Plan de Tratamiento de Riesgos 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

1. INTRODUCCION

El Plan de Tratamiento de Riesgo se define con el fin de evaluar las posibles acciones que se deben tomar para mitigar los riesgos existentes, estas acciones son organizadas en forma de medias de seguridad, y para cada una de ellas se define el nombre de la medida, objetivo, justificación, responsable de la medida y su prioridad. Mediante la definición del Plan de Tratamiento de Riesgos se busca mitigar los riesgos presentes en el análisis de riesgos como: perdida de la confidencialidad de los activos, perdida de Integridad de los activos y perdida de disponibilidad de los activos; evitando aquellas situaciones que impidan el logro de los objetivos. Debemos contar con una buena gestión de la seguridad de la información, para la Corporación autónoma regional del Tolima CORTOLIMA, de no hacerlo puede traer consecuencias graves, como pérdida fuga o robo de información, alteración de documentos, negación de servicios etc.

2. DEFINICIONES

Activo: Bienes, recursos o derechos que tenga valor para una organización.

Activo de Información: Toda la información que maneja con la que cuenta una organización para un correcto funcionamiento.

Amenazas: Cualquier evento, persona, situación o fenómeno que pueda causar daño.

Análisis de brechas: es una herramienta de análisis para comparar el estado y desempeño real de una organización, estado o situación en un momento dado.

Análisis de Riesgo: Método empleado para evaluar los riesgos informáticos y obtener respuesta de peligro.

Control o Medida: acciones o mecanismos definidos para prevenir o reducir el impacto de los eventos que ponen en riesgo, la adecuada ejecución de las actividades y tareas requeridas para el logro de objetivos de los procesos de una entidad.

Evento: Acción que puedo haber causado daño, pero fue controlado.

Gestión del Riesgo Informáticos: Actividades empleadas para mitigar los riesgos informáticos.

Impacto: Daño que provoca la materialización de una amenaza.

Incidente de seguridad informática: daño que puede comprometer las operaciones de la corporación.

Información: Conjunto de datos que tienen un significado.

MSPI: Modelo de seguridad y privacidad de la información

PHVA: Planear, hacer, verificar, actuar.

Probabilidad: Posibilidad de que una amenaza se materialice

Riesgo: Probabilidad de ocurrencia de una amenaza.

Seguridad de la información: Se Ocupa de evaluar el riesgo y las amenazas, traza el plan de acción y esquemas normativos. Es la línea estratégica de las Seguridad.

Seguridad informática: Se ocupa de la implementación técnica y de la operación para la protección de la información.

SGSI: Sistema de Gestión de seguridad de la Información

Vulnerabilidades: Falla o debilidad en un sistema que puede ser explotada por quien la conozca.

3. OBJETIVOS

3.1. OBJETIVO GENERAL

Aminorar los riesgos informáticos en CORTOLIMA, mediante la aplicación de la norma ISO 27001.

3.2. OBJETIVOS ESPECÍFICOS

- Identificar la ubicación y responsables de los activos de información a través del inventario del mismo.
- Valorar y Categorizar los activos de información.
- Establecer los controles y políticas de la seguridad de la información que garantice la confidencialidad integridad y disponibilidad de la información.
- Adaptar y fortalecer el conocimiento referente a la gestión de riesgos Seguridad y Privacidad de la información

4. 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 Tratamiento de Riesgo tendrá en cuenta los riesgos que se encuentren en los niveles Alto y Extremo acorde con los lineamientos definidos por la corporación, Los riesgos que se ubiquen en una zona de riesgo “Bajo” no requieren de acciones de control, serán aceptados por la Entidad.

