PLAN DE TRATAMIENTO DE RIESGO DE SEGURIDAD DE LA INFORMACION

UNIMOS EMPRESA MUNICIPAL DE TELECOMUNICACIONES DE IPIALES S.A. E.S.P.

2022

Carrera 5 No. 12 -04 · (+57) 2 7732333
www.unimosesp.com.co - unimos@unimosesp.com.co
Ipiales, Nariño, Colombia

Empresa Municipal de Telecomunicaciones de Ipiales S.A. E.S.P.	**UNIMOS EMPRESA MUNICIPAL DE TELECOMUNICACIONES DE IPIALES S.A. E.S.P.**	Hablamos con hechos

PLAN DE TRATAMIENTO DE RIESGO DE SEGURIDAD DE LA INFORMACION - 2022		
ELABORÓ	**REVISÓ**	**APROBÓ**
Javier Salazar Betancourt	Jose David Lafaurie Ponce	Diana Isabel Obando Guerrero
Jefe de Operaciones Digitales	Jefe Oficina Asesora de Planeación	UNIMOS S.A. E.S.P.
FECHA	**FECHA**	**FECHA**
14/01/2022	18/01/2022	25/01/2022

REGISTRO DE MODIFICACIONES
Actualización de lineamientos al Plan de Desarrollo Municipal “Hablamos con Hechos”.
Actualización a reestructuración organizacional Decisión 003 de 2021
Actualización de metas medidas por indicadores de gestión

TABLA DE CONTENIDO

1. INTRODUCCIÓN

El plan de tratamiento de Riesgos de Seguridad y Privacidad de la información, Seguridad Digital y Continuidad de la Operación, se basa en una orientación estratégica que requiere el desarrollo de una cultura de carácter preventivo, de manera que, al comprender el concepto de riesgo, así como el contexto, se planean acciones que reduzcan la afectación a la entidad en caso de materialización, adicional se busca desarrollar estrategias para la identificación, análisis, tratamiento, evaluación y monitoreo de dichos riesgos con mayor objetividad, dando a conocer aquellas situaciones que pueden comprometer el cumplimiento de los objetivos trazados en el Entorno TIC para el Desarrollo Digital, ciudadanos y hogares empoderados del Entorno Digital, Transformación Digital Sectorial y Territorial e Inclusión Social Digital.

Lo anterior dando cumplimiento a la normativa establecida por el estado colombiano, CONPES 3854 de 2016, Modelo de Seguridad y Privacidad de MINTIC y lo establecido en el decreto 1008 de 14 de junio 2018, adoptando las buenas prácticas y los lineamientos de los estándares ISO 27001:2013, ISO 31000:2018 y la guía para la administración del riesgo y el diseño de controles en entidades públicas - Riesgos de gestión, corrupción y seguridad digital - Versión 4 emitida por el DAFP.

2. OBJETIVOS

2.1. Objetivo General.

Generar el Plan de Tratamiento de Riesgos de Seguridad de Información como una guía metodológica alineada al instructivo para la Gestión del Riesgo (E-IN-005), que permita a los responsables de los procesos de UNIMOS Empresa de Telecomunicaciones de Ipiales S.A. E.S.P., gestionar los riesgos que en materia de seguridad y privacidad de la información.

2.2. Objetivos Específicos.

- ✓ Identificar los riesgos asociados a los procesos y los activos de información que hacen parte del alcance del SGSI.
- ✓ Calcular el nivel de riesgo.
- ✓ Establecer el plan de tratamiento de riesgos.
- ✓ Fortalecer y apropiar conocimiento referente a la gestión de riesgos Seguridad y Privacidad de la información, Seguridad Digital y Continuidad de la Operación.
- ✓ Realizar seguimiento y control a la eficacia del Plan de Tratamiento de Riesgos de Seguridad de la Información.

