Empresa Municipal de Telecomunicaciones de Ipiales S.A. E.S.P.
NIT: 900292948-3

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN 2020

Tabla de contenido

1. INTRODUCCIÓN

Uno de los activos más valiosos y primordiales para cualquier tipo de organización es la información, de ahí la importancia de que esta se mantenga de forma segura, garantizando su integridad, confidencialidad y disponibilidad, lo que implica la necesidad de tener una adecuada gestión de los recursos con el objeto de controlar su debido acceso, el tratamiento y uso de la misma.

Si bien la seguridad absoluta sobre la información es imposible y existen una gran diversidad de amenazas sobre las organizaciones, las mismas han establecido medidas que han permitido mantener en salvaguarda este activo. Para ello, es indispensable velar por los recursos que mejoren las medidas de seguridad orientadas a prevenir y detectar los riesgos que atenten contra la seguridad y privacidad de la información.

Consciente de que la seguridad y privacidad de la información es fundamental para garantizar su debida gestión financiera, administrativa y operativa Unimos Empresa Municipal de Telecomunicaciones de Ipiales S.A. E.S.P. establecerá un marco normativo que contemple las políticas con responsabilidades y obligaciones frente a la seguridad y privacidad de la información.

El presente documento contiene el plan de seguridad y privacidad de la información establecido para el año 2020

2. OBJETIVO GENERAL DEL PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Establecer las actividades que están contempladas en el Modelo de Seguridad y Privacidad de la Información, alineadas con la NTC/IEC ISO 27001:2013, la Política de Seguridad Digital y Continuidad del servicio, en el Mapa de Procesos del Ministerio de Tecnologías de la Información y las Comunicaciones – MINTIC

2.1. OBJETIVOS ESPECÍFICOS DEL PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Identificar el estado actual de Unimos S.A. E.S.P. frente a los requerimientos del Modelo de Seguridad y Privacidad de la Información.

Continuar con la construcción del plan de seguridad y privacidad de la información, usando una metodología de gestión de los riesgos conexo a todos los procesos de la empresa.

Definir los lineamientos para la implementación del Plan de Seguridad y Privacidad de la Información.

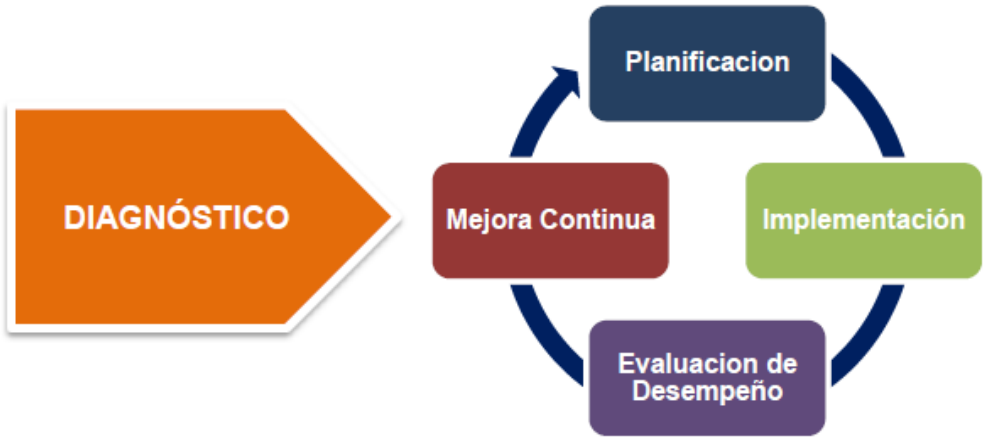
Establecer los métodos de seguimiento y monitoreo mediante la definición de indicadores para el Plan de Seguridad y Privacidad de la Información

Definir el método de consolidación de los resultados obtenidos para establecer el plan de mejoramiento continuo.

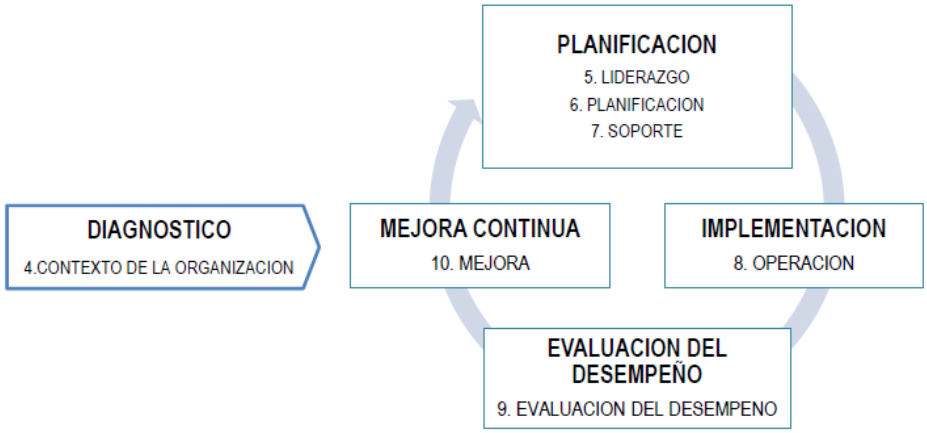
3. METODOLOGÍA DE IMPLEMENTACIÓN DE MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

