PLAN DE GESTIÓN DE RIESGOS DE SEGURIDAD DIGITAL

Departamento Administrativo de la Defensoría del Espacio Público

2019

TABLA DE CONTENIDO

Tabla de Ilustraciones

1 INTRODUCCIÓN

La gestión de riesgos de seguridad digital establece procesos, procedimientos y actividades encaminados a lograr un equilibrio entre la prestación de servicios y los riesgos asociados a los activos de información que dan apoyo y soporte en el desarrollo de la misionalidad de la entidad. En tal sentido, se debe considerar e implementar medidas que implican tiempo, esfuerzos y recursos necesarios para dar un adecuado tratamiento a los riesgos, generando una estrategia de seguridad digital efectiva que controle y administre la materialización de eventos o incidentes, mitigando los impactos adversos o considerables al interior de la entidad.

2 OBJETIVO GENERAL

Establecer un marco de gestión de riesgos de digital a través del cual se mitiguen las vulnerabilidades y amenazas asociados a los activos de información del Departamento Administrativo de la Defensoría del Espacio Público – DADEP, con el fin de lograr niveles de aceptación razonable del riesgo en relación con los atributos de disponibilidad, integridad y confidencialidad de la información de la entidad.

2.1 Objetivos específicos

- Evaluar y analizar los riesgos de seguridad digital relacionados a los activos de información para facilitar el desarrollo de la misionalidad del Departamento Administrativo de la Defensoría del Espacio público.
- Identificar las amenazas e impactos de seguridad digital asociadas a los procesos de la entidad.
- Identificar e implementar controles que atiendan la gestión de riesgos y facilite la toma de decisiones sobre el riesgo residual.
- Definir el plan de tratamiento del riesgo residual de la entidad.

3 ALCANCE

El alcance del plan de gestión de riesgos de seguridad digital inicia con la definición del contexto estratégico de los riesgos de seguridad digital a los que está expuesta la entidad dando cubrimiento a los procesos estratégicos, misionales, de soporte, de verificación y mejora; y concluye con el plan de acción mediante el cual se realizará el tratamiento, monitoreo y revisión de los riesgos de seguridad digital identificados.

4 DEFINICIONES Y SIGLAS

4.1 Definiciones

Para la adecuada gestión de riesgos de seguridad digital se debe manejar con propiedad los siguientes términos:

- **Activo:** [Según **ISO 27000**]: En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de la misma (sistemas, soportes, edificios, personas...) que tenga valor para la organización.
- **Amenaza:** [Según **ISO 27000**]: Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización.
- **Análisis del riesgo:** [NTC ISO 31000:2011]: Proceso sistemático para comprender la naturaleza del riesgo y determinar el nivel de riesgo.
- **Apetito de riesgo**: Es el nivel máximo de riesgo que la entidad está dispuesta a asumir.
- **Consecuencia:** [NTC ISO 31000:2011]: Resultado o impacto de un evento que afecta a los objetivos.
- **Controles:** [Según ISO 27000]: Las políticas, los procedimientos, las prácticas y las estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido. Control es también utilizado como sinónimo de salvaguarda o contramedida. En una definición más simple, es una medida que modifica el riesgo.
- **CSIRT:** Equipo de Respuesta a Incidentes de Seguridad Informática
- **Criterios del riesgo:** [Según NTC ISO 31000:2011]: Términos de referencia frente a los cuales se evalúa la importancia de un riesgo.
- **Evaluación del riesgo:** [Según NTC ISO 31000:2011]: Proceso de comparación de los resultados del análisis del riesgo, con los criterios del riesgo, para determinar si el riesgo, su magnitud o ambos son aceptables o tolerables.
- **Identificación del riesgo:** [Según NTC ISO 31000:2011]: Proceso para encontrar, reconocer y describir el riesgo.

- **Impacto:** [Según ISO 27000]: El coste para la empresa de un incidente -de la escala que sea-, que puede o no ser medido en términos estrictamente financieros -p.ej., pérdida de reputación, implicaciones legales, etc.

