Gobernación del Archipiélago
de San Andrés, Providencia y Santa Catalina

FASE DE PLANIFICACIÓN

PLAN DE SEGURIDAD DE LA INFORMACION

VERSIÓN 2.0

ACTUALIZÓ: ING. SHARY LLANOS ANTONIO
30-ENERO-2021

Principales modificaciones por versión de este documento

Historial de Versiones

Versión	Autor	Fecha	Descripción de la Modificación
1.0	Ing. Viviana López B. Ing. Enrique Santiago	15 Julio del 2019	Elaboración de Estructura y Contenido
2.0	Ing. Shary Llanos Antonio	30 de Enero de 2021	Actualización

Este documento ha sido revisado por:

Versión	Revisor	Firma
1.0	Grupo TIC	
2.0	Secretaría General – Grupo TIC	

Este documento ha sido aprobado por:

Versión	Revisor	Firma
1.0	Secretaría General	
2.0	Secretaría General	

CONTENIDO

1. INTRODUCCIÓN

Este documento hace parte integral del programa de seguridad de la Información de la Gobernación del Archipiélago de San Andrés, Providencia y Santa Catalina, enfocados a brindar un acercamiento al Modelo de Seguridad y privacidad de la información – MSPI propuesto por el gobierno nacional.

El Sistema de Gestión de Seguridad de la Información- SGSI que propone el ministerio de las TIC – MSPI, brinda un modelo que posee un conjunto de lineamientos, políticas, normas y procesos que proveen y promueven la puesta en marcha, supervisión, mejora y control de la implementación de un sistema de seguridad de la información.

La GOBERNACIÓN DEL ARCHIPIÉLAGO DE SAN ANDRES, PROVIDENCIA Y SANTA CATALINA comprometida con la gestión de la seguridad de la información de sus procesos misionales, adopta la gestión de la seguridad de sus activos de información definiendo el presente plan resultante del análisis de riesgos realizado en la institución.

Teniendo en cuenta lo anterior, se actualiza el presente documento dando cumplimiento a lo establecido en el Decreto 612 de 2018, actualizando el Plan de implementación de Seguridad y Privacidad de la Información al interior de la Entidad.

2. DEFINICIONES

Activo: Elemento que por la importancia que tiene para los procesos de la organización, es considerado como un bien que tienen un valor para lo organización. Los activos pueden incluir, personas, edificios, sistemas computacionales, redes, registros en papel, faxes, etc.

Activo de Información: colección de datos en formato físico o digital generado o transformado por la organización y que se considera parte de la materia prima de los procesos de la organización.

Nivel de Clasificación de los Activos de Información: Valor ponderado del activo de información asignado por el propietario del mismo de acuerdo a las propiedades de seguridad de la información.

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).

Administración de riesgos: conjunto de etapas secuenciales que se deben desarrollar para el adecuado tratamiento de los riesgos

Análisis del riesgo: etapa de la administración del riesgo, donde se establece la probabilidad de ocurrencia y el impacto del riesgo antes de determinar los controles (análisis del riesgo inherente).

Asumir el riesgo: opción de manejo donde se acepta la pérdida residual probable, si el riesgo se materializa.

Causa: medios, circunstancias y/o agentes que generan riesgos.

Calificación del riesgo: estimación de la probabilidad de ocurrencia del riesgo y el impacto que puede causar su materialización.

Compartir o transferir el riesgo: opción de manejo que determina traspasar o compartir las pérdidas producto de la materialización de un riesgo con otras organizaciones mediante figuras como outsourcing, seguros, sitios alternos.

Consecuencia: efectos que se pueden presentar cuando un riesgo se materializa.

Control: acción o conjunto de acciones que minimiza la probabilidad de ocurrencia de un riesgo o el impacto producido ante su materialización.

Control preventivo: acción o conjunto de acciones que eliminan o mitigan las causas del riesgo; está orientado a disminuir la probabilidad de ocurrencia del riesgo.

Control correctivo: acción o conjunto de acciones que eliminan o mitigan las consecuencias del riesgo; está orientado a disminuir el nivel de impacto del riesgo.

Debilidad: situación interna que la entidad puede controlar y que puede afectar su operación.

Evaluación del riesgo: resultado del cruce cuantitativo de las calificaciones de probabilidad e impacto, para establecer la zona donde se ubicará el riesgo.

Evitar el riesgo: opción de manejo que determina la formulación de acciones donde se prevenga la materialización del riesgo mediante el fortalecimiento de controles identificado.

Frecuencia: ocurrencia de un evento expresado como la cantidad de veces que ha ocurrido un evento en un tiempo dado.

Identificación del riesgo: etapa de la administración del riesgo donde se establece el riesgo con sus causas (asociadas a factores externos e internos de riesgo), consecuencias y se clasifica de acuerdo con los tipos de riesgo definidos

Impacto: medida para estimar cuantitativa y cualitativamente el posible efecto de la materialización del riesgo.

Mapa de riesgos: documento que, de manera sistemática, muestra el desarrollo de las etapas de la administración del riesgo.

Materialización del riesgo: ocurrencia del riesgo identificado

Opciones de manejo: posibilidades disponibles para administrar el riesgo posterior a la valoración de los controles definidos (asumir, reducir, evitar compartir o transferir el riesgo residual).

Plan de contingencia: conjunto de acciones inmediatas, recursos, responsables y tiempos establecidos para hacer frente a la materialización del riesgo y garantizar la continuidad del servicio

Probabilidad: medida para estimar cuantitativa y cualitativamente la posibilidad de ocurrencia del riesgo.

Procedimiento: conjunto de especificaciones, relaciones, responsabilidades, controles y ordenamiento de las actividades y tareas requeridas para cum

Confidencialidad: propiedad de los activos de información referente a que este solo sea accesible a los usuarios a los que la entidad previamente les ha otorgado la autorización.

