FASE PLANIFICACION

PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION

VERSIÓN 00

22 de Octubre de 2018

Contiene 11 páginas

ELABORÓ	REVISÓ	APROBÓ
Nombre: Network Security Team Cargo: Contratista Fecha: 22-OCT-2018	Nombre: Grupo TIC Cargo: Fecha: 6-NOV-2018	Nombre: Cargo: Secretaría General Fecha: 14-NOV-2018

Principales modificaciones por versión de este documento

Historial de Versiones

Versión	Autor	Fecha	Descripción de la Modificación
00	Network Security Team	22 Octubre del 2018	Elaboración de Estructura y Contenido

Este documento ha sido revisado por:

Versión	Revisor	Firma
00	Grupo TIC	

Este documento ha sido aprobado por:

Versión	Revisor	Firma
00	Secretaría General	

ÍNDICE DE CONTENIDO

Contenido

1. INTRODUCCIÓN 4
2. DEFINICIONES 4
3. MARCO LEGAL 7
4. DOCUMENTOS DE REFERENCIA 7
5. OBJETIVO 7
6. ALCANCE 7
6.1 Procesos incluidos: 8
6.2 Plataformas Tecnológicas: 8
6.3 Activos de Información 8
6.4 Exclusiones del alcance 8
7. PLAN DE TRATAMIENTO 9
8. ANEXOS 10

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. MARCO LEGAL

Decreto 1078 de 2015: "Modelo de Seguridad y Privacidad de la Información de la estrategia de Gobierno en Línea"

Ley 1581 de 2012 "Por la cual se dictan disposiciones generales para la Protección de Datos Personales Decreto 2693 de 2012"

Política Pública: CONPES 3701 de 2011 Lineamientos de Política para Ciberseguridad y Ciberdefensa, CONPES 3854 de 2016 Política Nacional de Seguridad digital.

4. DOCUMENTOS DE REFERENCIA

Documento de Políticas de Seguridad de la Información: Versión 1.0 construida por la Gobernación de San Andrés y providencia.

Norma ISO/IEC 27001: Elemento de la norma 4.3

Guía de Gestión de Riesgos de MINTIC: publicada en el portal de MINTIC como: articles-5482_G7_Gestion_Riesgos.pdf

5. OBJETIVO

El objetivo del presente documento es definir el plan de tratamiento de los riesgos identificados en los procesos evaluados como parte del programa de seguridad de la información en la GOBERNACION DEL ARCHIPIELAGO DE SAN ANDRES.

6. ALCANCE

El plan de tratamiento de riesgos incluye a todos los activos identificados y valorados en los procesos como parte de la clasificación de activos y en el

análisis de riesgos realizado en la GOBERNACION DEL ARCHIPIELAGO DE SAN ANDRES.

A continuación se relacionan los activos cubiertos en el alcance:

6.1 Procesos incluidos:

Se consideran parte del alcance todos los procesos incluidos el mapa de procesos de la organización, tales como:

- Proceso de Gestión Administrativa y tecnológica
- Proceso de Gestión Documental
- Proceso de Servicio al Ciudadano
- Procesos de Gestión Financiera
- Proceso de Gestión Jurídica
- Proceso de Gestión de Talento Humano

6.2 Plataformas Tecnológicas:

Se consideran parte del alcance todas las plataformas de hardware y software que soportan a los procesos incluidos en el alcance, tales como:

- Plataforma de red cableada
- Plataforma de red Inalámbrica
- Servidores
- Estaciones de trabajo
- Impresoras
- Sitio web
- Sistemas de Información
- Sistemas de seguridad lógica

6.3 Activos de Información

Se consideran parte del alcance todos los documentos lógicos relacionados con los procesos incluidos en el alcance que han sido identificados y clasificados, tales como:

- Documentos electrónicos.
- Documentos físicos.

6.4 Exclusiones del alcance

Todos los activos de información que no han sido relacionados en los apartados anteriores de este documento

7. PLAN DE TRATAMIENTO

Una vez identificados los activos, valorados y evaluado el nivel de riesgos al que se encuentran expuestos, se procede a determinar el tratamiento que habrá de darse a cada uno de ellos, que acciones deberán realizarse, quienes serán los responsables de esta implementación y que procedimientos se ejecutaran para monitorizar y hacer seguimiento de la ejecución de las acciones.