- **Inventario de activos:** [Según ISO 27000.ES]: Sigla en inglés: Assets inventory. Lista de todos aquellos recursos (físicos, de información, software, documentos, servicios, personas, intangibles, etc.) dentro del alcance del SGSI, que tengan valor para la organización y necesiten, por tanto, ser protegidos de potenciales riesgos.

- **Nivel de riesgo:** [Según NTC ISO 31000:2011]: Magnitud de un riesgo o de una combinación de riesgos expresada en términos de la combinación de las consecuencias y su probabilidad.

- **Perfil del riesgo:** [Según NTC ISO 31000:2011]: Descripción de cualquier conjunto de riesgos.

- **Política:** [Según ISO/IEC 27000:2016]: Intenciones y dirección de una organización como las expresa formalmente su alta dirección.

- **Política:** para la gestión del riesgo [Según NTC ISO 31000:2011]: Declaración de la dirección y las intenciones generales de una organización con respecto a la gestión del riesgo.

- **Reducción del riesgo:** [Según NTC ISO 31000:2011]: Acciones que se toman para disminuir la posibilidad, las consecuencias negativas o ambas, asociadas con un riesgo.

- **Riesgo:** [Según ISO 27000]: 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.

- **Riesgo Residual:** [Según ISO 27000]: El riesgo que permanece tras el tratamiento del riesgo.

- **Vulnerabilidad:** [Según ISO 27000]: Debilidad de un activo o control que puede ser explotada por una o más amenazas.

4.2 Siglas

- DADEP: Departamento Administrativo de la Defensoría del Espacio Público.

- SIDEP: Sistema de Información del Espacio Público.

- SIDGDEP: Sistema Geográfico del Espacio Público.
- CPM: Sistema de acciones correctivas, preventivas y/o de mejora. k. MAP: Modelo de Autoevaluación por Procesos.

5 PLAN DE GESTIÓN DE RIESGOS DE SEGURIDAD DIGITAL

El Departamento Administrativo de la Defensoría del Espacio Público – DADEP siguiendo los lineamiento trazados por el Gobierno Nacional con lo expuesto en la Ley de transparencia 1712 de 2014, la Estrategia Gobierno en Línea y la Política de Gobierno Digital. Establece un plan de gestión de riesgos de seguridad digital en el cual se identifiquen las amenazas, las vulnerabilidades, el impacto y el nivel de riesgo asociados a los activos de información sin importar el nivel de criticidad que tienen para la entidad.

En la gestión de riesgos de seguridad digital resulta importante lograr una aceptación de los riesgos con base en las posibles consecuencias de afectación; establecer una estrategia de mitigación adecuada que logre un entendimiento y aceptación del riesgo residual así como de los recursos empleados en relación costo-beneficio con el fin de emplear medidas para salvaguardar, proteger y custodiar la información de las aplicaciones, servicios tecnológicos, bases de datos, redes de comunicaciones, equipos de cómputo y documentos físicos garantizando la disponibilidad, confidencialidad e integridad de la información.