Integridad: propiedad de los activos de información referente a que solo los usuarios autorizados por la organización puedan realizar cambios sobre los activos en el marco de un proceso legítimo de la compañía.

Disponibilidad: propiedad de los activos de información referente a que estos, siempre estén al alcance los usuarios de la organización en el momento en el que sean requeridos dentro de un proceso legítimo de la compañía.

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

SGSI/Sistema de Gestión de Seguridad de la Información: Proceso continuo a través del cual la organización garantiza la preservación de las propiedades de la seguridad de la información, conocidas como: Confidencialidad, Integridad y Disponibilidad como también a otras propiedades como la autenticidad, no repudio y trazabilidad.

3. OBJETIVO

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 los procesos de la Entidad.

4. ALCANCE

Aplica a todos los niveles de la GOBERNACIÓN DEL ARCHIPIÉLAGO DE SAN ANDRES, PROVIDENCIA Y SANTA CATALINA, a todos sus funcionarios, contratistas, proveedores, operadores y aquellas personas o terceros que en razón del cumplimiento de sus funciones y las de la Entidad compartan, utilicen, recolecten, procesen, intercambien o consulten su información, así como a los Entes de Control, Entidades relacionadas que accedan, ya sea interna o externamente a cualquier tipo de información, independientemente de su ubicación. Así mismo, esta lo dispuesto en este documento y su implementación aplica a toda la información creada, procesada o utilizada por la Entidad, sin importar el medio, formato, presentación o lugar en el cual se encuentre.

5. PROCESO DE SEGURIDAD Y PRIVACIDAD DE LA INFROMACIÓN

La GOBERNACION DEL ARCHIPIELAGO DE SAN ANDRES, PROVIDENCIA Y SANTA CATALINA, a través de los comités de gestión y desempeño institucional, apoyarán e impulsarán la adopción del Modelo de Seguridad y Privacidad de la Información propuesto por MinTIC - MSPI, considerando las actividades asociadas a los procesos definidos dentro del alcance y tomando como referencia los riesgos que podrían afectar los activos de información de la Institución.

La Gestión de la Seguridad de la Información del MSPI está basada en el ciclo de mejora continua adoptado por varios sistemas de gestión y conocido como el Ciclo de DEMING tal como su modelo principal de referencia ISO 27000.

Figura 1. Ciclo de Deming

Este ciclo de mejora continua permite que se pueda realizar la adopción, gestión y afinamiento permanente de las actividades encaminadas a reducir la exposición a múltiples amenazas que podrían afectar la seguridad de la información de la institución.

La adopción del MSPI se realizará en 4 Fases alineadas con el Ciclo de mejora continua de Deming antes descrito, posteriormente a la realización de un análisis de brecha (GAP) que sirve de diagnóstico para determinar la postura actual de la seguridad de la información a nivel institucional, la madurez como también permitirá determinar el nivel de esfuerzo requerido para alinearse con los lineamientos del Gobierno Nacional.

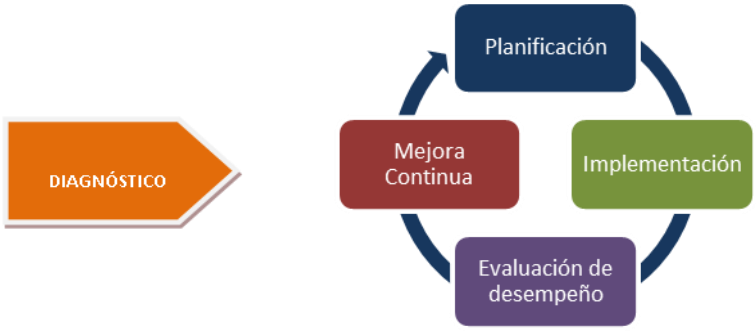

Figura 2. Ciclo de Operación del MSPI, Fuente: MinTIC

La fase de planificación está alineada con la 1era fase "PLANIFICAR" del ciclo de mejora continua del ciclo de Deming y está orientada a establecer el Modelo de Seguridad de la Información; esta incluye la construcción de las políticas de seguridad, los objetivos, los procedimientos de seguridad necesarios para gestionar los activos de información. Siendo la actividad principal, el Análisis de Riesgos a todos los activos relevantes de la institución.

La siguiente fase del ciclo de Deming "HACER" está alineada con la segunda fase del Ciclo de operación de MSPI llamada Implementación, en la cual se lleva a cabo la implementación y la operación del MSPI.

Una vez implementadas las políticas de seguridad de la información y en consecuencia con la 3ra fase del ciclo de mejora continua "EVALUAR", se procederá a revisar, hacer seguimiento y medir el desempeño del sistema de seguridad en adopción.

Finalmente se ejecutarán las actividades de la fase de Mejora Continua alineada con la 4ta fase del ciclo de Deming "ACTUAR", que tiene como fin Mantener y Mejorar el MSPI en la Organización.

6. ESTABLECIMIENTO Y GESTION DEL MSPI

En concordancia con el ciclo de mejora continua, las actividades del modelo en cuestión están distribuidas en cuatro (4) fases posteriores a la de Diagnóstico. Para facilitar la adopción del MSPI, el Ministerio de las TIC ha dispuesto una serie de guías alcanzables a través del URL: https://www.mintic.gov.co/gestionti/615/w3-propertyvalue-7275.html

Las fases deben ejecutarse de forma secuencial, ya que los resultados obtenidos en cada fase son empleados como entradas para la fase siguiente.

A continuación, se describen las Fases del Modelo de Seguridad y Privacidad de la Información definido por los lineamientos del Gobierno Digital.

