DEPARTAMENTO ADMINISTRATIVO DE DESARROLLO INSTITUCIONAL

Alcaldía Municipal
Santander de Quilichao

PLAN DE TRATAMIENTO DE RIESGO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION. VIGENCIA 2024

CONTENIDO

1. INTRODUCCIÓN

El Plan de Tratamiento de Riesgos se elabora con el fin de dar a conocer cómo se realizará la implementación y socialización del componente de Gobierno digital en el Eje Temático de la Estrategia en seguridad y privacidad de la información, el cual busca proteger los datos de los ciudadanos garantizando la seguridad de la información.

La gestión de la seguridad de la información debe realizarse mediante un proceso sistemático, documentado y conocido por toda la organización.

Este proceso es el que constituye un SGSI, que podría considerarse, como el sistema de calidad para la seguridad de la información.

Garantizar un nivel de protección total es virtualmente imposible, incluso en el caso de disponer de un presupuesto ilimitado. El propósito de un sistema de gestión de la seguridad de la información es, por tanto, garantizar que los riesgos de la seguridad de la información sean conocidos, asumidos, gestionados y minimizados por la organización de una forma documentada, sistemática, estructurada, repetible, eficiente y adaptada a los cambios que se produzcan en los riesgos, el entorno y las tecnologías.

La importancia de que las administraciones cuenten con un plan de tratamiento de riesgos de seguridad y privacidad de la información, este aporta la evidencia de los nieles de riesgos en que se encuentran los activos mediante el nivel de madurez de la seguridad existente y sobre todo incentivar a los funcionarios a seguir las respectivas normas y procedimientos referentes a la seguridad de la información y recurso.

2. TERMINOS Y DEFINICIONES

Acceso a la Información Pública: Derecho fundamental consistente en la facultad que tienen todas las personas de conocer sobre la existencia y acceder a la información pública en posesión o bajo control de sujetos obligados. (Ley 1712 de 2014, art 4).

Activo: En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de la misma (sistemas, soportes, edificios, personas...) que tenga valor para la organización. (ISO/IEC 27000).

Activo de Información: En relación con la privacidad de la información, se refiere al activo que contiene información pública que el sujeto obligado genere, obtenga, adquiera, transforme o controlar en su calidad de tal.

Archivo: Conjunto de documentos, sea cual fuere su fecha, forma y soporte material, acumulados en un proceso natural por una persona o entidad pública o privada, en el transcurso de su gestión, conservados respetando aquel orden para servir como testimonio e información a la persona o institución que los produce y a los ciudadanos, o como fuentes de la historia. También se puede entender como la institución que está al servicio de la gestión administrativa, la información, la investigación y la cultura. (Ley 594 de 2000, art 3).

Amenazas: Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización. (ISO/IEC 27000).

Análisis de Riesgo: Proceso para comprender la naturaleza del riesgo y determinar el nivel de riesgo. (ISO/IEC 27000).

Auditoría: Proceso sistemático, independiente y documentado para obtener evidencias de auditoría y obviamente para determinar el grado en el que se cumplen los criterios de auditoría. (ISO/IEC 27000).

Autorización: Consentimiento previo, expreso e informado del Titular para llevar a cabo el tratamiento de datos personales (Ley 1581 de 2012, art 3).

Bases de Datos Personales: Conjunto organizado de datos personales que sea objeto de Tratamiento (Ley1581 de 2012, art 3).

Ciberseguridad: Capacidad del Estado para minimizar el nivel de riesgo al que están expuestos los ciudadanos, ante amenazas o incidentes de naturaleza cibernética. (CONPES 3701).

Ciberespacio: Es el ambiente tanto físico como virtual compuesto por computadores, sistemas computacionales, programas computacionales (software), redes de telecomunicaciones, datos e información que es utilizado para la interacción entre usuarios. (Resolución CRC 2258 de 2009).

Control: 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. Control es también utilizado como sinónimo de salvaguarda o contramedida. En una definición más simple, es una medida que modifica el riesgo.

Datos Abiertos: Son todos aquellos datos primarios o sin procesar, que se encuentran en formatos estándar e interoperables que facilitan su acceso y reutilización, los cuales están bajo la custodia de las entidades públicas o privadas que cumplen con funciones públicas y que son puestos a disposición de cualquier ciudadano, de forma libre y sin restricciones, con el fin de que terceros puedan reutilizarlos y crear servicios derivados de los mismos (Ley 1712 de 2014, art 6).