5. MARCO REFERENCIAL

POLÍTICA DE ADMINISTRACION DE RIESGOS

La Corporación Autónoma Regional del Tolima " CORTOLIMA" define su política de Administración del Riesgo, teniendo como base los lineamientos en el marco del Modelo Integrado de Planeación y Gestión – MIPG, así como los del Modelo de Control Interno, en lo referente a las líneas de Defensa, los lineamientos de la Guía administración del riesgo y diseño de controles sector público DAFP 2018, la cual unificó la metodología existente para la administración del riesgo de gestión y corrupción, con el fin de hacer más sencilla la utilización de esta herramienta gerencial para las entidades públicas y así evitar duplicidad o reprocesos, haciendo más evidente la importancia de fortalecer la metodología para diseñar y aplicar controles que permitan asegurar el logro de los objetivos Corporativos. Se unificaron los criterios en cuanto la Identificación de los riesgos con todas las dependencias para que fuera más sencillo la identificación, el análisis, la valoración y el tratamiento a los riesgos, así como lo constituye los lineamientos de la Función Pública brindando una seguridad razonable frente al logro de los objetivos Corporativos. Para administrar adecuadamente los riesgos CORTOLIMA acata la metodología propia y determina las acciones para asumir, reducir y mitigar el riesgo al igual que establece planes de contingencia ante la materialización del riesgo.

La política identifica las opciones para tratar y manejar los riesgos basados en su valoración, permiten tomar decisiones adecuadas y fijar los lineamientos para administración de los mismos; a su vez, transmiten la posición de la dirección y establecen las guías de acción necesarias a todos los colaboradores de la corporación.

6. METODOLOGÍA

El Plan de Tratamiento de Riesgos contempla la definición de las actividades a desarrollar en aras de mitigar los riesgos sobre los activos.

6.1. DESARROLLO METODOLÓGICO

FASES	ACTIVIDAD	TAREA	RESPONSABLES	FECHA DE INICIO	FECHA DE FIN
FASE 1	Definir el alcance	Establecer los objetivos, justificación del procedimiento que se va a	PLANEACION Y GESTION TECNOLOGICA	1/1/2018	1/03/2018

		realizar, los funcionarios implicados y el contexto de seguridad informática con el que cuenta la corporación.			
FASE 2	Identificación de activos	El principal activo de la corporación es la información en sí, la cual puede estar en forma física como documentos impresos o escritos a mano, en medios electrónicos almacenados en discos duros externos, memorias USB o en forma digital, en los equipos de cómputo o en la nube. toda esta información requiere ser analizada para su protección.	PLANEACION Y GESTION TECNOLOGICA	02/03/2018	02/06/2018
FASE 3	Identificación de riesgos	El objetivo de la identificación de riesgos es conocer los incidentes o eventos que pueden causar pérdidas o alteración en el funcionamiento de la corporación y pueden afectar la confidencialidad, integridad y disponibilidad de la información.	PLANEACION Y GESTION TECNOLOGICA	02/06/2018	02/09/2018

FASE 4	Identificación de amenazas	Una amenaza se identifica como un evento, persona, situación o fenómeno que pueda causar daño a los activos de la organización. las amenazas pueden ser de origen humano o ambientales.	PLANEACION Y GESTION TECNOLOGICA	02/092018	02/10/2018
FASE 5	Identificación de vulnerabilidades	Las vulnerabilidades son las fallas o debilidades en un sistema, que puede ser explotada por quien la conozca. cuando la amenaza encuentra la vulnerabilidad es cuando se crea el riesgo. por eso es necesario conocer la lista de amenazas y el inventario de activos de información	PLANEACION Y GESTION TECNOLOGICA	02/10/2018	02/11/2018

FASE 6	Identificación de controles	La identificación de los controles existentes permite realizar la evaluación de riesgos. lo controles garantizan que al momento de la materialización de un riesgo se reduzcan o mitiguen los riesgos informáticos y la organización funcionen correctamente. pero se debe tener en cuenta que nunca se va a estar 100% seguros. Dada la importancia de los controles, con que cuenta la corporación no es adecuado exponerlos en el proyecto, por lo que se pueden crear perfiles de ataque.	PLANEACION Y GESTION TECNOLOGICA	02/11/2018	02/12/2018
FASE 7	Evaluación de riesgo	La evaluación de riesgo se realiza con enfrentamiento entre la probabilidad de ocurrencia y el impacto que genera el riesgo en los activos de información, dado por la matriz de calificación, evaluación y respuestas a los riesgos.	PLANEACION Y GESTION TECNOLOGICA	02/01/2019	02/03/2019