Figura 3. Fases de Adopción del MSPI

Fase de Diagnóstico

Este Modelo de Seguridad y Privacidad de la Información requiere la ejecución de una fase previa a la planificación, llamada fase de diagnóstico que tiene como fin determinar el estado actual de la organización con respecto al cumplimiento de los lineamientos de seguridad y privacidad de la información definidos por el estado colombiano.

Las principales actividades de esta fase son:

- Identificar el Estado actual de la Entidad en cuanto a los lineamientos de Seguridad del Estado.
- Identificación del Nivel de Madurez de la organización con respecto al cumplimiento de los lineamientos de seguridad y la adopción del MSPI.
- Levantamiento de información referente a los principales activos de la organización.
- Identificación de las principales vulnerabilidades y amenazas a las que están expuestos los principales procesos y activos de información al igual que la efectividad de los controles implementados (si existen).

El levantamiento de información y la identificación de fallos técnicos y administrativos de los procesos corporativos y de los activos de información, se realiza aplicando la metodología de pruebas de efectividad, definida por MinTIC como parte del modelo de seguridad. Esta metodología se aprecia en la figura siguiente:

Figura 4. Componentes de la metodología de pruebas de efectividad, Fuente: MinTIC

Fase de Planificación

Una vez finalizado el diagnostico e identificado el análisis GAP (brecha o diferencia entre un estado ideal y el estado actual identificado), entre los requerimientos del MSPI y el estado actual de la seguridad de la información en la organización, se procede con la definición de la estrategia referente a la planificación de la adopción del Modelo de Seguridad y privacidad de la Información que incluye:

- Determinar el Contexto de la Organización
- Liderazgo
- Planificación
- Soporte

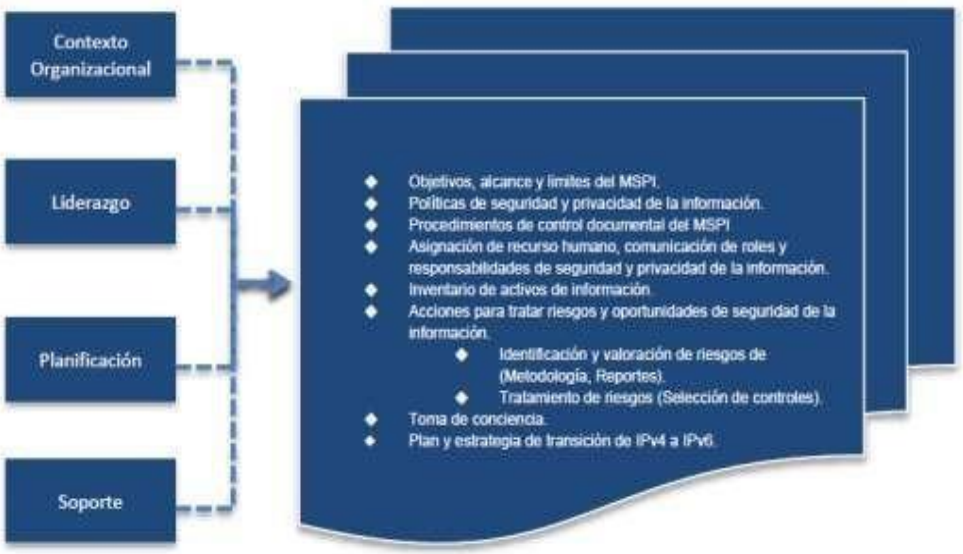

Figura 5. Principales componentes de la fase de Planificación.

En esta etapa se definen los lineamientos, se definen las bases y se construyen los instrumentos necesarios que facilitaran la implementación del MSPI.

A continuación, se relacionan las principales actividades de la fase de Planificación.

- La definición los objetivos, del alcance y de los límites del SGSI.
- Se asignan los responsables de la gestión de la Seguridad y la privacidad de la información.
- Se construyen las políticas de seguridad de la Información.
- Definir el plan de capacitación, comunicación y sensibilización del nuevo SGSI contenidos en las políticas de seguridad.
- Se construye la documentación requerida para la operación del SGSI que incluye:
  - Procedimientos de seguridad de la información:
    - Procedimiento de control de documentos
    - Procedimiento para auditorías internas
    - Procedimiento para la clasificación de activos
    - Procedimiento para la gestión de incidentes de seguridad de la información.
    - Procedimiento de gestión de llaves criptográficas

- Procedimientos de Backup.
- Otros procedimientos.
  - Formatos, instructivos y demás documentación requerida por el MSPI

- Se realiza el inventario y la clasificación de activos de información.
- Se realiza el análisis de riesgos al que están expuestos los activos de información.
- Se construye el plan de tratamiento de riesgos
- Construcción del plan de diagnóstico referente a la transición del direccionamiento IPv4 actual a IPv6.

Fase de Implementación

En esta fase se procede a operacionalizar los lineamientos definidos en la planificación al igual que las políticas, procedimientos y demás instrumentos construidos en la fase anterior.

Figura 6. Principales componentes de la fase de Implementación. Fuente: MinTIC

A continuación, se relacionan las principales actividades referentes a la Implementación del MSPI:

- Realizar la planificación y el control de la operación corporativa
- Realizar la Implementación de los planes de:
  - Tratamiento de riesgos (resultante del análisis de riesgos)
  - plan de capacitación, comunicaciones y sensibilización.
  - Entre otros.

- Implementar los procedimientos de:
  - Control de documentos
  - Backups
  - Gestión de incidentes de seguridad
  - Auditorías internas
  - Gestión de llaves criptográficas.
- Seguridad en las Operaciones.
- Entre otros.
  - Definir los indicadores de gestión que permitan medir el cumplimiento de los lineamientos del SGSI. Tales como:
  - La efectividad de los controles
  - La Eficiencia del SGSI adoptado
  - Proveer los estados de seguridad de los principales componentes del sistema
  - Entre otros.
- Definir la estrategia del plan de implementación del direccionamiento IPv6 en la plataforma de TI.