Datos Personales: Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables. (Ley 1581 de 2012, art 3).

Datos Personales Públicos: Es el dato que no sea semiprivado, privado o sensible. Son considerados datos públicos, entre otros, los datos relativos al estado civil de las personas, a su profesión u oficio y a su calidad de comerciante o de servidor público. Por su naturaleza, los datos públicos pueden estar contenidos, entre otros, en registros públicos, documentos públicos, gacetas y boletines oficiales y sentencias judiciales debidamente ejecutoriadas que no estén sometidas a reserva. (Decreto 1377 de 2013, art 3).

Datos Personales Privados: Es el dato que por su naturaleza íntima o reservada sólo es relevante para el titular. (Ley 1581 de 2012, art 3 literal h).

Datos Personales Mixtos: Para efectos de esta guía es la información que contiene datos personales públicos junto con datos privados o sensibles.

Datos Personales Sensibles: Se entiende por datos sensibles aquellos que afectan la intimidad del Titular o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición, así como los datos relativos a la salud, a la vida sexual, y los datos biométricos. (Decreto 1377 de 2013, art 3).

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. (ISO/IEC27000).

Derecho a la Intimidad: Derecho fundamental cuyo núcleo esencial lo constituye la existencia y goce de una órbita reservada en cada persona, exenta de la intervención del poder del Estado o de las intromisiones arbitrarias de la sociedad, que le permite a dicho individuo el pleno desarrollo de su vida personal, espiritual y cultural (Jurisprudencia Corte Constitucional).

Encargado del Tratamiento de Datos: Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, realice el Tratamiento de datos personales por cuenta del responsable del Tratamiento. (Ley 1581 de 2012, art 3)

Gestión de incidentes de seguridad de la información: Procesos para detectar, reportar, evaluar, responder, tratar y aprender de los incidentes de seguridad de la información. (ISO/IEC 27000).

Información Pública Clasificada: Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, pertenece al ámbito propio, particular y privado o semiprivado de una persona natural o jurídica por lo que su acceso podrá ser negado o exceptuado, siempre que se trate de las circunstancias legítimas y necesarias y los derechos particulares o privados consagrados en el artículo 18 de la Ley 1712 de 2014. (Ley 1712 de 2014, art 6).

Información Pública Reservada: Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, es exceptuada de acceso a la ciudadanía por daño

a intereses públicos y bajo cumplimiento de la totalidad de los requisitos consagrados en el artículo 19 de la Ley 1712 de 2014. (Ley 1712 de 2014, art 6).

Plan de continuidad del negocio: Plan orientado a permitir la continuación de las principales funciones misionales o del negocio en el caso de un evento imprevisto que las ponga en peligro. (ISO/IEC 27000).

Plan de tratamiento de riesgos: Documento que define las acciones para gestionar los riesgos de seguridad de la información inaceptables e implantar los controles necesarios para proteger la misma (ISO/IEC 27000).

Privacidad: En el contexto de este documento, por privacidad se entiende el derecho que tienen todos los titulares de la información en relación con la información que involucre datos personales y la información clasificada que estos hayan entregado o esté en poder de la entidad en el marco de las funciones que a ella le compete realizar y que generan en las entidades destinatarias del Manual de GEL la correlativa obligación de proteger dicha información en observancia del marco legal vigente.

Responsabilidad Demostrada: Conducta desplegada por los responsables o Encargados del tratamiento de datos personales bajo la cual a petición de la Superintendencia de Industria y Comercio deben estar en capacidad de demostrarle a dicho organismo de control que han implementado medidas apropiadas y efectivas para cumplir lo establecido en la Ley 1581 de 2012 y sus normas reglamentarias.

Responsable del Tratamiento de Datos: Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, decida sobre la base de datos y/o el Tratamiento de los datos. (Ley 1581 de 2012, art 3).

Riesgo: 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. (ISO/IEC 27000).

Seguridad de la información: Preservación de la confidencialidad, integridad, y disponibilidad de la información. (ISO/IEC 27000).

Sistema de Gestión de Seguridad de la Información SGSI: Conjunto de elementos interrelacionados o interactuantes (estructura organizativa, políticas, planificación de

actividades, responsabilidades, procesos, procedimientos y recursos) que utiliza una organización para establecer una política y unos objetivos de seguridad de la información y alcanzar dichos objetivos, basándose en un enfoque de gestión y de mejora continua. (ISO/IEC 27000).