3.1. CICLO DE OPERACIÓN

El Modelo de Seguridad y Privacidad de la Información establece objetivos, metas y herramientas (guías) que permiten que la seguridad y privacidad de la información sea un sistema de gestión sostenible dentro de las entidades, todo esto contenido en un ciclo de operación de cinco fases



3.2. ALINEACIÓN NORMA ISO 27001:2013 VS CICLO DE OPERACIÓN



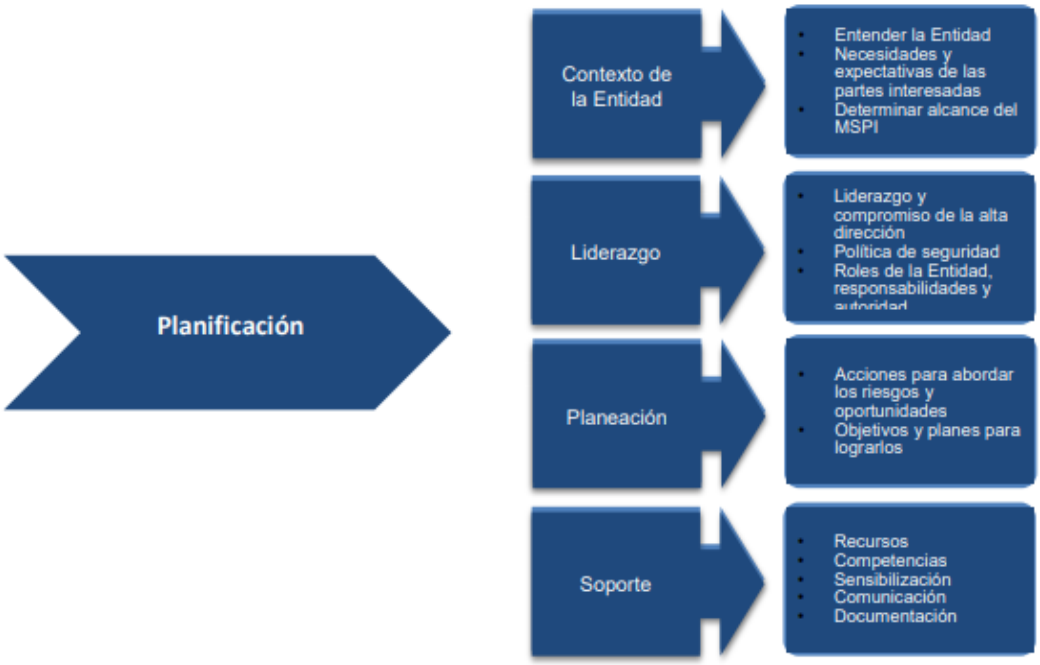
4. Contexto organizacional		Entendimiento de la Organización y su contexto Expectativas de las partes interesadas Alcances del SGSI
5. Liderazgo	PLAN	Liderazgo y compromiso de la Alta Dirección Políticas Organización de los roles, responsables y autoridades
6. Planificación		Como abordar riesgos y oportunidades
7. Soporte		Recursos, competencias, concientización, comunicación, información documentada
8. Operación	DO	Plan de tratamiento de riesgos Implementar el plan y documentar los resultados
9. Evaluación de funcionamiento del SGSI	CHECK	Plan de seguimiento, medición, análisis y evaluación Planear y realizar auditorías internas del SGSI Revisiones regulares de la Alta Dirección
10. Mejoras y acciones Correctivas	ACT	No conformidad y acciones correctivas Mejora continua del SGSI

4. FASE DE DIAGNÓSTICO

En esta fase se pretende identificar el estado actual de la organización con respecto a los requerimientos del MSPI.