Las actividades más importantes de esta fase están orientadas al tratamiento del riesgo identificado, basados en las necesidades de seguridad de la información y en la declaración de aplicabilidad previamente construida, como también en la puesta en producción de las medidas de seguridad y controles técnico- administrativos que faciliten la ejecución de los procesos de negocio y el resto de la operación corporativa de forma segura.

Fase de Evaluación de desempeño

Una vez finalizada la implementación, el MSPI define que debe llevarse a cabo el seguimiento y la monitorización del nuevo SGSI.

Figura 7. Principales componentes de la fase de Evaluación de Desempeño, Fuente: MinTIC

Esta medición del desempeño se realiza a partir del resultado de los indicadores de gestión que miden la efectividad, la eficiencia y la eficacia de las acciones implementadas en la fase anterior.

Las principales actividades de esta fase se relacionan a continuación:

- Monitoreo, medición, análisis y evaluación del plan de tratamiento de riesgos a partir de la medición de la efectividad de los controles técnicos y demás contramedidas administrativas adoptadas por la organización.
- Revisión de la efectividad del SGSI por parte de la alta dirección.

Fase de Mejora continúa

En esta fase, se toman los resultados obtenidos de la monitorización, medición y evaluación del nuevo SGSI como parámetros de entrada para diseñar un plan para el mejoramiento continuo de la postura de seguridad de la organización.

La fase se centra en la ejecución de:

- Las Acciones correctivas requeridas
- La Mejora continua del sistema de gestión de seguridad.

Figura 8. Principales componentes de la fase de Mejora Continua, Fuente: MinTIC

Las principales actividades de esta fase son:

- La creación de un plan de mejoramiento del SGSI
- El plan de comunicación de los resultados
- Realización de los ajustes necesarios a las políticas, procedimientos, controles y demás elementos del SGSI.

7. RESPONSABILIDAD DE LA DIRECCION

7.1. Compromiso de la dirección

La dirección de la GOBERNACION DE SAN ANDRES, PROVIDENCIA Y SANTA CATALINA tiene claro que la confidencialidad, integridad y la disponibilidad de su información es muy importante para garantizar el cumplimiento de la misión institucional, ya que es consciente de que esta es uno de los activos más importantes que posee y que reducir el riesgo al que se encuentra expuesta requiere la asignación permanente de recursos para establecer, implementar, operar, hacer seguimiento, mantenimiento y mejorar continuamente la postura de seguridad de la información. En cumplimiento con las responsabilidades de ley y la necesidad de salvaguardar los activos de información, la dirección de la Entidad está comprometida con la implementación del Modelo de Seguridad y Privacidad de la información, propuesto por MinTIC. Y para asegurar su adopción debe aprobar el

establecimiento de las políticas de Seguridad de la Información, según acto administrativo; de la misma forma se debe crear el rol de Oficial de Seguridad de la información, y asignar al Comité Institucional de Gestión y Desempeño las funciones referentes a la gestión de la Seguridad de la Información.

Las políticas de seguridad han sido socializadas a partir de su aprobación, como puede evidenciarse en los registros de control de asistencia referente a las actividades de sensibilización sobre las políticas de seguridad de la información a funcionarios y contratistas de la institución.

La Dirección de la Entidad junto con el Oficial de Seguridad de la Información y el Comité Institucional de Gestión de Desempeño, definieron los criterios de aceptación para los riesgos y los niveles de riesgo aceptables, que fueron considerados en el análisis de riesgos realizado posteriormente.

Con el fin de garantizar la pertinencia y la efectividad del nuevo Sistema de Gestión de Seguridad de la Información, dentro de las políticas de seguridad se incluyó la realización de auditorías internas y la realización de revisiones periódicas al MSPI por parte de la dirección.

7.2. Gestión de recursos

La GOBERNACION DE SAN ANDRES, PROVIDENCIA Y SANTA CATALINA, tiene claro que es necesario hacer un esfuerzo y destinar unos recursos para la gestión permanente de la seguridad de la Información.

7.2.1. Provisión de recursos

La Entidad como resultado de las actividades de la fase de diagnóstico estimo los recursos de personal y financieros mínimos requeridos para:

- El establecimiento, implementación, operación, seguimiento, mantenimiento y mejora del MSPI. Los principales recursos de este ítem son:
    - Nombramiento de Oficial de Seguridad, Comité de Seguridad de la Información y contratación de servicio de Consultoría Externa.

- La Definición de políticas y procedimientos de seguridad de la información en cumplimiento con el MSPI y alineados con las necesidades de la institución. Para esto se realizó:
    - Evaluación de las necesidades de seguridad de los principales procesos institucionales.
    - Construcción de los procedimientos de seguridad de la Información.
- Identificación de los requisitos de las partes interesadas y legales para definir las políticas. Para cumplir con esto se hizo uso de personal interno de la organización con apoyo de un servicio de consultoría externo.
- La realización del análisis de riesgo para determinar los fallos de seguridad de la organización y la determinación de los controles requeridos para asegurar la información corporativa. Para cumplir con esta actividad, la institución se apoyó en personal interno y externo especialista en el área.
- Se determinó que el personal del comité de seguridad, el oficial de seguridad con apoyo de un equipo de especialistas externo dará cumplimiento al plan de auditoria definido en las políticas de seguridad y apoyaran también la revisión periódica del MSPI.
- A partir de los resultados de la revisión de la tercera fase del MSPI, se determinarán los recursos requeridos para reducir y corregir las desviaciones que podrían ser identificadas.