Titulares de la información: Personas naturales cuyos datos personales sean objeto de Tratamiento. (Ley 1581 de 2012, art 3).

Trazabilidad: Cualidad que permite que todas las acciones realizadas sobre la información o un sistema de tratamiento de la información sean asociadas de modo inequívoco a un individuo o entidad. (ISO/IEC 27000)

3. OBJETIVOS

3.1. General

Crear, gestionar y mitigar los riesgos de seguridad y privacidad de la información, identificados en la Alcaldía Municipal de Santander De Quilichao con el fin de proteger los activos de información, el manejo de medios, el control de acceso y la gestión de los usuarios.

3.2. Específicos

1) Determinar el alcance del plan de gestión de riesgos de la seguridad y privacidad de la información.
2) Aplicar las metodologías del DAFP e ISO respectivamente en seguridad y riesgo de la información, para la Alcaldía de Santander de Quilichao.
3) Proponer soluciones para minimizar los riesgos a los que está expuesto cada activo.
4) Definir los principales activos a proteger en la alcaldía.
5) Evaluar y comparar el nivel de riesgo actual con el impacto generado después de implementar el plan de gestión de seguridad de la información.
6) Gestionar los eventos de seguridad de la información para detectar y tratar con eficiencia, en particular identificar si es necesario o no clasificarlos como incidentes de seguridad de la información.

4. ALCANCE

La planeación se enfocará en fortalecer la implementación de acciones para el tratamiento de riesgos de seguridad y privacidad de la información de acuerdo a los lineamientos emitidos por el Ministerio de Tecnologías de la Información y las Comunicaciones y el departamento administrativo de la función pública, enfocados a la seguridad informática de la plataforma tecnológica de la Alcaldía de Santander de Quilichao frente a ciber amenazas, como un aporte a las acciones que realizará la entidad en torno a la seguridad y privacidad de la información institucional, teniendo en cuenta las capacidades y recursos disponibles, para mejorar la confianza de los ciudadanos, usuarios, socios y demás partes interesadas.

5. CONTEXTO NORMATIVO

A continuación, se relaciona la normativa que reglamenta el Plan de Tratamiento de Riesgo de Seguridad y Privacidad de la Información de la Alcaldía Municipal de Santander de Quilichao.

Marco Normativo	Descripción
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, del 11 de abril de 2016	Política Nacional de Seguridad Digital de Colombia, el crecimiento en el uso masivo de las Tecnologías de la Información y las Comunicaciones (TIC) en Colombia, reflejado en la masificación de las redes de telecomunicaciones como base para cualquier actividad socioeconómica y el incremento en la oferta de servicios disponibles en línea, evidencian un aumento significativo en la participación digital de los ciudadanos. Lo que a su vez se traduce en una economía digital con cada vez más participantes en el país. Desafortunadamente, el incremento en la participación digital de los ciudadanos trae consigo nuevas y más sofisticadas formas para atentar contra su seguridad y la del Estado. Situación que debe ser atendida, tanto brindando protección en el ciberespacio para atender estas amenazas, como reduciendo la probabilidad de que estas sean efectivas, fortaleciendo las capacidades de los posibles afectados para identificar y gestionar este riesgo
Ley 1581 de 2012	Por la cual se dictan disposiciones generales para la protección de datos personales.

Marco Normativo	Descripción
Ley 1712 del 2014	Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones.
Decreto 1377 de 2013	Por la cual se reglamenta parcialmente la Ley 1581 de 2012.
Decreto 2157 de 2017	Por medio del cual se adoptan directrices generales para la elaboración del plan de gestión del riesgo de desastres de las entidades públicas y privadas en el marco del artículo 42 de la ley 1523 de 2012.
CONPES 3701-2011	Lineamientos de Política para Ciberseguridad y Ciberdefensa Estrategia Nacional de Ciberseguridad y Ciberdefensa.
CONPES 3854 - 2016	Política Nacional de Seguridad Digital.
ISO 22301:2019	Seguridad y resiliencia - Sistemas de gestión de la continuidad del negocio. Requisitos.
GTC-ISO/IEC 27031:2016	Tecnología de la información. Técnicas de seguridad. Directrices para la preparación de la tecnología de información y las comunicaciones para la continuidad de negocio
ISO 22317:2015	Seguridad social - Sistemas de gestión de la continuidad del negocio - Directrices para el análisis de impacto empresarial (BIA).
NTC-ISO/IEC 27001:2013	Norma Técnica Colombiana NTC-ISO-IEC 27001. Sistemas de Gestión de la Seguridad de la Información. Requisitos.
Lineamientos MINTIC LI.ST.05, LI.ST.09, LI.ST.10, LI.ST.13 - 2015	Orientaciones de carácter general que corresponden a una disposición o directriz que debe ser implementada en las entidades del Estado colombiano, específicamente en operación y soporte de los servicios tecnológicos.