3. MARCO LEGAL

NORMA	DESCRIPCIÓN
Decreto 1078 de 2015	Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones.
Decreto 1008 de 2018	Por el cual se establecen los lineamientos generales de la política de Gobierno Digital y se subroga el capítulo 1 del título 9 de la parte 2 del libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones.
CONPES 3854 de 2016	Política Nacional de Seguridad Digital
Manual para la Implementación de la Política de Gobierno Digital	Implementación de la política de Gobierno Digital. Decreto 1008 de 2018 (Compilado en el Decreto 1078 de 2015, capítulo 1, título 9, parte 2, libro 2) Versión 7, abril de 2019
Modelo de Seguridad y privacidad de la información - MSPI	Se encuentra alineado con el Marco de Referencia de Arquitectura TI y soporta transversalmente los otros componentes de la Política de Gobierno Digital, TIC para el Estado y TIC para la Sociedad. TIC, que son habilitados por tres elementos transversales: Seguridad de la Información, Arquitectura y Servicios Ciudadanos Digitales
NTC / ISO 27001:2013	Tecnología de la información. Técnicas de seguridad. Sistemas de gestión de la seguridad de la información (SGSI).
NTC/ISO 31000:2009	Gestión del Riesgo. Principios y directrices.
Guía para la administración del riesgo y el diseño de controles en entidades públicas – Versión 4	Riesgos de Gestión, Corrupción y Seguridad Digital Función Pública octubre 2018

Fuente: Diseño propio del autor.

4. ALCANCE

Realizar una eficiente gestión de riesgos de Seguridad y Privacidad de la información, Seguridad Digital y Continuidad de la Operación, que permita integrar en los procesos de la entidad, buenas prácticas que contribuyan a la toma de decisiones y prevenir incidentes que puedan afectar el logro de los objetivos. Junto con Guía de Gestión de Riesgos de Seguridad y Privacidad de la Información (MinTIC: 2016), se dan los lineamientos para poder identificar, analizar, tratar, evaluar y monitorear los riesgos de seguridad y privacidad de la información en MinTIC.

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 el Ministerio TIC, los riesgos que se encuentren en niveles inferiores serán aceptados por la empresa.

5. TERMINOLOGÍA

- **Administración del Riesgo:** Conjunto de elementos de control que al Interrelacionarse brindan a la entidad la capacidad para emprender las acciones necesarias que le permitan el manejo de los eventos que puedan afectar negativamente el logro de los objetivos institucionales y protegerla de los efectos ocasionados por su ocurrencia.
- **Activo de Información:** En relación con la seguridad de la información, se refiere a cualquier información o elemento de valor para los procesos de la Organización.
- **Análisis de Riesgos:** Es un método sistemático de recopilación, evaluación, registro y difusión de información necesaria para formular recomendaciones orientadas a la adopción de una posición o medidas en respuesta a un peligro determinado.

  Proceso para comprender la naturaleza del riesgo y determinar el nivel de riesgo. (ISO/IEC 27000)
- **Amenaza:** Es la causa potencial de una situación de incidente y no deseada por la organización

- **Causa:** Son todo aquello que se pueda considerar fuente generadora de eventos (riesgos). Las fuentes generadoras o agentes generadores son las personas, los métodos, las herramientas, el entorno, lo económico, los insumos o materiales entre otros.
- **Confidencialidad:** Propiedad de la información de no ponerse a disposición o ser revelada a individuos, entidades o procesos no autorizados.
- **Consecuencia:** Resultado de un evento que afecta los objetivos.
- **Criterios del Riesgo:** Términos de referencia frente a los cuales la importancia de un riesgo se evaluada.
- **Control:** Medida que modifica el riesgo. Las políticas, los procedimientos, las prácticas y las estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido.
- **Declaración de aplicabilidad:** Documento que enumera los controles aplicados por el Sistema de Gestión de Seguridad de la Información – SGSI, de la organización tras el resultado de los procesos de evaluación y tratamiento de riesgos y su justificación, así como la justificación de las exclusiones de controles del anexo A de ISO 27001.
- **Disponibilidad:** Propiedad de la información de estar accesible y utilizable cuando lo requiera una entidad autorizada.
- **Evaluación de Riesgos:** Proceso de comparación de los resultados del análisis del riesgo con los criterios del riesgo, para determinar si el riesgo, su magnitud o ambos son aceptables o tolerables.
- **Evento:** Un incidente o situación, que ocurre en un lugar particular durante un intervalo de tiempo específico.
- **Estimación del Riesgo:** Proceso para asignar valores a la probabilidad y las consecuencias de un riesgo.
- **Evitación del Riesgo:** Decisión de no involucrarse en una situación de riesgo o tomar acción para retirarse de dicha situación.