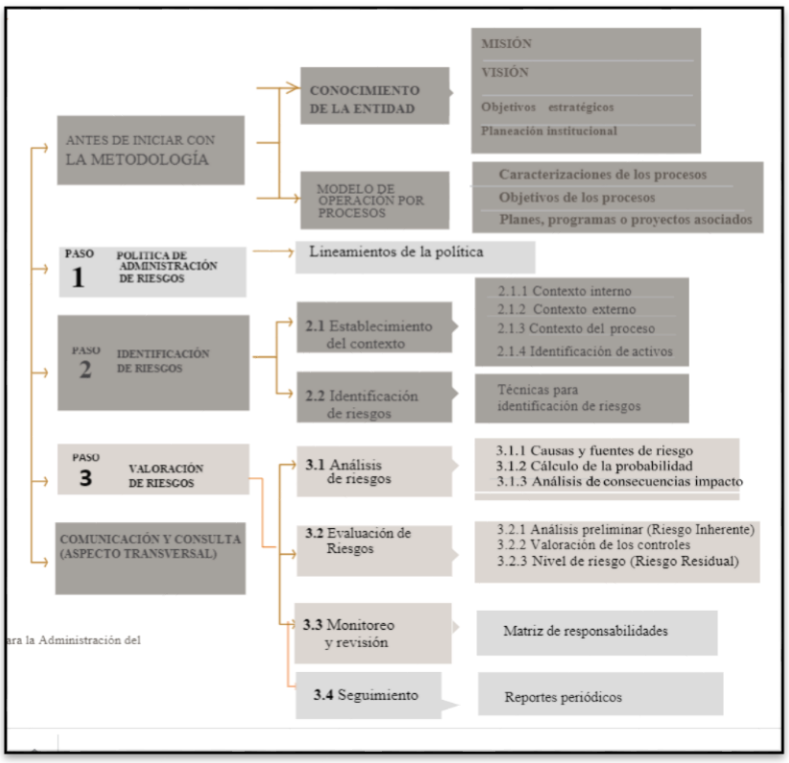
Por consiguiente, resulta indispensable definir actividades que de manera articulada permitan implementar medidas de control que coadyuven a la prevención, contención y mitigación de amenazas a las que se encuentran expuestos los activos de información de la entidad por medio de una metodología descrita a continuación:

5.1 FASE DE PLANIFICACIÓN

5.1.1 Metodología de gestión de riesgos de seguridad digital

El Departamento Administrativo para la Defensoría del Espacio Público – **DADEP** adoptará la metodología de la guía para la Administración de los Riesgos de Gestión, Corrupción y Seguridad Digital de la Presidencia de la Republica complementando con buenas prácticas del estándar ISO-27005.

Ilustración 1 Metodología para la Administración de Riesgos

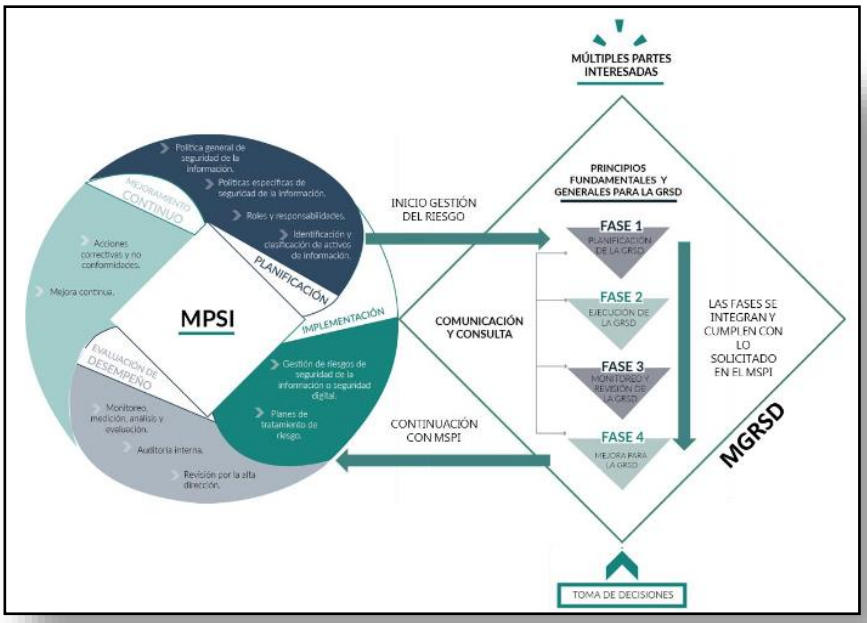


Fuente: Guía Para la Gestión de Riesgos de Seguridad Digital

En la ilustración 1. **Guía para la Administración de los Riesgos de Gestión, Corrupción Seguridad Digital y el Diseño de Controles en Entidades** se propone una metodología que a través de fases y actividades, permite gestionar los riesgos de seguridad digital a los que están expuestos los activos de información del DADEP.

Por su parte, el Plan de Gestión de Riesgos de Seguridad de la Información que hace parte del Modelo de Seguridad y Privacidad de la Información MSPI se integra con cada una de las fases propuestas en el Modelo de Gestión de Riesgos de Seguridad Digital MGRSD como se observa en la ilustración 2.