Tabla 1 Contexto Normativo

6. AVANCES DE LA ENTIDAD

El proceso de apoyo de sistemas y TICs en el entre los años 2022 y 2024 ha hecho énfasis en abordar la gestión de riesgos de seguridad informática sobre los activos de tecnologías de información frente a ciberamenazas, en atención a la cantidad de procesos que realizan sus actividades apoyadas en el uso de tecnologías de información y de las comunicaciones.

6.1. Servicios de TI

Los servicios tecnológicos que ofrece la oficina TIC están pensados para garantizar el correcto funcionamiento de la arquitectura tecnológica de la entidad, dando respuesta oportuna a los requerimientos que se presenten.

Nombre	Descripción Funcional
Acceso a internet por WIFI	Acceso a la red de colaboradores de la Entidad de manera inalámbrica a través de dispositivos móviles y computadores portátiles. La velocidad de 100 Mbps de bajada, 50 Mbps de subida y soporta máximo 100 usuarios conectados concurrentemente
Acceso a la Intranet	Acceso a la red protegida para el uso de los recursos tecnológicos. (Aplicaciones, impresoras, Telefonía IP, etc.)
Acceso a internet	Acceso a internet. Con una velocidad de 100 Mb de bajada, 20 Mb de subida.
Administración configuración servicio de correo electrónico	Consiste en la asignación de cuentas a los funcionarios y configuración de clientes de correo en los equipos de la entidad, gestión de novedades ante el operador externo.
Servicio de entrenamiento y capacitación uso de las soluciones de TI	Servicio que suministra capacitación y entrenamiento sobre las funciones de los sistemas de información que maneja la entidad.
Plataforma de mesa de servicio	Plataforma para registro, consulta y respuesta de peticiones, quejas, reclamos, sugerencias y denuncias. Aplicación
Telefonía IP	Servicio de comunicaciones telefónicas entre usuarios internos y externos de la institución.
Antivirus	Instalación de software que detecta y elimina virus informáticos y otras amenazas informáticas en la red, sistemas de información, PC, dispositivos móviles y demás.
Gestión de equipos de cómputo y periféricos	Adquisición, instalación, configuración y mantenimientos preventivos y correctivos de hardware y software base de los equipos asignados a los funcionarios y contratistas de la Entidad
Servicio de Instalación de software en Equipos de computo	Instalación de software por demanda en los equipos de cómputo de los funcionarios o contratistas

Nombre	Descripción Funcional
Videollamadas	Acceso de servicio de video llamada a través de (Teams, Meet, Zoom, etc.)
Página web institucional	Sitio web institucional disponible a los ciudadanos que integra información sobre servicios institucionales, trámites, noticias, eventos de interés, políticas y normatividad. Gestión compartida con operador externo.
Sitio Intranet	Sitio web institucional que integra información sobre servicios internos, trámites, noticias, eventos de interés, políticas, normatividad.
Administración de licencias de software	Servicio de adquisición de licencias de software requeridas para usar en los diferentes procesos de la organización.
Almacenamiento de datos e información	Servicio que se encarga de almacenar datos e información en repositorios y bases de datos.
Administrar repositorios de archivos.	Permite a los usuarios dentro de la entidad tener acceso a los archivos digitalizados de cada dependencia.
Respaldo y recuperación de datos e información	Servicio que se encarga de generar respaldo de datos, así como la recuperación de estos en caso de pérdida o alteración indebida
Pruebas de vulnerabilidades	Servicio que se encarga de realizar pruebas de vulnerabilidades a la arquitectura de TI.
Administración configuración directorio activo.	Permite organizar y gestionar todos los recursos de red en la entidad: cuentas de usuarios, dominios, equipos, privilegios o permisos, políticas de seguridad.
Hosting	Servicio de alojamiento de componentes de software en Servidores físicos o virtuales.
DNS	Servicio que permite asignar nombre de dominio a los diferentes elementos que hacen parte de la red.
Soporte de primer nivel en línea y remoto.	Servicio que se encarga de brindar soporte inicial, responsable de las incidencias básicas de los clientes.
Gestión de incidentes y solución de problemas.	Servicio que tiene como objetivo prevenir o reparar en el menor tiempo posible cualquier interrupción o retraso que afecte a la calidad del servicio minimizando el impacto en las actividades de la entidad.