FASE 8	Valoración de controles	La valoración de controles, evalúa los controles existentes en la organización y la efectividad para mitigar la exposición al riesgo.	PLANEACION Y GESTION TECNOLOGICA	02/03/2019	02/08/2019

Fase 2: Identificación de activos

A continuación, se comparte un formato de inventario de activos de información que contiene los siguiente:

Nombre del funcionario
Función que realiza el funcionario

TIPO DOCUMENTAL:

Nombre del activo de información / Nombre correspondiente al activo de información como Base de Datos, Actas, informes, Sistemas de información etc.

Descripción del activo de información

TIPOLOGÍA:

Software / el activo de información se encuentra en forma digital
Hardware/ el activo de información se encuentra en física
Servicios / el activo de información se emplea como servicio a terceros
Descripción del soporte

TIPO DE SOPORTE (medio de conservación y/o Soporte):
Análogo / Copia adicional del documento en forma física
Digital / Copia de seguridad en otro equipo, en correo electrónico o en la Nube.
Electrónico / Copia de seguridad en equipo electrónico como Disco Duro Externo USB.

Presentación de la información (formato o extensión) / en que aplicación se realiza el activo de información Ej. PDF, DOC, XLS, PowerPoint, etc.

Clasificación del activo de información

Nivel del Criterio: Confidencialidad, Integridad, Disponibilidad

Estado de la información

Localización del documento o del activo de información
Publicada en
Área/Dependencia
Observaciones

<table>
<tr><td rowspan="2"></td><td colspan="5">Nombre del funcionario</td></tr>
<tr><td colspan="5">Función que realiza el funcionario</td></tr>
<tr><td>TIPO DOCUMENTAL</td><td colspan="3">Nombre del activo de información / Nombre correspondiente al activo de información como Base de Datos, Actas, informes, Sistemas de información etc.</td><td colspan="2">Descripción del activo de información</td></tr>
<tr><td rowspan="4">TIPOLOGÍA</td><td colspan="5">Software / el activo de información se encuentra en forma digital</td></tr>
<tr><td colspan="5">Hardware/ el activo de información se encuentra en física</td></tr>
<tr><td colspan="5">Servicios / el activo de información se emplea como servicio a terceros</td></tr>
<tr><td colspan="5">Descripción del soporte</td></tr>
<tr><td rowspan="6">TIPO DE SOPORTE (medio de conservación y/o Soporte):</td><td colspan="5">Análogo / Copia adicional del documento en forma física</td></tr>
<tr><td colspan="5">Digital / Copia de seguridad en otro equipo, en correo electrónico o en la Nube.</td></tr>
<tr><td colspan="5">Electrónico / Copia de seguridad en equipo electrónico como Disco Duro Externo USB.</td></tr>
<tr><td colspan="5">Presentación de la información (formato o extensión)</td></tr>
<tr><td>PDF</td><td>DOC</td><td>XLS</td><td>PowerPoint</td><td>Otros</td></tr>
<tr><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td rowspan="2">Clasificación del activo de información</td><td colspan="5">Nivel del Criterio</td></tr>
<tr><td>Confidencialidad</td><td colspan="2">Integridad</td><td colspan="2">Disponibilidad</td></tr>
</table>

Estado de la información	
Localización del documento o del activo de información	
Publicada en	
Área/Dependencia	
OBSERVACIONES	

Nivel del Criterio: Confidencialidad		
Nivel	**Descripción Criterio de Confidencialidad**	**Denominación**
0	Información que puede ser conocida y utilizada sin autorización por cualquier persona, sea empleado de la corporación o no	Publico
1	Información que puede ser conocida y utilizada por todos los empleados de la corporación y algunas entidades externas debidamente autorizadas, y cuya divulgación o uso no autorizados podría ocasionar riesgos o pérdidas leves para la corporación, el Sector Público Nacional o terceros.	Reservada – Uso Interno
2	Información que sólo puede ser conocida y utilizada por un grupo de empleados, que la necesiten para realizar su trabajo, y cuya divulgación o uso no autorizados podría ocasionar pérdidas significativas a corporación o a terceros.	Reservada - Confidencial
3	Información que sólo puede ser conocida y utilizada por un grupo muy reducido de empleados, generalmente de la alta dirección de la corporación, y cuya divulgación o uso no autorizados podría ocasionar pérdidas graves al mismo o a terceros.	Reservada Secreta