DIAGNÓSTICO			
METAS	PRODUCTO / ACTIVIDADES	INSTRUMENTOS	ALINEACIÓN ISO 27001:2013
Determinar el estado actual de la gestión de seguridad y privacidad de la información al interior de la Entidad.	Diligenciamiento de la herramienta. Diagnóstico de la situación actual. Diagnóstico del nivel de cumplimiento. Valoración del estado actual.	Instrumento de identificación de línea de base de seguridad. Instructivo para el diligenciamiento de herramienta. Guía No 1 - Metodología de pruebas de	CAP 4. CONTEXTO DE LA ORGANIZACIÓN
Identificar el nivel de madurez de seguridad y privacidad de la información en la Entidad	Diligenciamiento de la herramienta. Diagnóstico del nivel de madurez de seguridad y privacidad de la información.	Instrumento de identificación de línea de base de seguridad. Instructivo para el diligenciamiento de herramienta. Guía No 1 - Metodología de pruebas de efectividad.	
Identificar vulnerabilidades técnicas y administrativas que sirvan como insumo para la fase de planificación.	Diligenciamiento de la herramienta. Diagnóstico de vulnerabilidades.	Instrumento de identificación de línea de base de seguridad. Instructivo para el diligenciamiento de herramienta. Guía No 1 - Metodología de pruebas de efectividad.	

5. FASE DE PLANIFICACIÓN



PLANIFICACIÓN			
METAS	PRODUCTO / ACTIVIDADES	INSTRUMENTOS	ALINEACIÓN ISO 27001:2013
Política de Seguridad y Privacidad de la Información	Documento con la política de seguridad de la información, debidamente aprobado por la alta Dirección y socializada al interior de la Entidad. Manual con las políticas de seguridad y privacidad de la información, debidamente aprobadas por la alta dirección y socializadas al interior de la Entidad.	Guía No 2 – Política General MSPI	CAP 5: LIDERAZGO CAP 6: PLANIFICACIÓN CAP 7: SOPORTE
Procedimientos de seguridad de la información.	Procedimientos, debidamente documentados, socializados y aprobados por el comité que integre los sistemas de gestión institucional.	Guía No 3 - Procedimientos de Seguridad y Privacidad de la Información	
Roles y responsabilidades de seguridad y privacidad de la información.	Acto administrativo a través del cual se crea o se modifica las funciones del comité gestión institucional (o el que haga sus veces), en donde se incluyan los temas de seguridad de la información en la entidad, revisado y aprobado por la alta Dirección, deberá designarse quien será el encargado de seguridad de la información dentro de la entidad.	Guía No 4 - Roles y responsabilidades de seguridad y privacidad de la información.	
Inventario de activos de información.	Documento con la metodología para identificación, clasificación y valoración de activos de información, validado por el comité de seguridad de la información o quien haga sus veces y revisado y aprobado por la alta dirección. Matriz con la identificación, valoración y clasificación de activos de información. Documento con la caracterización de activos de información, que contengan datos personales Inventario de activos de IPv6	Guía No 5 - Gestión De Activos Guía No 20- Transición Ipv4 a Ipv6	
Integración del MSPI con el Sistema de Gestión documental	Documento de Integración del MSPI, con el sistema de gestión documental de la entidad	Guía No 6 - Gestión Documental	
Identificación, Valoración y tratamiento de riesgo.	Documento con la metodología de gestión de riesgos. Documento con el análisis y evaluación de riesgos. Documento con el plan de tratamiento de riesgos. Documento con la declaración de aplicabilidad. Documentos revisados y aprobados por la alta Dirección.	Guía No 7 - Gestión de Riesgos Guía No 8 - Controles de Seguridad	
Plan de Comunicaciones.	Documento con el plan de comunicación, sensibilización y capacitación para la entidad.	Guía No 14 - Plan de comunicación, sensibilización y capacitación	
Plan de diagnóstico de IPv4 a IPv6.	Documento con el Plan de diagnóstico para la transición de IPv4 a IPv6	Guía No 20- Transición IPv4 a IPv6	