Nombre	Descripción Funcional
Administración de servidores (locales y en hosting).	Servicio que se encarga del monitoreo, mantenimiento hardware y software, entre otras importantes tareas de gestión, permitiendo la disponibilidad de los servicios.
Monitoreo desempeño de infraestructura de red.	Consiste en la revisión y supervisión de las actividades que se realizan a través de la infraestructura tecnológica, lo que permite identificar patrones de uso y comportamientos en la red, para implementar estrategias de aprovechamiento de recursos y la revisión de amenazas cibernéticas.
Administración de infraestructura de red.	Consiste en la revisión y supervisión de todos los elementos hardware y software de la red, para identificar fallos, mejorar el rendimiento y garantizar la calidad en los servicios.
Gestión de mejoras a funcionalidades en aplicaciones suministradas por terceros	Se encarga de recoger y analizar las peticiones o sugerencias de los usuarios, para luego trasladar el requerimiento de mejora al proveedor de la aplicación
Administrar publicaciones de contenido en la web.	Permite a los usuarios publicar información de interés en el sitio web de la entidad.
Mantener dispositivos de impresión, escaneo, fax.	Servicio que se encarga de los mantenimientos preventivos y correctivos de hardware y software de los equipos asignados a los funcionarios y contratistas de la Entidad
Apoyo técnico en la toma de decisiones.	Consiste en asesorar a la entidad y sus dependencias en la adquisición, implementación y uso de las tecnologías de la información para conseguir sus objetivos.

Tabla 2 Descripción catálogo de Servicios de TI

6.2. Infraestructura

La infraestructura tecnológica que soporta los servicios y procesos de la alcaldía está conformada por servicios de conectividad, elementos software (aplicaciones, sistemas de información) y elementos físicos (Router, Switches, puntos de acceso, etc.) Distribuidos en las nueve sedes de la entidad.

Ubicación	Elementos
CAM	Centro de cableado principal (Servidores, Router, Switches, Access Point, Transceiver Fibra), Equipos de cómputo y teléfonos.
Casa Consistorial	Switches, Access Point, Transceiver Fibra, Equipos de cómputo, impresoras, scanner y teléfonos.
Casa de Justicia	Switches, Access Point, Transceiver Fibra, Equipos de cómputo, impresoras, scanner y teléfonos.
Secretaría de Movilidad	Switches, Access Point, Transceiver Fibra, Equipos de cómputo, impresoras, scanner y teléfonos.
Biblioteca	Switches, Access Point, Equipos de cómputo, impresoras, scanner y teléfonos.
CRAV	Switches, Access Point, Transceiver Fibra, Equipos de cómputo, impresoras, scanner y teléfonos.
Infraestructura	Switches, Access Point, Equipos de cómputo, impresoras, scanner y teléfonos
Centro Vida	Equipos de cómputo, impresoras, scanner y teléfonos.

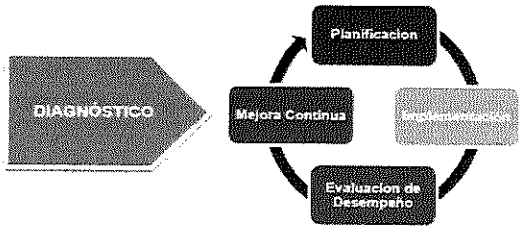
Tabla 2 Sedes Alcaldía Municipal de Santander de Quilichao

7. METODOLOGÍA

Para llevar a cabo la implementación del Modelo de Seguridad y Privacidad de la Información en la Alcaldía Municipal de Santander De Quilichao, se toma referencia la metodología PHVA (Planear, Hacer, Verificar y Actuar) y los lineamientos emitidos por el Manual de implementación versión 3.02 del Ministerio de Tecnologías de la Información y las Comunicaciones.