Nivel del Criterio: Integridad	
Nivel	**Descripción Criterio de Integridad**
0	Información cuya modificación no autorizada puede repararse fácilmente, o no afecta la operatoria de la corporación.
1	Información cuya modificación no autorizada puede repararse, aunque podría ocasionar pérdidas leves para la corporación o terceros
2	Información cuya modificación no autorizada es de difícil reparación y podría ocasionar pérdidas significativas para la corporación o terceros.
3	Información cuya modificación no autorizada no podría repararse, ocasionando pérdidas graves a la corporación o a terceros.

Nivel del Criterio: Disponibilidad	
Nivel	**Descripción Criterio de Disponibilidad**
0	Información cuya inaccesibilidad no afecta la operatoria de la corporación.
1	Información cuya inaccesibilidad permanente durante una semana podría ocasionar pérdidas significativas para la corporación o terceros.
2	Información cuya inaccesibilidad permanente durante un día podría ocasionar pérdidas significativas a la corporación o a terceros.
3	Información cuya inaccesibilidad permanente durante una hora podría ocasionar pérdidas significativas a la corporación o a terceros.

Fase 3: Identificación de riesgos

El objetivo de la identificación de riesgos es conocer los incidentes o eventos que pueden causar pérdidas o alteración en el funcionamiento de la corporación.

RIESGOS INFORMÁTICOS	CAUSAS	EFECTO
Copia con errores o no verificada	Fallas en las comunicaciones	Restauración fallida, perdidas de información relevante para la continuidad del negocio
Publicación de información errónea	Falta de verificación de la oficina de comunicaciones y del líder la actividad	Demandas en contra de la entidad y pérdida de credibilidad

Error de información enviada por parte de los supervisores	Parametrización de usuarios erróneos Deficiencia en los controles legales y técnicos asignación de perfiles no requeridos	Usuarios creados con error o asignaciones de roles no permitidos
Equipo en mal funcionamiento o instalación de software ilegal	Desconocimiento del procedimiento y licenciamiento de la entidad	Mal funcionamiento de los equipos o problemas legales por falta de licenciamiento
Fallas en comunicación	Parametrización errada monitoreo ineficiente, oportunidad escaza	Servicios inactivos Funcionarios desatendidos, continuidad del negocio deficiente
Ataques Informáticos	Estimulo o Reto personal, rebelión, ánimo de lucro, espionaje	Daño en los equipos tecnológicos, incidente en la confidencialidad, integridad y disponibilidad de la información, denegación de servicios, secuestro de la información
Daño en los equipos tecnológicos	Manejo inadecuado de los equipos, falta de mantenimiento o mala conexión de los mismos en las instalaciones eléctricas, falta de equipos de potenciación, fallas por defectos de fábrica, derrame de líquido	Perdida de información, Perdidas de los quipos informáticos, Indisponibilidad del Servicio, traumatismos en los procesos
Robo, Perdida o Fuga de Información	Ataques cibernéticos internos o externos, Empleados no capacitados en los temas de riesgos informáticos, Prestar los equipos informáticos a personal no autorizado, No cerrar sesión cuando se desplaza del puesto, Fallas en el proceso de copia de respaldo o de restauración de la información, o pérdida de la misma.	Pérdida o fuga de información, afectación parcial o total de la continuidad de las operaciones de los servicios del Incumplimiento normativo

Fase 4: Identificación de amenazas

<u>Una amenaza es una situación</u> potencial de un incidente no deseado, el cual puede ocasionar daño a un sistema o a una organización.