7.2.2. Formación, toma de Conciencia y Competencia

La Entidad tiene claro que la adopción del MSPI requiere la participación de profesionales con la formación y las competencias profesionales necesarias para darle cumplimiento a las políticas de Gobierno Digital, y que también se requiere la toma de conciencia de todo el personal de la institución, por esto se ha definido:

- La evaluación y la determinación de las competencias requeridas por el personal que tendrá responsabilidades en el MSPI.
- La realización de un conjunto de actividades de capacitación dirigidas a todo el personal de la institución, orientadas a la concienciación de funcionarios y contratistas con

respecto a los cuidados, mejores prácticas y uso seguro de los activos de información corporativos.

- La contratación de varias sesiones de entrenamiento relacionado con la adopción de un SGSI alineado con ISO/IEC 27001 y con los requisitos del MSPI dirigido a los funcionarios que tendrán responsabilidades asignadas en el nuevo Sistema de Gestión de Seguridad de la Información.
- Realizar una evaluación de la eficacia de las actividades de formación una vez realizadas las sesiones de sensibilización sobre seguridad de la información.
- Construir, llevar y mantener los registros de formación de las diferentes sesiones de entrenamiento y sensibilización del personal de la institución.

8. AUDITORIAS INTERNAS DEL MSPI

La Entidad realizara anualmente un conjunto de auditorías internas alineadas con la norma NTC-ISO 19011:2018, orientadas a validar el cumplimiento de los objetivos de control, la efectividad de los controles administrativos, técnicos y a los procedimientos del Sistema de Gestión de Seguridad de la Información.

Para facilitar la ejecución de estas auditorías, se definirá un Programa Anual de Auditorías documentado, en el que se determinara el periodo de la auditoria, el alcance, los criterios, el método y los auditores que realizaran las actividades.

La ejecución de las auditorias definidas dentro del plan de auditorías será realizada conforme a un Procedimiento para Auditoría Interna construido para garantizar el cubrimiento esperado del alcance del SGSI. Los resultados de las auditorias serán volcados en el informe de auditoría interna.

Las auditorías internas servirán para determinar si se cumplen los requisitos de la norma y de la legislación nacional.

También permitirá conocer si se están cumpliendo con los requerimientos de seguridad de la información de los procesos definidos en el alcance.

De igual forma las auditorías internas servirán para determinar si están implementados todos los controles definidos en el documento de declaración de aplicabilidad y validar su desempeño y efectividad.

9. REVISION DEL MSPI POR LA DIRECCION

La dirección general de la Entidad realizará una vez al año una revisión del Sistema de Gestión de Seguridad de la Información con el fin de verificar la conveniencia, adecuación y la eficacia del SGSI.

Información para la revisión

La siguiente información que será considerada como materia prima para la revisión de la dirección se relacionará en una minuta:

- Informes de Auditoría Interna
- Retroalimentación de las partes involucradas
- Procedimientos del SGSI
- Informe de evaluación y tratamiento de riesgos
- Estado de implementación del Plan de tratamiento de riesgos
- Estado de las no conformidades y medidas correctivas
- Informe sobre el cumplimiento de los objetivos resultado de la revisión del SGSI
- Estado de las actividades de seguimiento posteriores a la última revisión de la dirección.

Resultados de la revisión

En la minuta se incluirá el resultado de la revisión y las decisiones que sean tomadas por la dirección de la entidad con respecto a:

La actualización de los procedimientos y controles relacionados con la seguridad de la información, que podrían incluir:

- Requisitos de la Organización
- Requisitos de seguridad de la información
- Niveles de riesgo
- Niveles de aceptación del riesgo
- Procesos de la entidad que afectan los requisitos de negocio existentes
- Los requerimientos legales
- Requerimientos contractuales

También la actualización de la evaluación de riesgos y el plan de tratamiento de estos.

Los recursos requeridos para facilitar la correcta Gestión de la Seguridad de la Información.

La mejora en la eficacia del SGSI

La mejora de las técnicas de medición de la eficacia de los controles del SGSI

10. MEJORA DEL MSPI

Mejora continua

La entidad adquiere el compromiso de mejorar continuamente la eficacia del Sistema de Gestión de Seguridad de la Información, con el fin de facilitar la administración de este y mantener reducido el riesgo. Para esto la GOBERNACION DE SAN ANDRES Y PROVIDENCIA realizara las siguientes acciones:

- Hará uso de las políticas de seguridad de la información y velará por su cumplimiento.
- Tendrá en cuenta los objetivos de la seguridad de la información
- Considerará para la mejora continua, el resultado de los informes de auditoría del SGSI.
- Realizara el análisis de los eventos a los que se les esté haciendo seguimiento.
- A partir de las desviaciones identificadas en las auditorías y en la revisión de la dirección, se realizarán las acciones preventivas y correctivas que sean necesarias para reducir el riesgo.

Acciones Preventivas

Con el fin de eliminar la causa de las no conformidades potenciales con los requerimientos del SGSI y así reducir la probabilidad de que se vean comprometidos los activos de información de la entidad, se requiere determinar las acciones preventivas apropiadas.

Para facilitar la ejecución de las acciones preventivas, se construirá un procedimiento documentado que permita:

- Identificar no conformidades potenciales y sus causas
- Permitir la evaluación de la necesidad de acciones para impedir que las no conformidades ocurran.
- Determinar las acciones preventivas requeridas.
- Implementar las acciones preventivas necesarias.
- Llevar el registro de los resultados de las acciones realizadas.
- Revisar las acciones preventivas ejecutadas.

Acciones Correctiva

Una vez se identifique alguna desviación, la entidad emprenderá las acciones necesarias para eliminar la causa de las no conformidades asociadas a los requerimientos del SGSI con el fin de prevenir su ocurrencia en el futuro.