- **Factores de Riesgo:** Situaciones, manifestaciones o características medibles u observables asociadas a un proceso que generan la presencia de riesgo o tienden a aumentar la exposición, pueden ser internos o externos a la entidad.
- **Gestión del Riesgo:** Actividades coordinadas para dirigir y controlar una organización con respecto al riesgo, se compone de la evaluación y el tratamiento de riesgos.
- Identificación del riesgo: Proceso para encontrar, enumerar y caracterizar los elementos de riesgo.
- **Incidente de seguridad de la información:** Evento único o serie de eventos de seguridad de la información inesperados o no deseados que poseen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información (Confidencialidad, Integridad y Disponibilidad).
- **Integridad:** Propiedad de la información relativa a su exactitud y completitud.
- **Impacto:** Cambio adverso en el nivel de los objetivos del negocio logrados.
- **Nivel de riesgo:** Magnitud de un riesgo o de una combinación de riesgos, expresada en términos de la combinación de las consecuencias y su posibilidad.
- **Matriz de Riesgos:** Instrumento utilizado para ubicar los riesgos en una determinada zona de riesgo según la calificación cualitativa de la probabilidad de ocurrencia y del impacto de un riesgo.
- **Monitoreo:** Mesa de trabajo anual, la cual tiene como finalidad, revisar, actualizar o redefinir los riesgos de seguridad de la información en cada uno de los procesos, partiendo del resultado de los seguimientos y/o hallazgos de los entes de con trol o las diferentes auditorías de los sistemas integrados de gestión.
- **Plan de tratamiento de Riesgos:** Documento que define las acciones para gestionar los riesgos inaceptables en el marco de la seguridad de la información e implantar los controles necesarios para proteger la misma.

- **Parte interesada (Stakeholder):** Persona u organización que puede afectar a, ser afectada por, o percibirse a sí misma como afectada por una decisión o actividad.
- **Propietario del Riesgo:** Persona o entidad con la responsabilidad de rendir cuentas y la autoridad para gestionar un riesgo.
- **Proceso:** Conjunto de actividades interrelacionadas que apuntan a un objetivo o que interactúan para transformar una entrada en salida.
- **Riesgo en la seguridad de la información:** Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias.
- **Riesgo Inherente:** Es el nivel de riesgo propio de la actividad, sin tener en cuenta el efecto de los controles.
- **Riesgo Residual:** El riesgo que permanece tras el tratamiento del riesgo o nivel resultante del riesgo después de aplicar los controles.
- **Reducción del Riesgo:** Acciones que se toman para disminuir la probabilidad las consecuencias negativas, o ambas, asociadas con un riesgo.
- **Retención del Riesgo:** Aceptación de la pérdida o ganancia proveniente de un riesgo particular. Seguridad de la información: Preservación de la confidencialidad, integridad y disponibilidad de la información.
- **Seguimiento:** Mesa de trabajo semestral, en el cual se revisa el cumplimiento del plan de acción, indicadores y metas de riesgo y se valida la aplicación n de los controles de seguridad de la información sobre cada uno de los procesos.
- **Tratamiento del Riesgo:** Proceso para modificar el riesgo" (Icontec Internacional, 2011).
- **Valoración del Riesgo:** Proceso global de identificación del riesgo, análisis del riesgo y evaluación de los riesgos.

- **Vulnerabilidad:** Debilidad de un activo o control que puede ser explotada por una o más amenazas.

6. RESPONSABLE

El responsable de presentar el Plan de Tratamiento del Riesgo de Seguridad de la Información, y actualizarlo cada vez que se produzcan las mismas, corresponde al Jefe de la Oficina de Operaciones Digitales de la Empresa Municipal de Telecomunicaciones de Ipiales Unimos S.A E.S.P. o a quien haga sus veces.

