FASE PLANIFICACION

PLAN DE SEGURIDAD DE LA INFORMACION

VERSIÓN 1.0

15 de Julio de 2019

Contiene 28 páginas

Principales modificaciones por versión de este documento

Historial de Versiones

Versión	Autor	Fecha	Descripción de la Modificación
1.0	Ing. Viviana López B.	15 Julio del 2019	Elaboración de Estructura y Contenido

Este documento ha sido revisado por:

Versión	Revisor	Firma
1.0	Ing. Enrique Santiago	

Este documento ha sido aprobado por:

Versión	Revisor	Firma
1.0		

ÍNDICE DE CONTENIDO

Contenido

1. INTRODUCCIÓN

Este documento hace parte integral de los requisitos del servicio de consultoría limitados a la ejecución del programa de seguridad de la información, 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 GOBERNACION DEL ARCHIPIELAGO DE SAN ANDRES 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 de tratamiento de riesgos resultante del análisis de riesgos realizado en la institución.

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).

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. REQUISITOS GENERALES

La GOBERNACION DEL ARCHIPIELAGO DE SAN ANDRES, PROVIDENCIA Y SANTA CATALINA, a través de los comités de gestión y desempeño institucional, apoyaran e impulsaran 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.

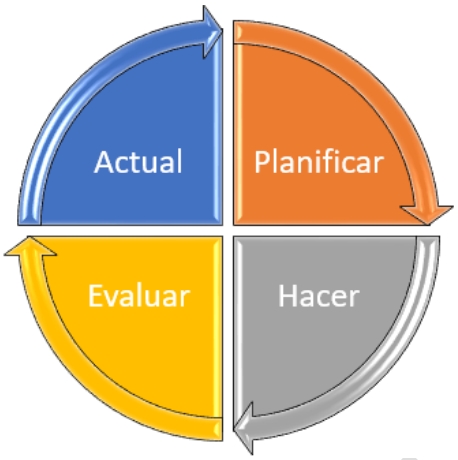

Figura 1: Ciclo de Deming. Fuente: NST S.A.S

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 realizara 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 las 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.

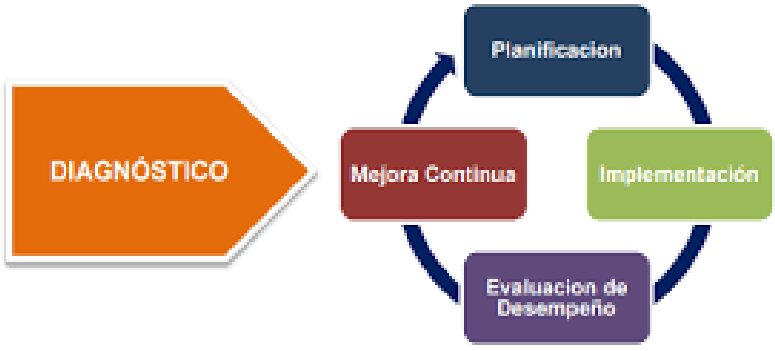

Figura 2: Ciclo de Operación del MSPI, Fuente: MinTIC

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 las 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 ejecutaran 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.

4. 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 Diagnostico. 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, Fuente: NST S.A.S

