PORTADA

A) HISTORIAL DE CAMBIOS

VERSIÓN	FECHA	JUSTIFICACIÓN DE LA MODIFICACIÓN
1	25/01/2019	Lanzamiento del plan
2	30/10/2019	Se hace referencia a la guía para la administración del riesgo y el diseño de controles en entidades públicas versión 4 del DAFP que contempla la metodología a seguir para identificación y valoración de riesgos de seguridad digital

B) REVISIONES Y APROBACIONES DEL DOCUMENTO

ELABORÓ	REVISÓ	APROBÓ
Nombre: Jesús Goyes Alvarado	Nombre: Armando Delgado Suárez	Francisco Alvaro Ramírez Rivera
Cargo: Contratista Asesor TI Planeación y Sistemas	Cargo: Jefe Oficina Asesora de Planeación y Sistemas	Cargo: Director General
Fecha: 22/10/2019	Fecha: 29/10/2019	Fecha: 30/10/2019

REVISÓ	REVISO
Nombre: Oscar Herrera Isaza	Nombre: Luis Enrique Cortes
Cargo: Contratista Asesor de Calidad	Cargo: Profesional Especializado Unidad de Riesgo Operativo
Fecha: 29/10/2019	24/10/2019

C) LISTA DE DISTRIBUCIÓN

N°	NOMBRE Y CARGO
1	Armando Delgado Suárez Jefe Oficina Asesora de Planeación y Sistemas
2	Jesús Goyes Alvarado Contratista Asesor Planeación y Sistemas
3	Joe Alexander Nuñez Yaguna Profesional Oficina Asesora de Planeación y Sistemas
4	Carolina Tobar Sierra Profesional Especializado Oficina Asesora de Planeación y Sistemas
5	Ricardo Freddy Simbaqueba – Profesional Universitario Oficina Asesora de Planeación y Sistemas
6	Fernando Duque Echeverry – Técnico Operativo Oficina Asesora de Planeación y Sistemas

PLAN PARA EL TRATAMIENTO DE RIESGOS DE SEGURIDAD DE LA INFORMACION V2

TABLA DE CONTENIDO

1. INTRODUCCION

El presente plan, enmarca una serie de actividades a fin de fortalecer la seguridad de la Información, con el propósito de proteger los activos de información de la Entidad, en cualquiera de sus estados ante una serie de amenazas o brechas que atenten contra sus principios fundamentales de confidencialidad, integridad y su disponibilidad.

2. OBJETIVOS

1. Adoptar un plan de tratamiento de riesgos de seguridad de la información, en cumplimiento del Decreto 612 de 2018.

2. Construir el plan tomando en consideración los estándares internacionales NTC/ISO/IEC 27001 e ISO/IEC 27032, como marcos de referencia, así como el contexto del modelo de seguridad y privacidad.

3. Establecer como metodología la guía para la administración del riesgo y el diseño de controles en entidades públicas versión 4 del DAFP, para que cada proceso identifique, adopte y fortalezca su mapa de riesgos, incluyendo riesgos y controles específicos para la seguridad de la información.

3. ALCANCE

Este plan se establece como una herramienta orientadora para todos los servidores públicos de la Entidad, para que junto con la unidad de gestión del riesgo de FONPRECON, permitan y faciliten el desarrollo de las etapas de reconocimiento del contexto, identificación de los riesgos de seguridad de la información, análisis, ~~y~~ evaluación, y opciones de tratamiento o manejo del riesgo según la zona en la que se encuentre, para preservar la seguridad de la información en la entidad; además será aplicada sobre cualquier proceso, sistema de información, y en general sobre el inventario de activos de información de la Entidad.

4. TÉRMINOS Y DEFINICIONES

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 controle en su calidad de tal. Fuente: MinTIC - Modelo de Seguridad y Privacidad de la Información – Glosario

Riesgo: Efecto de la incertidumbre sobre los objetivos.

Riesgo Inherente: Es el nivel de riesgo propio de la actividad, sin tener en cuenta el efecto de los controles.

Riesgo Residual: El riesgo que permanece tras el tratamiento del riesgo o nivel resultante del riesgo después de aplicar los controles.

Riesgo en la seguridad de la información: Potencial de que una amenaza determinada explote las vulnerabilidades de los activos o grupos de activos causando así daño a la organización.