AMENAZA	TIPO
Polvo, Corrosión	Evento Naturales
Inundación	Evento Naturales
Incendios	Evento Naturales

Fenómenos Sísmicos	Evento Naturales
Fenómenos Térmicos	Evento Naturales y Daños físicos
Perdida en el suministro de energía	Daño Físico
Espionaje remoto	Acciones no autorizadas
Ingeniería Social	Acciones no autorizadas
Intrusión	Acciones no autorizadas
Accesos forzados al sistema	Acciones no autorizadas
Manipulación del Hardware	Acciones no autorizadas
Manipulación con Software	Acciones no autorizadas
Fallas del equipo	Fallas técnicas
Saturación del sistema de información	Fallas técnicas

Fase 5: Identificación de vulnerabilidades

Las vulnerabilidades son las Fallas o debilidades en un sistema, que puede ser explotada por quien la conozca.

VULNERABILIDADES	DESCRIPCIÓN
Fácil acceso a las dependencias	No hay un control para el acceso de las personas no autorizadas a las secretarías.
Falta de Capacitación de los funcionarios en temas de seguridad Informática.	El eslabón más débil en términos de seguridad informática en una organización son los funcionarios, dado que no tienen conocimiento sobre las amenazas y riesgos que enfrentan y como poder mitigarlos.

Fase 6: Identificación de controles

La identificación de los controles existentes permite realizar la evaluación de riesgos.

Fase 7: Evaluación de riesgo

La evaluación de riesgo se realiza con enfrentamiento entre la probabilidad y el impacto que genera el riesgo en los activos de información, dado por la matriz de calificación, evaluación y respuestas a los riesgos.

TABLA DE PROBABILIDAD			
NIVEL	**D E S C R I P TO R**	**D E S C R I P C I Ó N**	**F R E C U E N C I A**
5	**Casi seguro**	Se espera que el evento ocurra en la mayoría de las circunstancias.	Más de 1 vez al año.
4	**Probable**	Es viable que el evento ocurra en la mayoría de las circunstancias.	Al menos 1 vez en el último año.
3	**Posible**	El evento podrá ocurrir en algún momento.	Al menos 1 vez en los últimos 2 años.
2	**Improbable**	El evento puede ocurrir en algún momento.	Al menos 1 vez en los últimos 5 años.
1	**Rara vez**	El evento puede ocurrir solo en circunstancias excepcionales (poco comunes o anormales).	No se ha presentado en los últimos 5 años.

TABLA DE IMPACTO		
NIVEL	**IMPACTO** **Consecuencias (Cuantitativo)**	**IMPACTO** **Consecuencias (Cualitativo)**
CATASTRÓFICO	* Impacto que afecte la ejecución presupuestal en un valor ≥50%. * Pérdida de cobertura en la prestación de los servicios de la entidad ≥50%. * Pago de indemnizaciones a terceros por acciones legales que pueden afectar el presupuesto total de la entidad en un valor ≥50%. * Pago de sanciones económicas por incumplimiento en la normatividad aplicable ante un ente regulador, las cuales afectan en un valor ≥50% del presupuesto general de la entidad.	* Interrupción de las operaciones de la entidad por más de cinco (5) días. * Intervención por parte de un ente de control u otro ente regulador. * Pérdida de información crítica para la entidad que no se puede recuperar. * Incumplimiento en las metas y objetivos institucionales afectando de forma grave la ejecución presupuestal. * Imagen institucional afectada en el orden nacional o regional por actos o hechos de corrupción comprobados.
MAYOR	* Impacto que afecte la ejecución presupuestal en un valor ≥20%. * Pérdida de cobertura en la prestación de los servicios de la entidad ≥20%. * Pago de indemnizaciones a terceros por acciones legales que pueden afectar el presupuesto total de la entidad en un valor ≥20%. * Pago de sanciones económicas por incumplimiento en la normatividad aplicable ante un ente regulador, las cuales afectan en un valor ≥20% del presupuesto general de la entidad.	* Interrupción de las operaciones de la entidad por un (1) día. * Reclamaciones o quejas de los usuarios que podrían implicar una denuncia ante los entes reguladores o una demanda de largo alcance para la entidad. * Inoportunidad en la información, ocasionando retrasos en la atención a los usuarios. * Reproceso de actividades y aumento de carga operativa. * Imagen institucional afectada en el orden nacional o regional por retrasos en la prestación del servicio a los usuarios o ciudadanos. * Investigaciones penales, fiscales o disciplinarias.
MODERADO	* Impacto que afecte la ejecución presupuestal en un valor ≥5%. Pérdida de cobertura en la prestación de los servicios de la entidad ≥10%. * Pago de indemnizaciones a terceros por acciones legales que pueden afectar el pre- supuesto total de la entidad en un valor ≥5%.	* Interrupción de las operaciones de la entidad por un (1) día. * Reclamaciones o quejas de los usuarios que podrían implicar una denuncia ante los entes reguladores o una demanda de largo alcance para la entidad.