Fase de Diagnostico

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

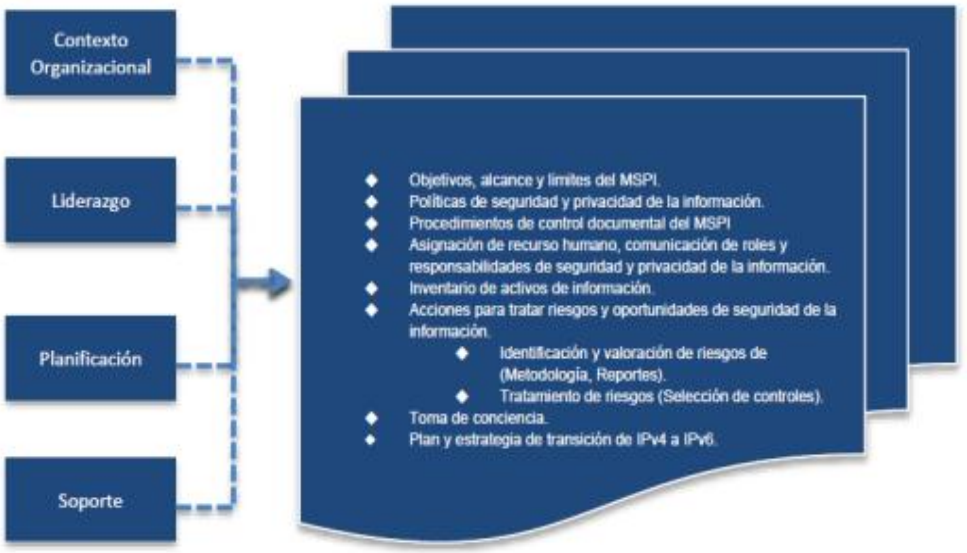

Figura 5. Principales componentes de la fase de Planificación.

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.

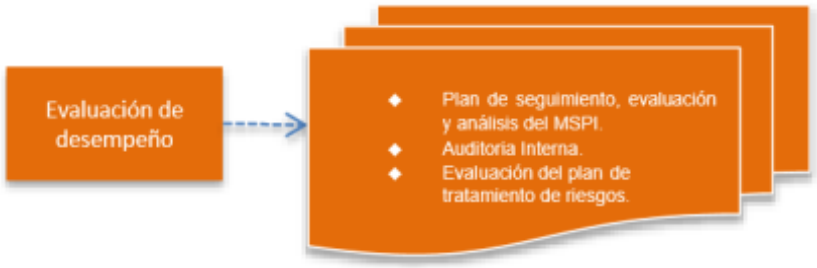

Figura 7: Principales componentes de la fase de Evaluación de Desempeño, Fuente: MinTIC

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. REQUISITOS DE DOCUMENTACION

7.1. Generalidades

La documentación del Modelo de Seguridad y Privacidad de la Información – MSPI incluye registros de las decisiones de la dirección con el fin de que pueda garantizarse que esta, se encuentra alineada con las políticas de la GOBERNACION DE SAN ANDRES, PROVIDENCIA Y SANTA CATALINA, y que se tiene trazabilidad de ella.

Se consideran documentos internos a todos documentos creados dentro de la organización.

7.2. Formato de los documentos

El texto del documento se escribe utilizando fuente Calibri, tamaño 11. Los títulos de capítulo se escriben con tamaño de fuente 14 y en negrita; mientras que para los títulos de capítulo nivel 2 se utiliza el tamaño de

fuente 12 en negrita. Los títulos de capítulo nivel 3 se escriben con tamaño de fuente 11, en negrita y cursiva.

El encabezado del documento incluye el logo Institucional, el nombre del documento, el código, la versión actual, la fecha de creación del documento, la fecha de aprobación y la cantidad de páginas, así como el nivel de confidencialidad. En la última página aparece el control de cambios, quien elaboro, quien reviso y aprobó el documento.

7.3. Aprobación de documentos

Todos los documentos, ya sean documentos nuevos o nuevas versiones de documentos existentes, deben ser aprobados de acuerdo con el nivel al que pertenecen. Los niveles y el encargado de su aprobación se relacionan a continuación:

Nivel del Documento	Debe ser Aprobado por
Políticas	Dirección General
Procedimientos	Director de Proceso/ Jefe de Área/ Comité de Seguridad de la información
Instructivos	Responsable de actividad
Manuales	Responsable de Proceso / Comité de Seguridad de la Información
Bitacoras	Director de Proceso

Todos los documentos deberán ser revisados por el Oficial de Seguridad de la Información y el Comité de Seguridad, si lo amerita.

Los documentos son aprobados de la siguiente forma: El encargado de la aprobación del documento validara la coherencia, la completitud y la seguridad de las acciones contenidas en este como parte del proceso de revisión. Una vez el responsable considere que debe ser aprobado, procederá a informar por correo electrónico al área de Calidad y se cargara al sistema de gestión documental con la etiqueta aprobado (En caso de haber sido montado previamente, se cambiara su estado).

7.4. Publicación y distribución de documentos; retiro de circulación

7.4.1. Documentos con el nivel de confidencialidad más bajo

Para los documentos públicos, para los cuales se permite el acceso de todos los empleados incluidos dentro del alcance del SGSI, el oficial de Seguridad de la Información debe publicarlos en la Intranet, en la carpeta de

DOCUMENTOS PUBLICOS VIGENTES con permisos de solo lectura. Cuando se publica un nuevo documento o una nueva versión del mismo, el Oficial de Seguridad debe informar por correo electrónico a todos los empleados indicados como usuarios del documento". Si es necesario entregar una versión impresa del documento a algunos empleados, esto es responsabilidad del líder de Proceso.