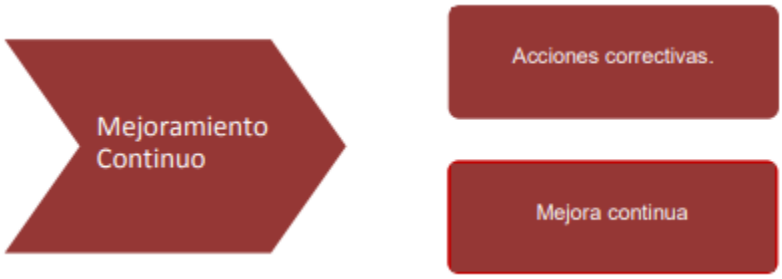
6. FASE DE IMPLEMENTACIÓN

IMPLEMENTACIÓN			
METAS	PRODUCTO / ACTIVIDADES	INSTRUMENTOS	ALINEACIÓN ISO 27001:2013
Planificación y Control Operacional.	Documento con la estrategia de planificación y control operacional, revisado y aprobado por la alta Dirección.	Documento con el plan de tratamiento de riesgos. Documento con la declaración de aplicabilidad.	CAP 8: OPERACIÓN
Implementación del plan de tratamiento de riesgos.	Informe de la ejecución del plan de tratamiento de riesgos aprobado por el dueño de cada proceso.	Documento con la declaración de aplicabilidad. Documento con el plan de tratamiento de riesgos.	
Indicadores De Gestión.	Documento con la descripción de los Indicadores de gestión de seguridad y privacidad de la información.	Guía No 9 - Indicadores de Gestión SI.	
Plan de Transición de IPv4 a IPv6	Documento con las estrategias del plan de implementación de IPv6 en la entidad, aprobado por la Oficina de TI.	Documento con el Plan de diagnóstico para la transición de IPv4 a IPv6. Guía No 20- Transición de IPv4 a IPv6 para Colombia. Guía No 19– Aseguramiento del Protocolo IPv6.	

7. FASE DE EVALUACIÓN DE DESEMPEÑO

EVALUACIÓN DE DESEMPEÑO			
METAS	PRODUCTO / ACTIVIDADES	INSTRUMENTOS	ALINEACIÓN ISO 27001:2013
Plan de revisión y seguimiento, a la implementación del MSPI.	Documento con el plan de seguimiento y revisión del MSPI revisado y aprobado por la alta Dirección.	Guía No 16– Evaluación del desempeño.	CAP 9: EVALUACIÓN DE DESEMPEÑO
Plan de Ejecución de Auditorias	Documento con el plan de ejecución de auditorías y revisiones independientes al MSPI, revisado y aprobado por la Alta Dirección.	Guía No 15– Guía de Auditoría	

8. MEJORA CONTINUA



MEJORA CONTINUA			
METAS	PRODUCTO / ACTIVIDADES	INSTRUMENTOS	ALINEACIÓN ISO 27001:2013
Plan de mejora continua	Documento con el plan de mejoramiento. Documento con el plan de comunicación de resultados.	Resultados de la ejecución del Plan de Revisión y Seguimiento, a la Implementación del MSPI. Resultados del plan de ejecución de auditorías y revisiones independientes	CAP 10: MEJORA

9. IMPLEMENTACIÓN PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

ACTIVIDAD	2020											
	ENERO	FEBRERO	MARZO	ABRIL	MAYO	JUNIO	JULIO	AGOSTO	SEPTIEMBRE	OCTUBRE	NOVIEMBRE	DICIEMBRE
DIAGNIOSTICO												
METAS												
Determinar el estado actual de la gestión de seguridad y privacidad de la información al interior de la Entidad.												
Identificar el nivel de madurez de seguridad y privacidad de la información en la Entidad												
Identificar vulnerabilidades técnicas y administrativas que sirvan como insumo para la fase de planificación.												
PLANIFICACIÓN												
METAS												
Generar y/o verificar y aprobar la política de seguridad de la información.												
Generar y/o verificar y aprobar el manual de políticas de seguridad de la información.												
Generar y/o verificar, documentar y socializar los procedimientos de seguridad de la información.												
Generar el acto administrativo que define los roles y responsabilidades de SPI.												
Documetar la metodología de identificación, clasificación y valoración de activos de inf.												
Generar la matriz con la identificación, clasificación y valoración de activos de inf												
Documentar la caracterización de los activos de la información que contengan datos personales												
Generar un inventario de activos IPV6												
Generar documento de integración de MSPI con el sistema de gestion documental.												
Documentar la metodología de gestión de riesgos												
Documentar el analisis y la evaluacion de riesgos												
Documentar el plan de tratamiento de riesgos												
Documentar la declaracion de aplicabilidad												
Documentar el plan de comunicación, sensibilizacion y capacitacion												
Documentar el Plan de diagnóstico para la transición de IPv4 a IPv6.												
IMPLEMENTACIÓN												
METAS												
Documentar la estrategia de planificación y control operacional												
Implementar del plan de tratamiento de riesgos.												
Imlementar medidas objetivos de control Anexo A ISO 27001												
Implementar procedimientos de gestion de eventos e incidentes de seguridad												
Ejecutar plan de capacitación y sensibilización de seguridad												
Verificar indicadores de gestion del SGSI												
Implementar el plan de transición de IPV4 a IPV6												
EVALUACIÓN DE DESEMPEÑO												
METAS												
Ejecutar el plan de revisión y seguimiento a la implementación del MSPI												
Ejecutar el plan de ejecución de auditorias												
MEJORA CONTINUA												
METAS												
Diseñar plan de mejora continua												