7. CRONOGRAMA

El Plan de Tratamiento de Riesgos contempla la definición de las actividades a desarrollar en aras de mitigar los riesgos sobre los activos, estas actividades se estructuraron de la siguiente manera, siguiendo las recomendaciones de la Guía de Gestión de Riesgos de Seguridad y Privacidad de la Información.

GESTION	ACTIVIDAD	TAREA	AREAS RESPONSABLES	FECHA DE INICIO	FECHA DE FINALIZACION
Gestión del Riesgo	Generación y aprobación de lineamientos de tratamiento de riesgos de seguridad y privacidad de la información	Actualizar política y metodología de gestión de riesgos	Oficna Asesora de Planeación	Enero	Febrero
	Sensibilización	Socialización de guía y herramientas de gestión de riesgos de seguridad y privacidad de la información	Oficna Asesora de Planeación	Marzo	Marzo
	Identificación de riegos de privacidad y seguridad de la información	Identificación, análisis y evaluación de riesgos	Subgerencia Técnica Oficna de Operaciones Digitales	Marzo	Abril
		Realimentación, revisión y verificación de los riesgos identificados	Subgerencia Técnica Oficna de Operaciones Digitales	Abril	Mayo
	Aceptación de riesgo identificados	Aceptación, aprobación de riesgos identificados y plan de tratamiento	Oficna Asesora de Planeación Subgerencia Técnica Oficna de Operaciones Digitales	Mayo	Mayo
	Publicación	Publicación de matriz de riesgos	Oficna Asesora de Planeación Oficina de Sistemas y Facturación	Junio	Junio
	Seguimiento fase de tratamiento	Seguimiento planes de tratamiento de riesgos identificados y verificación de evidencias	Oficna Asesora de Planeación Subgerencia Técnica Oficna de Operaciones Digitales	Junio	Diciembre
	Evaluación de riesgos residuales	Evaluación de riesgos residuales	Oficna Asesora de Planeación Subgerencia Técnica Oficna de Operaciones Digitales	Junio	Diciembre
	Mejoramiento	Identificación de oportunidades de mejora de acuerdo a la evaluación de riesgos residuales	Subgerencia Técnica Oficna de Operaciones Digitales	Junio	Diciembre
		Creación/actualización de guía de gestión de riesgos de privacidad de seguridad de la información	Subgerencia Técnica Oficna de Operaciones Digitales	Junio	Diciembre
	Monitoreo y revisión	Generación presentación y reportes	Subgerencia Técnica Oficna de Operaciones Digitales	Junio	Diciembre

8. RECURSOS

La estimación y asignación de los recursos para el plan de tratamiento de riesgos de Seguridad de la Información identificados en la entidad, corresponderá al dueño del riesgo, quien es el responsable de contribuir con el seguimiento y control de la gestión, además de la implementación de los controles definidos en el plan de tratamiento.

Si el establecimiento de los controles implica la adquisición de herramientas tecnológicas se deberá exponer el Análisis de la Necesidad desde la Oficina de Operaciones Digitales, describiendo los equipos y características necesarias para la mitigación del riesgo.

9. INDICADORES

La medición se realiza con un indicador de gestión que está orientado principalmente a disminuir el número de riesgos identificados con nivel alto y externo a través de la implementación y evaluación de controles.

El número de riesgos identificados como no aceptables no debe ser superior al 20% del total de riesgos identificados.

La Oficina de Operaciones Digitales asesora a las áreas en el proceso de identificación y valoración de los riesgos de seguridad de información y seguridad digital, los líderes de las áreas solicitarán a la Oficina asesora de planeación la inclusión de los mismos en el mapa de riesgos institucional, instrumento en donde se registran los riesgos identificados, su valoración y sus controles, para su seguimiento y control.

La Oficina de Operaciones Digitales apoyará a los responsables de las áreas en la definición de los controles y hará seguimiento a su implementación, con el fin, de evidenciar en el siguiente ciclo la efectividad de los controles implementados y en consecuencia la disminución del riesgo No aceptable.

Así mismo, si se llegan a presentar incidentes de seguridad se validarán los riesgos identificados para determinar si obedece a un riesgo identificado y proceder a valorar, recalificar e implementar nuevos controles.