Empresa Regional Aguas del Tequendama S.A. E.S.P.
Anapoima – La Mesa.

Política seguridad digital ERAT

La Mesa, 2023

Sede Administrativa y PQR:
Diagonal 8 No. 1 – 37 Barrio Quintas de San Pablo
La Mesa, Cundinamarca. Teléfono 8471213
usuario@aguasdeltequendama.com
info@aguasdeltequendama.com

Oficina PQR Anapoima - Cundinamarca. Carrera 3 # 1- 41 Sur San José
Celular PQR 3142807615
pqranapoima@aguasdeltequendama.com
www.aguasdeltequendama.com

MODELO INTEGRADO DE PLANEACION Y GESTION
EMPRESA REGIONAL AGUAS DEL TEQUENDAMA S.A. E.S.P.

Dimensión: GESTIÓN CON VALORES PARA RESULTADOS
Política Corporativa: POLÍTICA DE SEGURIDAD DIGITAL
Versión: 01

FECHA DE APROBACIÓN	APROBADO POR	VERSION
15 DE Marzo del 2023	Comité Institucional de gestión del desempeño 01 de 2023	01

DESCRIPCIÓN

En la Empresa Regional Aguas del Tequendama S.A. E.S.P. estamos comprometidos en identificar, gestionar, tratar y mitigar los riesgos de seguridad digital en las actividades socioeconómicas que realiza la empresa en el entorno digital, con el fin preservar la confidencialidad, privacidad e integridad de todos los activos de información de la entidad.

JUSTIFICACIÓN

La implementación de la política de Seguridad Digital se realiza acorde a lo indicado en el Manual Operativo del Modelo Integrado de Planeación y Gestión MIPG v.4 Capitulo III Articulo 3.2.1.3, con el fin de salvaguardar toda la información almacenada producto de la actividad de la empresa ante cualquier ataque cibernético.

ALCANCE

Esta política aplica a todos los procesos que se desarrollan en la entidad por ende los empleados de libre nombramiento y remoción, empleados con contrato a término indefinido y fijo, personas vinculadas como aprendices en modalidad contrato de aprendizaje, pasantías y contrato de prestación de servicios personales. En general todas aquellas personas naturales y jurídicas que realicen cualquier actividad en la empresa.

DIRECTRICES MIPG

Las directrices de esta política se encuentran enmarcadas en:

Conforme lo indica el ámbito de aplicación del Decreto 1078 de 2015 respecto a la estrategia de Gobierno Digital -GD-, las entidades públicas deben realizar la implementación del Modelo de Seguridad y Privacidad de la Información -MSPI- con el objetivo de conformar un Sistema de Gestión de Seguridad de la Información al interior de la entidad. El MSPI integra en cada una de sus fases tareas asociadas a la gestión de

riesgos de seguridad digital, ya que esta práctica constituye su base fundamental. La guía para la gestión del riesgo de función pública, junto con el presente Anexo, llevarán a cumplir dichas tareas de gestión de riesgo de seguridad digital requeridas en el MSPI.

En esencia, la interacción entre ambos modelos puede resumirse de la siguiente manera:

1. Las actividades de identificación de activos, identificación, análisis, evaluación y tratamiento de los riesgos se alinean con la fase de PLANIFICACIÓN del MSPI.

2. Las actividades de implementación de los planes de tratamiento de riesgos se alinean con la fase de IMPLEMENTACIÓN del MSPI.

3. Las actividades de monitoreo y revisión, revisión de los riesgos residuales, efectividad de los planes de tratamiento o los controles implementados y auditorías se alinean con la fase de MEDICIÓN DEL DESEMPEÑO del MSPI.

4. Las actividades de MEJORAMIENTO CONTINUO en ambos modelos son similares y trabajan simultáneamente, ya que dependerán de las fases de Medición del Desempeño para identificar aspectos a mejorar en la aplicación de ambos Modelos. A continuación, se ilustra en que acciones del MPSI se tendrá interacción directa con el Modelo de Gestión de Riesgos de Seguridad Digital (MGRSD):

