/2023	270	31/12/2023	
	Implementación Sistema de Gestión y Monitoreo de Red	Documentación de eventos ocurridos dentro del uso de la infraestructura de TI del Sistema de Gestión y Monitoreo de Red	1/04/2023	270	31/12/2023	
		Documentación de Incidentes ocurridos dentro del uso de la infraestructura de TI del Sistema de Gestión y Monitoreo de Red	1/04/2023	270	31/12/2023	
		Análisis y Evaluación de las causas generadoras de los Eventos e Incidentes	1/04/2023	270	31/12/2023	
		Actualización Políticas de Seguridad, Servicios de Red e Internet acorde a los requerimientos analizados	1/04/2023	270	31/12/2023	
		Proyección de Cambios en Infraestructura o Políticas de Seguridad con base a la base de Conocimiento generada por eventos e Incidentes	6/04/2022	30	31/12/2023	
	Ajustar Sistema de Gestión de la Seguridad de la Información	Actualizar políticas de la Seguridad de la Información ISO 27002	1/02/2023	90	31/12/2023	
		Adoptar y Documentar las buenas prácticas de Seguridad ISO/COBIT	1/02/2023	330	31/12/2023	
		Análisis, Evaluación y Adopción de ITIL como guía de buenas prácticas para la gestión de servicios de tecnologías de la información (TI) como proceso de mejoramiento continuo	1/02/2023	330	31/12/2023	