A continuación se relaciona el plan de tratamiento de riesgo propuesto:

ID	Dominio de la Norma	Tratamiento	Acción	Monitorización y Seguimiento	Responsables	% Avance
A.5	POLITICA DE SEGURIDAD DE LA INFORMACION	SI	Reducir	Documento revisión de políticas de seguridad	OSI y Comité	80%
A.6	ORGANIZACION DE LA SEGURIDAD DE LA INFORMACION	SI	Reducir	Documento de Nombramiento de OSI y Comité	OSI y Comité	30%
A.7	SEGURIDAD DE LOS RECURSOS HUMANOS	SI	Reducir	Registro de capacitación en seguridad	OSI y Comité	80%
A.8	GESTION DE ACTIVOS	SI	Reducir	Documento de Clasificación de Activos	OSI y Comité	50%
A.9	CONTROL DE ACCESO	SI	Reducir	Bitácora de revisión de derechos de usuarios	OSI y Comité	2
A.10	CRIPTOGRAFIA	SI	Reducir	Relación de Sistemas que usan cifrado	OSI y Comité	0%
A.11	SEGURIDAD FISICA Y AMBIENTAL	SI	Reducir	Bitácora de registros de acceso físico	OSI y Comité	60%
A.12	SEGURIDAD EN LAS OPERACIONES	SI	Reducir	Bitácora de registro de backups	OSI y Comité	60%
A.13	SEGURIDAD DE LAS COMUNICACIONES	SI	Reducir	Registro de acuerdos de confidencialidad con terceros	OSI y Comité	60%
A.14	ADQUISICION DESARROLLO Y MANTENIMIENTO DE SISTEMAS	SI	Reducir	Separación de Entorno de Producción y desarrollo	OSI y Comité	50%
A.15	RELACIONES CON LOS PROVEEDORES	SI	Reducir	Documento de entendimiento de las políticas de seguridad por parte de los proveedores	OSI y Comité	30%
A.16	GESTION DE INCIDENTES DE SEGURIDAD DE LA INFORMACION	SI	Reducir	Procedimiento documentado de gestion de Incidentes	OSI,Comite, Funcionarios y Contratistas	0%
A.17	ASPECTOS DE SEGURIDAD DE LA INFORMACION DE LA GESTION DE LA CONTINUIDAD DEL NEGOCIO	SI	Reducir	Bitacora de pruebas de los controles de continuidad de las operaciones	OSI y Comite	10%

A.18	CUMPLIMIENTO	SI	Reducir	Documento de politicas de proteccion de datos	OPD, OSI y COMITE	30%

Tabla 1: Plan de tratamiento de riesgo propuesto

A continuación se relaciona el cronograma propuesto para el tratamiento del riesgo identificado:

ID	Dominio de la Norma	Planificación										
		Feb.	Mar.	Abril	Mayo	Jun.	Julio	Agos.	Sept.	Oct.	Nov.	Dic.
A.5	POLITICA DE SEGURIDAD DE LA INFORMACION											
A.6	ORGANIZACION DE LA SEGURIDAD DE LA INFORMACION											
A.7	SEGURIDAD DE LOS RECURSOS HUMANOS											
A.8	GESTION DE ACTIVOS											
A.9	CONTROL DE ACCESO											
A.10	CRIPTOGRAFIA											
A.11	SEGURIDAD FISICA Y AMBIENTAL											
A.12	SEGURIDAD EN LAS OPERACIONES											
A.13	SEGURIDAD DE LAS COMUNICACIONES											
A.14	ADQUISICION DESARROLLO Y MANTENIMIENTO DE SISTEMAS											
A.15	RELACIONES CON LOS PROVEEDORES											
A.16	GESTION DE INCIDENTES DE SEGURIDAD DE LA INFORMACION											
A.17	ASPECTOS DE SEGURIDAD DE LA INFORMACION DE LA GESTION DE LA CONTINUIDAD DEL NEGOCIO											
A.18	CUMPLIMIENTO											

Tabla 2: Cronograma propuesto para la ejecución del plan de tratamiento de riesgo

8. ANEXOS

Adjunto a este documento se anexa:

Plan detallado de tratamiento de Riesgos: Versión 1.0 construida por la Gobernación de San Andrés y providencia.

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.

BIBLIOGRAFÍA:

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