De acuerdo con esto, se definen las siguientes fases de implementación del MSPI:

1. Diagnosticar
2. Planear
3. Hacer
4. Verificar
5. Actuar



Grafica 1Ciclo de operación del Modelo de Seguridad y Privacidad de la Información

El Plan de Tratamiento de Riesgos contempla la definición de las actividades a desarrollar en aras de mitigar los riesgos sobre los activos identificados en la entidad, 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 (MinTIC:2016)

No.	Actividades	Meta	Fecha Inicio	Fecha Final
1	Desarrollar campañas de socialización de las amenazas digitales, políticas y controles de seguridad, con el fin de mejorar conocimiento en temas de seguridad.	Desarrollar 2 socializaciones al interior de la entidad con relación a temas de amenazas digitales, políticas y controles de seguridad a través de los canales de comunicación que maneja la entidad.	01-02-2024	20-12-2024
2	Mantener la disponibilidad continua de servicios esenciales de Tecnologías de la información	Disponibilidad continua de servicios esenciales como telecomunicaciones e infraestructura.	01-02-2024	20-12-2024
3	Identificar y proteger los datos de carácter personal.	Datos de carácter personal identificados y protegidos.	01-02-2024	20-12-2024
4	Mantener una adecuada clasificación de la información bajo custodia de la Entidad de acuerdo con el marco legal vigente.	Información almacenada de manera adecuada y bajo custodia de la Entidad de acuerdo con el marco legal vigente.	01-02-2024	20-12-2024
5	Realizar la segregación apropiada de roles y privilegios en todos los sistemas de información.	Roles y privilegios en todos los sistemas de información administrados de manera adecuada.	01-02-2024	20-12-2024
6	Sensibilizar al interior de la Entidad las políticas de seguridad de la información.	Políticas de seguridad de la información al interior de la Entidad fortalecidas.	01-02-2024	20-12-2024
7	Reforzar el cumplimiento de los acuerdos de confidencialidad y los acuerdos de intercambio seguro de información.	Acuerdos de confidencialidad y de intercambio seguro de información cumplidos al interior de la Entidad.	01-02-2024	20-12-2024
8	Crear o continuar con la adopción de la estructura del Modelo de Gestión de Proyectos TI propuesta por MINTIC - MGPTI.G.GEN.01 en temas de gestión de riesgos.	Modelo de Gestión de Proyectos TI propuesta por MINTIC - MGPTI.G.GEN.01 en temas de gestión de riesgos fortalecido.	01-02-2024	20-12-2024
9	Realizar diagnósticos periódicos de seguridad y pruebas de vulnerabilidad, con el fin de identificar las brechas de seguridad.	Diagnósticos de seguridad y pruebas de vulnerabilidad desarrollados.	01-02-2024	20-12-2024
10	Actualizar los riesgos asociados a los sistemas de información de la entidad, contenidos en el mapa de riesgos institucional realizando seguimiento a los controles y planes de acción.	Riesgos, controles y acciones asociados a los sistemas de información de la entidad actualizados.	01-02-2024	20-12-2024

Tabla 4 Cronograma de Actividades

7.1. Seguimiento y Evaluación

Al finalizar cada actividad se realizará una reunión con la secretaria del Departamento Administrativo de Desarrollo Institucional, Responsable TIC para presentar el informe del avance del proyecto y de esta manera evaluar todos los pasos se han ido realizado.

7.2. Entregables

- ✓ Acta de Reunión.
- ✓ Informe de avance o resumen ejecutivo.
- ✓ Plan de tratamiento de riego aprobado.

8. RECURSOS

La alcaldía de Santander de Quilichao, en el marco de la gestión de riesgos de seguridad y Privacidad de la información, Seguridad Digital y Continuidad de la Operación, dispone de los siguientes recursos.

8.1. Humanos

El proceso de apoyo de sistemas Tics, alcalde Municipal, secretarios y jefes de oficinas, líderes de los procesos.

8.2. Técnicos

Modelo de Seguridad y Privacidad de la Información (MSPI), Guía para la administración del riesgo y el diseño de controles en entidades públicas.

8.3. Financieros

Recursos para la adquisición de conocimiento, recursos humanos, técnicos, y desarrollo de auditorías, Plan de adquisiciones.

La estimación y asignación del presupuesto para el plan de tratamiento de riesgos de Seguridad y Privacidad 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.

VIKY JARIMA FRANCO SOLARTE
DIRECTORA DEPARTAMENTO ADMINISTRATIVO
DE DESARROLLO INSTITUCIONAL

Redactor/Transcriptor: Mar Zein Biscunda Quintana
Serie Sub serie documental: Planes Institucionales