Se construirá un procedimiento documentado para las acciones correctivas que permita:

- Identificar no conformidades presentes en el SGSI.
- Determinar las causas de las desviaciones y no conformidades identificadas.
- Evaluar de la necesidad de acciones que garanticen que las desviaciones y no conformidades vuelvan a repetirse.
- Determinar las acciones correctivas requeridas.
- Implementar las acciones correctivas necesarias.
- Registrar el resultado de las acciones realizadas.
- Revisar las acciones correctivas ejecutadas.

11. COMPATIBILIDAD DEL MSPI CON OTROS SISTEMAS DE GESTION

El Sistema de Gestión de la Seguridad de la Información adoptado por la entidad, estará alineado con la norma NTC ISO/IEC 27001, con el fin de facilitar la integración el Sistema de Gestión de Calidad existente, basado en la norma NTC ISO 9001:2018 y cualquier otro sistema de gestión relacionado.

El propietario de este documento es el Oficial de Seguridad de la Información de la institución, quien debe encargarse de actualizarlo por lo menos una vez al año.

12. PLAN DE IMPLEMENTACIÓN DEL MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN.

El Plan de implementación para la dimensión de Seguridad y Privacidad de la Información comprende el siguiente cronograma y se le hace seguimiento.

Gestión	Actividades	Tareas	Responsable de la Tarea	Fechas Programación Tareas	
				Fecha Inicio	Fecha Final
	Definir lineamientos para el levantamiento de activos de información	Actualización de metodología e instrumento de levantamiento de activos de información	Grupo TIC	jun-01-2021	jun-30- 2021
		Socializar la guía de activos de Información.	Grupo TIC	jun-01-2021	jun-30- 2021
		Validar activos de información en el instrumento levantado en la vigencia anterior	Líder de cada proceso, Grupo TIC	jul-01-2021	jul-30-2021

Activos de Información	Levantamiento Activos de Información	Identificar nuevos activos de información en cada dependencia	Líder de cada proceso, Grupo TIC	jul-15-2021	jul-30-2021
		Revisar los instrumentos de activos de Información y realimentar a las áreas con las modificaciones.	Grupo TIC	ago-02-2021	ago-30-2021
		Realizar correcciones a los instrumentos de activos de Información, Cambios físicos de la ubicación de activos de información	Líder de cada proceso	ago-23-2021	ago-30-2021
		Realizar informe de actualización a los activos de información por alguna de las siguientes novedades: Actualizaciones al proceso al que pertenece el activo, Adición de actividades al proceso, Inclusión de un nuevo activo, Cambios o migraciones de sistemas de información en donde se almacenan o reposan activos de la ubicación ya inventariados, Materialización de riesgos que cambien la criticidad del activo.	Líder de cada proceso, Grupo TIC	ago-20-2021	dic-29- 2021
	Publicación de Activos de Información	Validar y aceptar los activos de información para su publicación en el Sistema de gestión por cada líder de proceso.	Líder de cada proceso, Grupo TIC	sept-01- 2021	sept-30-2021
		Consolidar el instrumento de activos de Información.	Equipo de Activos	oct-01-2021	oct-29- 2021
		Publicar los instrumentos de activos de información consolidado en Sistema de gestión	Planeación	dic-01-2021	dic-20- 2021

	Registros activos de información ley 1712	Actualizar el instrumento de Registro Activos de Información con el insumo de los instrumentos de activos de Información.	Grupo TIC	oct-01-2021	oct-29-20
		Publicación del Registro Activos de Información en el sitio web de la Entidad.	Grupo TIC	dic-01-20	dic-20- 2021
Gestión de Riesgos	Actualización de lineamientos de riesgos	Actualizar política y metodología de gestión de riesgos	Grupo TIC	mar-22-2021	ago-31-2021
	Sensibilización	Socialización Guía y Herramienta - Gestión de Riesgos de Seguridad y privacidad de la Información, Seguridad Digital y Continuidad de la Operación	Grupo TIC	abr-19-2021	may-31-2021
	Identificación de Riesgos de Seguridad y Privacidad de la Información, Seguridad Digital y continuidad de la Operación	Identificación, Análisis y Evaluación de Riesgos - Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación	Grupo TIC	may-31- 2021	sep-30- 2021
		Realimentación, revisión y verificación de los riesgos identificados (Ajustes)	Grupo TIC	may-31- 2021	sep-30- 2021
	Aceptación de Riesgos Identificados	Aceptación, aprobación Riesgos identificados y planes de tratamiento	Grupo TIC	jun-21-2021	nov-19-2021
	Publicación	Publicación Matriz de riesgos – Sistema de gestión	Grupo TIC	jun-21-2021	nov-19-2021
	Seguimiento Fase de Tratamiento	Seguimiento Estado planes de tratamiento de riesgos identificados y verificación de evidencias	Grupo TIC	jun-21-2021	dic-20- 2021

	Evaluación de riesgos residuales	Evaluación de riesgos residuales	Grupo TIC	jun-21-2021	dic-20- 2021
	Mejoramiento	Identificación de oportunidades de mejora acorde a los resultados obtenidos durante la evaluación de riesgos residuales	Grupo TIC	jun-21-2021	dic-20- 2021
		Actualización Guía Gestión de Riesgos Seguridad de la información, de acuerdo a los cambios solicitados.	Grupo TIC	jun-21-2021	dic-20- 2021
	Monitoreo y Revisión	Generación, presentación y reporte de indicadores	Grupo TIC - Riesgos	jun-21-2021	dic-20- 2021
	Publicar y Socializar el procedimiento actualizado de incidentes de seguridad de la información	Revisión, actualización y publicación del procedimiento de incidentes de seguridad de la información basado en la norma ISO 27035.	Encargado de la Gestión de Incidentes de Seguridad de la Información.	feb-15-2021	mar-15-2021
		Socializar el procedimiento a los soportes en sitio y Mesa de Servicios, indicando los cambios en el procedimiento	Encargado de la Gestión de Incidentes de Seguridad de la Información.	mar-19-2021	mar-26-2021
		Socializar el procedimiento a los colaboradores de la Entidad.	Encargado de la Gestión de Incidentes de Seguridad de la Información	mar-19-2021	mar-26-2021
	Gestionar los incidentes de Seguridad de la Información identificados	Gestionar los incidentes de seguridad de la información de acuerdo con lo establecido en el procedimiento definido.	Gestión de la Información	ene-1-2021	dic-31- 2021