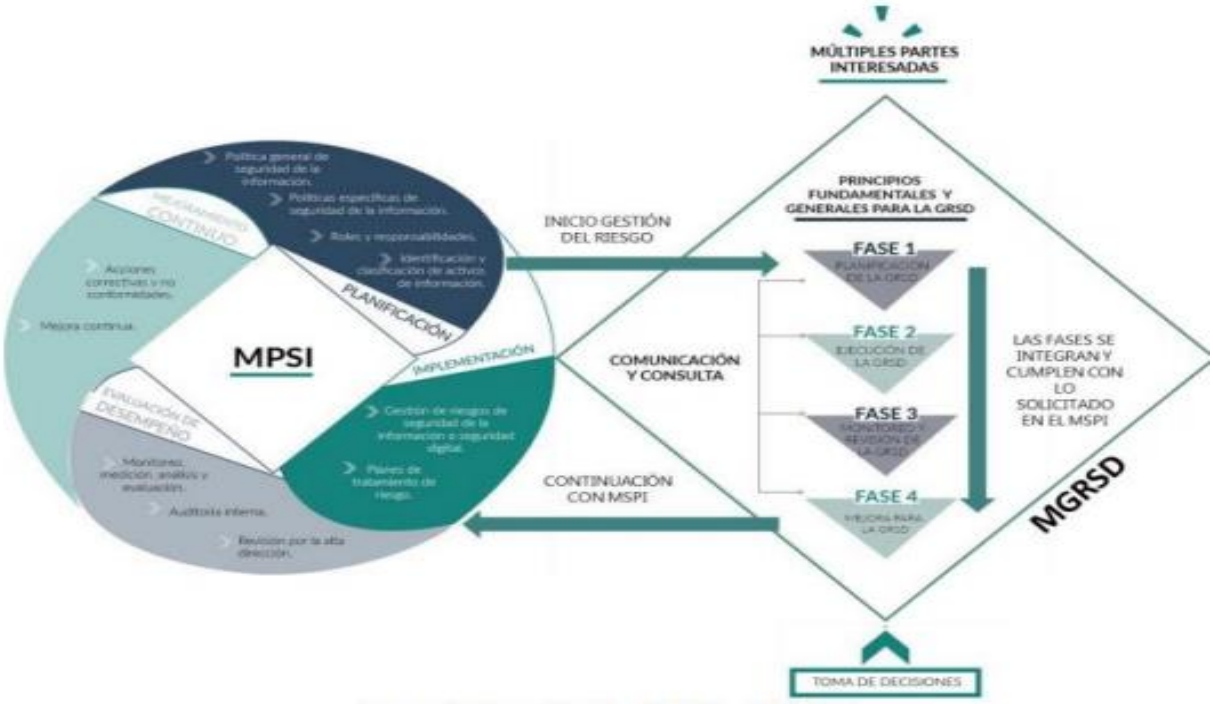

Imagen 1. Interacción entre el MSPI y el MGRSD.
Fuente: Ministerio de Tecnologías de la Información y las Comunicaciones

En este sentido, el desarrollo de la política deberá implementarse de acuerdo a lo establecido en el documento Lineamientos Para La Gestión De Riesgos De Seguridad Digital En Entidades Públicas, dicha información será documentada y las actividades serán establecidas en el formato Plan de Acción Modelo Integrado de Planeación y Gestión MIPG toda su documentación reposara en el área de sistemas bajo la custodia del Profesional Universitario de Sistemas quien es el responsable de la Seguridad Digital.

NORMATIVIDAD APLICABLE AL PROCESO

• Guía lineamientos para la gestión de riesgos de seguridad digital en entidades públicas.

• Ley 1928 de 2018 “Convenio sobre la Ciberdelincuencia”, adoptado el 23 de noviembre de 2001, en Budapest. • Acuerdo 02 de 2018: Por el cual se crea el comité de Seguridad Digital.

• Conpes 3854 de 2016: POLÍTICA NACIONAL DE SEGURIDAD DIGITAL • Decreto 1078 de 2015: “Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones”

• Ley 1712 de 2014 - Transparencia y Acceso a la Información Pública • Ley estatutaria 1581 del 2012: Por la cual se dictan disposiciones generales para la protección de datos personales.

• Decreto 103 de 2015: por el cual se reglamenta parcialmente la Ley 1712 de 2014 y se dictan otras disposiciones.

• Decreto 1499 de 2017. “Por medio del cual se modifica el Decreto 1083 de 2015, Decreto Único Reglamentario del Sector Función Pública, en lo relacionado con el Sistema de Gestión establecido en el artículo 133 de la Ley 1753 de 2015”. Presidencia de la República.

• Manual Operativo Modelo Integrado de Planeación y Gestión - MIPG Versión 4.

• Decreto 1083 de 2015 "Por el cual se adiciona el título 17 a la parte 2 del libro 2 del Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones, Decreto 1078 de 2015, para reglamentarse parcialmente el capítulo IV del título III de la Ley 1437 de 2011 y el artículo 45 de la Ley 1753 de 2015, estableciendo lineamientos generales en el uso y operación de los servicios ciudadanos digitales"

OBJETIVOS

• Identificar, analizar y mitigar riesgos de seguridad digital.

• Garantizar en un alto grado la disponibilidad, integridad y confidencialidad de la información.

• Garantizar el correcto funcionamiento del plan de contingencia.

INDICADORES

PROCESO	INDICADOR	PRINCIPIO MEDIDO	FUENTE
Gestión con valores	Nivel de implementación de la Política Seguridad Digital.	Eficacia	Resultados Autodiagnóstico.
Gestión con valores	Política seguridad Digital	Eficacia	Resultados Furag