	* Pago de sanciones económicas por incumplimiento en la normatividad aplicable ante un ente regulador, las cuales afectan en un valor ≥5% del presupuesto general de la entidad.	* Inoportunidad en la información, ocasionando retrasos en la atención a los usuarios. * Reproceso de actividades y aumento de carga operativa. * Imagen institucional afectada en el orden na- cional o regional por retrasos en la prestación del servicio a los usuarios o ciudadanos. * Investigaciones penales, fiscales o disciplinarias.
MENOR	* Impacto que afecte la ejecución presupuestal en un valor ≥1%. * Pérdida de cobertura en la prestación de los servicios de la entidad ≥5%. * Pago de indemnizaciones a terceros por acciones legales que pueden afectar el presupuesto total de la entidad en un valor ≥1%. * Pago de sanciones económicas por incumplimiento en la normatividad aplicable ante un ente regulador, las cuales afectan en un valor ≥1% del presupuesto general de la entidad.	* Interrupción de las operaciones de la entidad por algunas horas. * Reclamaciones o quejas de los usuarios, que implican investigaciones internas disciplinarias. * Imagen institucional afectada localmente por retrasos en la prestación del servicio a los usuarios o ciudadanos.
INSIGNIFICANTE	* Impacto que afecte la ejecución presupuestal en un valor ≥0,5%. * Pérdida de cobertura en la prestación de los servicios de la entidad ≥1%. * Pago de indemnizaciones a terceros por acciones legales que pueden afectar el presupuesto total de la entidad en un valor ≥0,5%. * Pago de sanciones económicas por incumplimiento en la normatividad aplicable ante un ente regulador, las cuales afectan en un valor ≥0,5% del presupuesto general de la entidad.	* No hay interrupción de las operaciones de la entidad. * No se generan sanciones económicas o administrativas. * No se afecta la imagen institucional de forma significativa.

IMPACTO DEL RIESGO						
MAPA DE CALOR		IMPACTO				
		INSIGNIFICANTE 1	MENOR 2	MODERADO 3	MAYOR 4	CATASTROFICO 5
PROBABILIDAD	CASI SEGURO 5			15	20	25
	PROBABLE 4			12	16	20
	POSIBLE 3			9	12	15
	IMPROBABLE 2			6	8	10
	RARA VEZ 1			3	4	5