Gestión de Incidentes de Seguridad de la Información	CSIRT	Socializar los boletines informativos de seguridad, Integrar con CSIRT de Gobierno	Oficial de Seguridad de la Información, Encargado de Seguridad Informática y GIT de Seguridad de la Información de Gobierno Digital	ene-22-2021	dic-15- 2021
	Eventos/vulnerabilidades	Realizar seguimiento a los informes de eventos y vulnerabilidades asociados a SGSI	Encargado de la Gestión de Incidentes de Seguridad de la Información.	ene-22-2021	dic-15- 2021
Plan de Cambio y Cultura de Seguridad y Privacidad de la Información, Seguridad Digital	Elaborar el Plan de Cambio y Cultura de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación	Elaborar el documento del Plan de Gestión de Cultura Organizacional en Apropiación del SGSI	Oficial de Seguridad de la Información, profesional del Grupo de uso y apropiación de TIC	ene-18-2021	ene-29-2021
y Continuidad de la Operación		Publicar y Socializar el Plan de Gestión de Cultura Organizacional en Apropiación del SGSI con los gestores de procesos	Oficial de Seguridad de la Información, profesional del Grupo de uso y apropiación de TIC	ene-29-2021	feb-12- 2021
	Ejecutar el Plan de Cambio y Cultura de Seguridad y Privacidad de la Información,	Implementar las estrategias del Plan de Gestión de Cultura	profesional del Grupo de uso y apropiación	feb-12-2021	dic-20- 2021

	Seguridad Digital y Continuidad de la Operación	Organizacional en Apropiación del SGSI	de TIC, Líderes de procesos y Talento Humano		
	Analizar el Plan de Cambio y Cultura de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación	Analizar los instrumentos de medición del Plan de Gestión de Cultura Organizacional en Apropiación del SGSI	Oficial de Seguridad de la Información, profesional del Grupo de uso y apropiación de TIC	feb-12-2021	dic-20- 2021
Matriz de verificación de Requisitos Legales de Seguridad de la Información	Creación de la Matriz de verificación de Requisitos Legales de Seguridad de la Información	Crear la Matriz de verificación de Requisitos Legales de Seguridad de la Información	Oficina Asesora Jurídica, Oficial de Seguridad de la Información	ene-22-2021	dic-22- 2021
	Revisión de la Matriz de verificación de Requisitos Legales de Seguridad de la Información	Evidenciar el cumplimiento de los Requisitos Legales de Seguridad de la Información	Oficina Asesora Jurídica, Oficial de Seguridad de la Información	jun-21-2021	dic-21- 2021
	Documentación del Análisis de Impacto de la Operación	Actualización del Análisis de Impacto del Negocio	Grupo TIC - Equipo de Continuidad del Negocio	abr-12-2021	dic-21- 2021
		Publicación del Análisis de Impacto del Negocio	Grupo TIC - Equipo de Continuidad del Negocio	dic-6-2021	dic-20- 2021

Plan de Continuidad del Negocio	Documentación de Valoración de Riesgos de Interrupción	Actualización del documento Valoración de Riesgos de interrupción para el plan de continuidad de la operación	Grupo TIC - Equipo de Continuidad del Negocio	abr-12-2021	dic-21- 2021
		Publicación Valoración de Riesgos de interrupción	Grupo TIC - Equipo de Continuidad del Negocio	dic-6-2021	dic-20- 2021
	Documentación de Estrategias de Continuidad	Actualización del documento Estrategias de Continuidad de la Operación	Grupo TIC - Equipo de Continuidad del Negocio	abr-12-2021	dic-21- 2021
		Publicación Estrategias de Continuidad de la Operación	Grupo TIC - Equipo de Continuidad del Negocio	dic-6-2021	dic-20- 2021
	Documentación del Plan de continuidad de la Operación	Crear Documentación del Plan de continuidad de la Operación	Grupo TIC - Equipo de Continuidad del Negocio	abr-12-2021	dic-21-2021
		Aprobación del Plan de continuidad de la Operación	Grupo TIC - Equipo de Continuidad del Negocio	dic-6-2021	dic-20-2021
Acciones correctivas y Notas de	Reporte del estado de las Acciones Correctivas y Oportunidades de Mejora	Generar reporte del estado actual de las AC y OM en SIMIG	Planeación	ene-18-2021	dic-20-2021
		Solicitar el cargue del análisis de causas o plan de tratamiento según sea requerido.	Planeación	ene-18-2021	dic-20-2021