Análisis de riesgos: Es un método sistemático de recopilación, evaluación, registro y difusión de información, necesaria para formular recomendaciones orientadas a la adopción de políticas o medidas, en respuesta a un peligro detectado.

Amenaza: Es la causa potencial de una situación de incidente y no deseada por la organización.

Causa: Es todo aquello que se pueda considerar como fuente generadora de eventos (riesgos), como lo son: las personas, los métodos, las herramientas, el entorno, lo económico, los insumos o materiales entre otros.

Confidencialidad: Propiedad de la información de no ponerse a disposición o ser revelada a individuos, entidades o procesos no autorizados.

Disponibilidad: Propiedad de la información de estar accesible y utilizable cuando lo requiera una persona autorizada o entidad competente.

Integridad: Propiedad de la información relativa a su exactitud y completitud.

Consecuencia: Resultado de un evento que afecta el resultado de los objetivos.

Criterios del riesgo: Términos de referencia frente a los cuales, la importancia de un riesgo es evaluada.

Control: Medida que permite mitigar el riesgo.

Impacto. Cambio adverso en el nivel del logro de los objetivos.

Nivel de riesgo: Magnitud de un riesgo o de una combinación de riesgos, expresada en términos de la combinación de las consecuencias y su probabilidad.

Matriz de riesgos: Instrumento utilizado para ubicar los riesgos en una determinada zona según la calificación cualitativa de la probabilidad de ocurrencia y del impacto de un riesgo.

5. MARCO DE REFERENCIA

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.

Ley Estatutaria 1581 de 2012 y Reglamentada Parcialmente por el Decreto Nacional 1377 De 2013: Por la cual se dictan disposiciones generales para la protección de datos personales.

Decreto 2693 de 2012: Lineamientos generales de la Estrategia de Gobierno en línea de la República de Colombia que lidera el Ministerio de las Tecnologías de Información y las Comunicaciones, se reglamentan parcialmente las Leyes 1341 de 2009 y 1450 de 2011, y se dictan otras disposiciones.

Ley 1273 DE 2009: Por medio de la cual se modifica el Código Penal, se crea un nuevo bien tutelado denominado “de la protección de la información y los datos” y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones.

ISO/IEC 27001:2013: Estándar internacional que define dentro de un marco de referencia, cómo organizar la seguridad de la información.

Decreto 612 de 2018: “*Integración de los planes institucionales y estratégicos al Plan de Acción.* Las entidades del Estado, de acuerdo con el ámbito de aplicación del Modelo Integrado de Planeación y Gestión, al Plan de Acción de que trata el artículo 74 de la Ley 1474 de 2011, deberán integrar los planes institucionales y estratégicos que se relacionan a continuación y publicarlo, en su respectiva página web, a más tardar el 31 de enero de cada año:

…

10. Plan Estratégico de Tecnologías de la Información y las Comunicaciones PETI
11. Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información
12. Plan de Seguridad y Privacidad de la Información”.

6. PLAN DE TRATAMIENTO DE LOS RIESGOS DE SEGURIDAD DE LA INFORMACIÓN.

6.1 REVISIÓN PERIODICA DEL CATALOGO DE ACTIVOS DE INFORMACIÓN

En cumplimiento del artículo 20 de la Ley 1712 de 2014 “Ley de Transparencia”, se debe realizar al menos una vez cada dos años o cuando se estime necesario:

Actividad	Responsable
Coordinar la revisión y actualización del inventario de activos de información, que resulte en un documento exacto, actualizado y consistente, que a su vez permita definir la criticidad de los activos de información, sus propietarios, custodios y usuarios	Oficina Asesora de Planeación y Sistemas Oficina Asesora Jurídica Dirección General Líderes de proceso

6.2 IDENTIFICACIÓN DE RIESGO

En función del catálogo de activos de información, cada proceso identifica riesgos y los incluye en su mapa de riesgos, bajo la asesoría y coordinación de la unidad de riesgo - URO:

Actividad	Responsable
1. La unidad de riesgo operativo, promueve y coordina la revisión del mapa de riesgos al menos una vez al año, o en el evento que el proceso lo solicite o por adopción de directrices y recomendaciones de gobierno.	URO Jefe de Planeación y Sistemas Líderes de proceso
2. Cada vez que hayan cambios en el catálogo de activos de información cada proceso Identifica riesgos para cada activo de información y los documenta en una nueva versión preliminar de su mapa de riesgos,	URO Jefe de Planeación y Sistemas Líderes de proceso
3. Redactar los riesgos en forma clara, basándose en las recomendaciones de la *Guía emitida por la Función Pública para la administración del riesgo y el diseño de controles en entidades públicas versión 4 de octubre de 2018, numeral 2.2.1 Técnicas para la redacción de riesgos.*	URO Líderes de proceso

6.3 CONSTRUCCIÓN E IMPLEMENTACIÓN DE CONTROLES.

Actividad	Responsable
1. En la redacción de un control, se deben integrar las variables indicadas en la *Guía emitida por la Función Pública para la administración del riesgo y el diseño de controles en entidades públicas versión 4 de octubre de 2018, numeral 3.2.2 Valoración de los controles – diseño de controles:* 1.1 Debe tener definido el responsable de llevar a cabo la actividad de control. 1.2 Debe tener una periodicidad definida para su ejecución. 1.3 Debe indicar cuál es el propósito del control. 1.4 Debe establecer el cómo se realiza la actividad de control. 1.5 Debe indicar qué pasa con las observaciones o desviaciones resultantes de ejecutar el control. 1.6 Debe dejar evidencia de la ejecución del control.	URO Líderes de proceso
2. La colección de controles, debe ser revisadas frente a los controles definidos dentro del Anexo A del estándar internacional NTC/ISO/IEC 27001, para verificar que no se han omitido controles necesarios.	URO Jefe de Planeación y Sistemas Líderes de proceso
3. Realice una declaración de aplicabilidad, es decir, indicar cuáles controles han sido adoptados y cuáles no con su respectiva justificación, de la norma NTC/ISO/IEC 27001, para verificar que no se han omitido controles necesarios allí contenidos y en la Guía No. 4 del DAFP.	URO Líderes de proceso

6.4 TRATAMIENTO DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN.

Como resultado de la etapa de evaluación del riesgo tendremos una lista ordenada de riesgos o una matriz con la identificación de los niveles de riesgo de acuerdo con la zona de ubicación, por tanto, se deberá elegir la(s) estrategia(s) de tratamiento del riesgo en virtud de su valoración y de los criterios establecidos en el contexto de gestión de riesgos.

De acuerdo con el nivel evaluación de los riesgos, se deberá seleccionar la opción de tratamiento adecuada por cada uno de los riesgos identificados; el costo/beneficio del tratamiento deberá ser un factor de decisión relevante para la decisión.

COSTO - BENEFICIO	OPCION DE TRATAMIENTO
El nivel de riesgo está muy alejado del nivel de tolerancia, su costo y tiempo del tratamiento es muy superior a los beneficios	**Evitar** el riesgo, su propósito es no proceder con la actividad o la acción que da origen al riesgo (ejemplo, dejando de realizar una actividad, tomar otra alternativa, etc.)
El costo del tratamiento por parte de terceros (internos o externos) es más beneficioso que el tratamiento directo	**Transferir o compartir** el riesgo, entregando la gestión del riesgo a un tercero (ejemplo, contratando un seguro o subcontratando el servicio).
El costo y el tiempo del tratamiento es adecuado a los beneficios	**Reducir o Mitigar** el riesgo, seleccionando e implementando los controles o medidas adecuadas que logren que se reduzca la probabilidad o el impacto
La implementación de medidas de control adicionales no generará valor agregado para reducir niveles de ocurrencia o de impacto.	**Retener o acepta**r el riesgo, no se tomará la decisión de implementar medidas de control adicionales. Monitorizarlo para confirmar que no se incrementa

La unidad de riesgo URO apoya el tratamiento de riesgos, a cada uno de los mapas de riesgos por proceso.

6.5 MONITOREO Y SEGUIMIENTO DE LOS RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

Corresponderá a los líderes de proceso, monitorear e informar a la Unidad de Riesgo Operativo el cumplimiento de los controles establecidos, teniendo en cuenta los siguientes períodos:

Riesgo Extremo o Alto → Mensualmente
Riesgo Moderado → Bimensualmente
Riesgo Bajo → Trimestralmente

La unidad de riesgo URO, realizará la verificación de los controles monitoreados, para la correspondiente valoración y seguimiento a los mismos.