BAJO	
MODERADO	
ALTO	
EXTREMO	

Matriz de calificación, evaluación y respuestas a los riesgos

ADMINISTRACIÓN DEL RIESGO
COPIA CONTROLADA

Código: F_EV_002 | Versión: 08 | Pág.: _ de _

IDENTIFICACION DEL RIESGO								ANALISIS DE CALIFICACION Y VALORACION (RIESGO INHERENTE)				EVALUACION DE CONTROLES Y DETERMINACIÓN DE RIESGO RESIDUAL					PLAN DE TRATAMIENTO DE RIESGOS							EVALUACION Y SEGUIMIENTO	
(1) TIPO DE PROCESO	(2) PROCESO	(3) SUBPROCESO	(4) ACTIVIDAD	(5) TIPOLOGÍA DEL RIESGO	(6) RIESGO	(7) CAUSA	(8) CONSECUENCIA	(9) PROBABILIDAD	(10) IMPACTO (INHERENTE)	(11) CALIFICACIÓN (# * 9)	(12) ZONA DE RIESGO (INHERENTE)	(14) CONTROLES	(14) PROBABILIDAD	(15) IMPACTO (RESIDUAL)	(16) CALIFICACIÓN (# * 15)	(17) ZONA DE RIESGO (RESIDUAL)	(18) TRATAMIENTO DEL RIESGO	(19) ACCIONES DE CONTROL	(20) EVIDENCIA DEL CONTROL	(21) ESTADO DE IMPLEMENTACIÓN	(22) PRIORIZACIÓN PARA LA IMPLEMENTA	(23) TIEMPO ESTIMADO DE LA IMPLEMENTA	(24) RESPONSABLE DE LA ACCION DE	(25) MONITOREO REVISION	(26) PLAN DE MEJORAMIE
SEGUIMIENTO Y MEJORA	PLANEACION Y GESTION TECNOLOGICA	GESTION TECNOLOGICA	Admon Copias De Seguridad	RIESGO DE SEGURIDAD DE LAINFORMACION	Copia con errores o no verificada	Fallas en las comunicaciones	Restauracion fallida, perdidas de informacion relevante para la continuidad del negocio	3	3	9	ALTO	Verificacion aleatoria de las copias de seguridad	1	3	3	BAJO	ACEPTAR	NA	NA	NA	NA	NA	NA		
SEGUIMIENTO Y MEJORA	PLANEACION Y GESTION TECNOLOGICA	GESTION TECNOLOGICA	Admon Sitio Web	RIESGO DE IMAGEN O REPUTACIONAL	Publicacion de informacion errorenea	Falta de verificacion de la oficina de comunicaciones y deficiente actividad	Demandas encontra de la entidad y perdida de credibilidad	2	3	6	MODERADO	Revicion por equipo editor y líder de la actividad de todos los	1	2	2	BAJO	ACEPTAR	NA	NA	NA	NA	NA	NA		
SEGUIMIENTO Y MEJORA	PLANEACION Y GESTION TECNOLOGICA	GESTION TECNOLOGICA	Admon Cuentas De Usuario	RIESGO DE SEGURIDAD DE LAINFORMACION	Error de informacion enviada por parte de los supervisores	Parametrizacion de usuarios erroneos Deficiencia en los controles legales y tecnicos asignacion de perfiles no requeridos	Usuarios creados con error o asignaciones de roles no permitidos	3	4	12	ALTO	Verificacion de los servicio solicitados posterior de	1	3	3	BAJO	ACEPTAR	NA	NA	NA	NA	NA	NA		
SEGUIMIENTO Y MEJORA	PLANEACION Y GESTION TECNOLOGICA	GESTION TECNOLOGICA	Mantenimiento Hardware Y Software	RIESGO DE SEGURIDAD DE LAINFORMACION	Equipo en mal funcionamiento o instalacion de software ilegal	Desconocimiento del procedimiento y licenciamiento de la entidad	Mal funcionamiento de los equipos o problemas legales por falta de licenciamiento	3	3	9	ALTO	Personal capacitado Verificacion de equipos	2	3	6	MODERADO	ACEPTAR	NA	NA	NA	NA	NA	NA		
SEGUIMIENTO Y MEJORA	PLANEACION Y GESTION TECNOLOGICA	GESTION TECNOLOGICA	Trabajo en Casa Por confinamiento	RIESGO OPERATIVO	Fallas en comunicacion	Parametrizacion errada monitoreo ineficiente oportunidad escaza	Servicios inactivos Funcionarios desalentdidos, continuidad del negocio deficiente	3	3	9	ALTO	Somos equipos para trabajo en casa, calan de internet	2	3	6	MODERADO	ACEPTAR	NA	NA	NA	NA	NA	NA		

Nota: Los riesgos que se ubiquen en una zona de riesgo “Bajo” no requieren de acciones de control. Para los riesgos anticorrupción se realizará teniendo en cuenta solamente los niveles moderado, mayor y catastrófico, dado que estos riesgos siempre serán significativos, en este orden de ideas, no aplican los niveles de impacto insignificante y menor, que sí aplican para los demás riesgos.