mejoras SGSI	Generar observaciones o recomendaciones a los acompañamientos realizados a los Procesos	Hacer seguimiento a las observaciones o recomendaciones dejadas a los acompañamientos realizados a los Procesos	Planeación	ene-18-2021	dic-20-2021
Planeación	Revisión Manual Políticas de Seguridad de la Información y Resolución de Seguridad de la Información	Actualizar Manual Políticas de Seguridad de la Información y Resolución de Seguridad de la Información.	Oficial de Seguridad de la Información	may-3-2021	may-31-2021
		Informe cumplimiento de los controles por dominios asignados (Políticas, Manual, etc.)	Oficial de Seguridad de la Información	jun-4-2021	dic-21-2021
Gobierno Digital	Gobierno Digital	Actualizar el documento de autodiagnóstico de la entidad en la implementación de Seguridad y Privacidad de la Información.	Oficial de Seguridad de la Información	abr-15-2021	may-14-2021
		Revisar y alinear la documentación del SGSI de la Entidad al MSPI, de acuerdo con la Normatividad vigente.	Oficial de Seguridad de la Información	abr-15-2021	may-14-2021
		Revisar el avance de implementación del Plan de Seguridad Digital en la Entidad	Oficial de Seguridad de la Información	abr-15-2021	may-14-2021
		Reuniones de Socialización de los avances de la implementación del plan de Seguridad Digital y la Estrategia del Modelo de Seguridad y Privacidad de la información	Oficial de Seguridad de la Información	abr-15-2021	may-14-2021
	CCOCI	Cumplimiento requerimientos infraestructuras críticas del gobierno	Oficial de Seguridad de la Información	mar-1-2021	dic-20-2021
Auditorías Internas y Externas	Participación en las auditorías internas y externas de la norma ISO 27001:2013	Participar en las auditorías internas y externas de la norma ISO 27001:2013 programadas en el PAAI	Todos los procesos	De acuerdo con programa de la OCI	De acuerdo con programa de la OCI

Enfoque sectorial	Dar lineamientos en seguridad y privacidad de la información a las entidades adscritas al sector	Realizar mesa sectorial de seguridad y privacidad de la información y seguridad digital y continuidad de los servicios	Oficial de Seguridad y Privacidad de la Información	feb-11-2021	dic-16-2021
		Generar reporte de la información histórica del cumplimiento de seguridad digital de las entidades adscritas al sector	Oficial de Seguridad y Privacidad de la Información	jul-30-2021	dic-27-2021
Revisión de los controles de la norma ISO 27001:2013	Revisión de los controles de la norma ISO 27001:2013,	Aplicar la herramienta diseñada para realizar la validación del cumplimiento de la Política General de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación	Oficial de Seguridad de la Información	jun-4-2021	dic-21-2021
Indicadores SGSI	Provisión de información a los indicadores de medición del SGSI	Formular, Implementar y actualizar los indicadores del SGSI	Oficial de Seguridad de la Información	ene-20-2021	jun-21-2021
		Reportar indicadores	Gestores de procesos	jul-21-2021	dic-21-2021
Vulnerabilidades	Definir lineamientos para ejecutar análisis GAP, análisis de vulnerabilidades y Éthical Hacking	Definir los lineamientos, estudios previos, anexo técnico y el alcance para la realización de análisis GAP, análisis de vulnerabilidades y Éthical Hacking	Oficial de Seguridad	abr-5-2021	abr-30-2021
	Contratar análisis GAP, análisis de vulnerabilidades y Éthical Hacking	Ejecutar el proceso de contratación para realizar análisis GAP, análisis de vulnerabilidades y Éthical Hacking teniendo en cuenta el alcance y metodología	Oficial De Seguridad, Contractual	may-3-2021	jul-30-2021
	Ejecución del contrato	Ejecución del contrato de análisis GAP, análisis de vulnerabilidades y Éthical Hacking de acuerdo al alcance y la metodología establecida	Proveedor	ago-9-2021	nov-30-2021
	Iniciar la ejecución del plan de remediación	Ejecutar el plan de remediación sobre los sistemas y plataforma de acuerdo a los resultados del análisis GAP, análisis de vulnerabilidades y Ethical Hacking	Oficial de Seguridad	dic-1-2021	dic-31-2021

Protección de datos personales	Recolectar bases de datos	Elaborar y emitir un memorando para la recolección de bases de datos personales de acuerdo con los estándares emitidos por la SIC	Oficial de Seguridad y Secretaría General	ene-18-2021	ene-29-2021
	Revisión de bases de datos	Revisar y realimentar la información recolectada por las áreas para el registro de las bases de datos	Oficial De Seguridad y Grupo TIC	feb-1-2021	dic-20-2021
	Registro y actualización de las bases de datos	Registrar o actualizar las bases de datos teniendo en cuenta la información suministrada por las áreas y el levantamiento de activos de información	Oficial de Seguridad	abr-22-2021	dic-20-2021

13. INDICADORES

La medición se realiza con un indicador de gestión que está orientado principalmente a aumentar el nivel de madurez de la implementación y operación del SGSI, para lo cual se utilizará el Instrumento de identificación de la línea base de seguridad, proporcionado por el Ministerio de Tecnologías de la Información y las Comunicaciones.

El avance en ciclo PHVA del sistema debe aumentar frente al diagnóstico actual, para lograr un avance anual.

14. RESPONSABLES

La Secretaría General a través del Grupo TIC asesora a las áreas en el proceso de implementación de controles de seguridad para la protección de la información, y realiza el proceso de sensibilización en Seguridad y privacidad de la información, con el fin de crear un cultura en seguridad que permita minimizar los riesgos a los que está expuesta la información, así mismo los líderes de las áreas cumplen con los procedimientos establecidos para la clasificación y protección de los activos de información que hacen parte de los procesos de cada una de las áreas.

El Grupo TIC hará seguimiento a la implementación del plan, con el fin, de evidenciar en el siguiente ciclo el avance de la madurez del modelo de Seguridad y privacidad de la información.

REFERENCIAS BIBLIOGRAFICAS

1. ISO/IEC 27002, Information Technology. Security Techniques. Code of practice for information security controls
2. Ley 1266 de 2008. Por la cual se dictan las disposiciones generales del Hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones.
3. Ley 1581 de 2012. Por la cual se dictan disposiciones generales para la protección de datos personales.
4. Ley 1712 de 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.
5. Política de Gobierno digital (en donde se encuentra como habilitador el Modelo de Seguridad de la Información)