Si hay una versión anterior del documento, el Oficial de Seguridad de la Información debe borrarla de la carpeta de DOCUMENTOS VIGENTES y debe colocarla en la Carpeta de HISTORICO DE DOCUMENTOS (con su respectiva versión). Si existen versiones anteriores de documentos impresos, el Oficial de Seguridad de la Información debe recolectar todos esos documentos y debe destruir todas las copias (aplicando el procedimiento de destrucción de archivos) menos el original firmado, que debe ser debidamente archivado; a esos originales se les debe escribir "Obsoleto" con un marcador.

7.4.2. Documentos con mayor nivel de confidencialidad

Los documentos que tienen un mayor nivel de confidencialidad, de acuerdo a lo especificado en la Política para manejo de INFORMACION PUBLICA CLASIFICADA, y cuya distribución es limitada, son publicados en la Intranet por el propietario del documento con permisos de solo lectura, en una carpeta a la cual se concede permiso de acceso solo a las personas especificadas en la *lista de distribución del documento*. El propietario del documento debe enviar una notificación por correo electrónico sobre este documento a todas las personas de la lista de distribución.

Si existe una versión anterior del documento, el propietario del documento debe borrarla de la carpeta de DOCUMENTOS VIGENTES y debe colocarla en la carpeta que de DOCUMENTOS OBSOLETOS, a la cual pueden acceder sólo las personas especificadas en la *lista de distribución del documento.*

7.5. Actualizaciones de documentos

La persona designada como propietaria del documento tiene la responsabilidad de actualizar el documento. Las actualizaciones se realizan conforme a la frecuencia definida para cada documento, pero, como mínimo, una vez por año.

Todos los cambios del documento deben ser realizados con "Control de cambios", dejando visibles solamente las revisiones sobre la versión anterior, y deben ser detallados en la tabla "Historial de modificaciones".

Es recomendable que cada documento tenga una tabla de "Historial de modificaciones" que se utilice para registrar cada modificación realizada sobre el mismo.

7.6. Control de registros

Cada documento interno en el SGSI debe definir cómo se deben administrar los registros generados a partir del uso de ese documento; es decir, debe especificar lo siguiente: (1) título del registro, (2) ubicación de archivo, (3) persona responsable del archivo, (4) controles para la protección del registro y (5) tiempo de retención.

Los empleados de la organización pueden acceder a registros archivados solamente después de obtener un permiso de la persona designada como responsable del archivo de registros individuales. Si la sensibilidad de determinados registros requiere que el permiso de acceso sea concedido por otra persona, esto debe quedar establecido en el documento interno en cuestión, en el *capítulo que detalla el control de registros.*

Los derechos de acceso y recuperación de registros son determinados por el propietario de los registros individuales. El Oficial de Seguridad de la Información es el responsable de destruir todos los registros cuyo tiempo de retención haya vencido, aplicando la *Política de Destrucción de Información.*

8. RESPONSABILIDAD DE LA DIRECCION

8.1. Compromiso de la dirección

La dirección de la GOBERNACION DE SAN ANDRES, PROVIDENCIA Y SANTA CATALINA tiene claro que la información es uno de los activos más importantes que posee y por esto está comprometida con la ejecución de todas las fases referentes al Modelo de Seguridad y Privacidad de la información, propuesto por MinTIC. Y para asegurar su adopción aprobó el establecimiento de las políticas del Seguridad de la Información, según acto administrativo XXXXXXXXX del XXXX; de la misma forma se creó el rol de Oficial de Seguridad de la información y le fue asignado al Comité Institucional de Gestión y Desempeño, las funciones referentes a la gestión de la Seguridad de la Información según acto administrativo XXXXXX del XXXXX.

Las políticas de seguridad han sido socializadas a partir de su aprobación, según el cronograma definido en el plan de tratamiento de riesgos.

8. ANEXOS

Adjunto a este documento se anexa:

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.

ELABORÓ	REVISÓ Y APROBO
Firma: **Nombre:** Ing. Enrique Santiago **Cargo:** Director de proyectos NST	**Firma:** **Nombre:** **Cargo:**

BIBLIOGRAFÍA:

1. ISO/IEC 27002, Information Technology. Security Techniques. *Code of practice for information security controls*