Plan de Seguridad y Privacidad de la Información

VERSION PRELIMINAR

Corporación Autónoma Regional del Tolima
¡Siembra Tu Futuro!

#SIEMBRA TU FUTURO

COMITÉ DE DIRECCIÓN CORTOLIMA

OLGA LUCIA ALFONSO LANNINI
Directora General CORTOLIMA

GUILLERMO AUGUSTO VALLEJO FRANCO
Subdirector de Desarrollo Ambiental

CARLOS ENRIQUE QUIROGA CALDERÓN
Subdirector de Planeación y Gestión Tecnológica

KATHERINE NIETO BARRERA
Subdirectora Administrativa y Financiera

WILLER ANDRÉS RODRÍGUEZ GARCÍA
Subdirector de Calidad Ambiental

JUAN CARLOS GUZMÁN CORTÉS
Jefe de la Oficina Asesora Jurídica

NUBIA YINERI MARTINEZ CUBILLOS
Asesora Oficina de Control Interno a la Gestión

DIRECTORES TERRITORIALES

OLGA LUCÍA OVIEDO VILLEGAS
Directora Territorial Oriente

JOSÉ GUILLERMO HERRERA GONZÁLEZ
Director Territorial Norte

DANILO ANDRÉS BRAVO
Director Territorial Sur

CARLOS ANDRÉS NAVARRO
Director Territorial Sur Oriente

Enero 2021

TABLA DE CONTENIDO

INTRODUCCIÓN

El Plan de Tratamiento 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

Comunicar 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

Brindar los pasos para la implementación y apropiación del Modelo de Seguridad y Privacidad de la Información – MSPI, con el objetivo de resguardar la información.

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

2. ALCANCE

Realizar una eficiente gestión de riesgos de Seguridad y Privacidad de la información, que permita integrar en los procesos de la corporación, buenas practicas que contribuyan a la toma de decisiones y prevenir incidentes que puedan afectar el logro de los objetivos. Se dan los lineamientos para poder identificar, analizar, tratar, evaluar y monitorear los riesgos de seguridad y privacidad de la información de la corporación. El Plan de Seguridad y Privacidad de la información identifica e incluye las alineaciones para la gestión del ciclo (PHVA) de operación del modelo de seguridad y privacidad de la información (MSPI), el cual debe ser aplicado sobre todos los procesos en la corporación y debe ser acatado por parte de todos los funcionarios de la entidad.

3. 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.
Confiabilidad 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. Pude 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 grabe 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.

4. 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

				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 Republica
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 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.

5. 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, subdirector administrativo y financiero o su delegado, subdirector de desarrollo ambiental o su delegado, jefe de oficina de planeación o quien haga sus funciones, jefe de oficina jurídica o su delegado, asesor de control interno, oficial de seguridad, profesional especializado y profesional universitario del área de recursos tecnológicos.

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. Todo director, 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.

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

GESTION	ACTIVIDADES	TAREAS	RESPONSABLES	FECHA DE PROGRAMACION	
				FECHA DE INICIO	FECHA FINAL
ACTIVOS DE LA FORMACION	Definir lineamientos para el levantamiento de activos de información	Actualización de metodologías e instrumento de levantamiento de activos de información	COMITÉ DE SEGURIDAD DE LA INFORMACION	01/03/2019	31/12/2022
	Levantamientos de activos de información	Revisión de la guía de activos de información	COMITÉ DE SEGURIDAD DE LA INFORMACION	01/03/2019	31/12/2022
		Mejoramiento de la guía de activos de la información	COMITÉ DE SEGURIDAD DE LA INFORMACION	01/03/2019	31/12/2022
		Identificación de los nuevos activos de información	COMITÉ DE SEGURIDAD DE LA INFORMACION	01/03/2019	31/12/2022
		Revisión de instrumentos de activos de información, cambios físicos de la ubicación de activos de información	COMITÉ DE SEGURIDAD DE LA INFORMACION	01/03/2019	31/12/2022
		Realizar correcciones a los instrumentos de activos de información, cambios físicos de la ubicación de activos de información	COMITÉ DE SEGURIDAD DE LA INFORMACION	01/03/2019	31/12/2022
		Actualización del informe de los activos de información, por novedades que se presenten en los procesos	COMITÉ DE SEGURIDAD DE LA INFORMACION	01/03/2019	31/12/2022
	Publicación de activos de información	Publicar los instrumentos de activos de información	COMITÉ DE SEGURIDAD DE LA INFORMACION	01/03/2019	31/12/2022
		Validar los activos para publicación	COMITÉ DE SEGURIDAD DE LA INFORMACION	01/03/2019	31/12/2022
		Consolidar los instrumentos de activos de la información	COMITÉ DE SEGURIDAD DE LA INFORMACION	01/03/2019	31/12/2022
	Reporte de datos personales	Verificar información recolectada, correspondiente a la base de datos	COMITÉ DE SEGURIDAD DE LA INFORMACION	01/03/2019	31/12/2022
Este documento, se realiza con las mejores prácticas de la ISO27001 desarrollado por el comité de seguridad de la información y certificado por ICONTEC.					