Fase 8: Valoración de controles

Se deben enumerar los controles que se han implementado para tratar el riesgo inherente. Estos controles deben: a) Tener un responsable, b) Ejecutar con periodicidad, c) Un propósito, d) Documentado.

Planear: Dentro de esta etapa se desarrollan las actividades definidas en las fases 1, 2, 3, 4 y 5.

Hacer: En este paso del ciclo de vida se desarrollarán las actividades enmarcadas en las fases 6, 7 y 8 de la metodología del tratamiento de riesgos.

Verificar: En esta etapa se desarrollarán las actividades que permiten hacer seguimiento o auditorías a la ejecución de cada una de las medidas.

Actuar: Dentro de esta etapa se realizarán las mejoras teniendo en cuenta el seguimiento y los resultados de las auditorías de la ejecución de los proyectos.

7. Oportunidad de Mejora

La corporación no solo deberá centrarse en los riesgos identificados, sino que este análisis o apreciación del riesgo debe ser la base para identificar oportunidades. Por lo anterior la oportunidad deberá entenderse como la consecuencia positiva frente al resultado del tratamiento del Riesgo.

8. Recursos

La Corporación dispone de los siguientes recursos humanos y financieros representados en el presupuesto de la entidad.

Profesional Universitario Especializado Gestión Tecnológica – Ing Félix Baena

Profesional Universitario Gestión Tecnológica – Juan Darío Sandarriaga

Contratista – Auditor ISO 27001 – Oscar Fernando Ramos Benavides

Contratista – Ingeniero de Sistemas Implementación de Controles – Hugo Martínez

Profesional Especializado – Sistema Integrado de Gestión – José Moreno Leal

Presupuesto

CONTRATOS GESTION TECNOLOGICA 2019 Y 2020	
2020	Servicio de canal de dedicado, internet y hosting para CORTOLIMA. Con corte hasta noviembre de 2020. (5 Canales, 1 Hosting, 1 Servidor de Correo)
	Compra de 320 licencias de GDATA ENDPOINT PROTECTIÓN ENTERPRISE. (1 Protección Antivirus)
	Contrato de Prestación de servicios como apoyo a la gestión de TICs (Helpdesk Nivel 1 y 2 y apoyo a la dirección)
	Contrato de Prestación de servicios como apoyo soporte a IPUSA
	Contrato de licenciamiento de Argis
	Contrato de Prestación de servicios como apoyo al desarrollo de software
	Licenciamiento de Gsuit (Correo Electrónico)
	Definir y diseñar el PETIC
	Mantenimiento al software administrativo y financiero
	Alquiler de impresoras
2019	Contrato de Prestación de servicios como apoyo a la gestión de TICs (Helpdesk Nivel 1 y 2 y apoyo a la dirección)
	Contrato de Prestación de servicios como apoyo soporte a IPUSA a los municipios
	Actualización y mantenimiento del software IPUSA
	Compra de 320 licencias de GDATA ENDPOINT PROTECTIÓN ENTERPRISE. (1 Protección Antivirus)
	Servicio de canal de dedicado, internet y hosting para CORTOLIMA. Con corte hasta noviembre de 2020. (5 Canales, 1 Hosting, 1 Servidor de Correo)
	LA COMPRA DE EQUIPOS Y SOFTWARE PARA CONTINUIDAD DEL SERVICIO y PARA APOYAR, MEJORAR Y APOYAR LOS SUBPROCESOS DE LA CORPORACION AUTONOMA REGIONAL DEL TOLIMA - CORTOLIMA.
	ADMINISTRACIÓN, MANTENIMIENTO Y SOPORTE TÉCNICO DEL SITIO WEB DE LA CORPORACIÓN AUTÓNOMA REGIONAL DEL TOLIMA - CORTOLIMA WWW.CORTOLIMA.GOV.CO.
	Mantenimiento al software administrativo y financiero (Adición Contrato del 2018)
	Alquiler de impresoras