Ilustración 2 Interacción entre el MSPI y el MGRSD



Fuente: Ministerio de Tecnologías de la Información y las Comunicaciones

5.1.2 Contexto Estratégico

El Departamento Administrativo de la Defensoría del Espacio Público creado mediante acuerdo del Distrito Capital 018 del 31 de julio de 1999, tiene como principal función definida en el artículo 3 *"Son funciones de la Defensoría del Espacio Público, sin perjuicio de las atribuciones de otras autoridades, la defensa, inspección, vigilancia, regulación y control del espacio público del Distrito Capital; la administración de los bienes inmuebles, y la conformación del inventario general del patrimonio inmobiliario Distrital"*. Por consiguiente, todas las acciones encaminadas sobre la gestión de riesgos de seguridad digital, están orientadas hacia la protección de la disponibilidad, integridad y confidencialidad de los datos e información que se crea, se procesa, se almacenada y se trasmite, previniendo la materialización de amenazas que puedan impactar de forma considerable la información concerniente a la defensa del espacio público y de la administración de bienes inmuebles que hacen parte de la ciudad.

5.1.2.1 Contexto Externo

A nivel nacional, el 17 de Octubre el Congreso de la República decretó la Ley 1581 por medio de la cual se establece un derecho fundamental de las personas para conocer, actualizar y rectificar toda información de carácter personal que recogida en las diferentes bases de datos o archivos de entidades de carácter público o privado. Por lo que toda información de carácter personal que se encuentra en los distintos medios o dispositivos de almacenamiento del DADEP, debe contemplar medidas de protección de dicha información de modo que no se vea afectada la integridad y buen nombre de las personas.

Así mismo, el 6 de marzo de 2014 el Congreso de la República estableció la Ley 1712 por medio de la cual se creó la ley de transparencia y del derecho de acceso a la información pública nacional. Por lo cual se convierte en un derecho constitucional para la personas el poder acceder a la información de carácter público que les permita realizar estudios de tipo estadísticos, científico o que simplemente les permita estar informados. En razón a esto, el DADEP está comprometido con la identificación y clasificación de todo tipo de información que es creada, almacenada, administrada y publicada, permitiendo así dar correcto cumplimiento a lo establecido en esta ley.

De acuerdo con el plan de desarrollo Bogotá 2016 – 2020 **"BOGOTÁ MEJOR PARA TODOS"**, el DADEP se encuentra alineado con el segundo pilar definido allí como **DEMOCRACIA URBANA - Espacio público, derecho de todos,** en donde se requiere *"…..transformar e incrementar del espacio público como un escenario democrático, seguro y de calidad….."* y para esto, se hace preciso realizar una adecuada gestión de los riesgos de seguridad de información y de los riesgos de seguridad digital sobre el sistema de información geográfica **SIGDEP** y el sistema de información misional **SIDEP** de tal manera que el DADEP contribuya con los proyectos y programas que forman parte del actual plan de desarrollo del Distrito.

Por su parte, el Ministerio de Tecnologías de la Información y las Comunicaciones **MINTIC** el 14 de Junio de 2018 estableció el decreto 1008 *"Por el cual se establecen los lineamientos generales de la política de Gobierno Digital y se subroga el capítulo 1 del título 9 de la parte 2 del libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones"* que por medio del uso de tecnologías de la información y las comunicaciones permita lograr una mejor competitividad, proactividad e innovación en la ciudadanía y el Estado, por lo que el DADEP desempeña un papel importante con la implementación de recursos tecnológicos que le permita alcanzar los propósitos que dispone esta ley, gestionando los riesgos y amenazas que traigan consigo la implementación de nuevas tecnologías de la información o avances tecnológicos.

5.1.2.1 Contexto Interno

El DADEP posee una estructura organizacional con procesos estratégicos, misionales, de Soporte, de verificación y mejora caracterizados en el Sistema Integrado de Gestión que permiten realizar la identificación, tratamiento, monitoreo y revisión de los riesgos de seguridad digital más críticos de la entidad que pueden impactar de manera considerable el desarrollo de funciones y logro de objetivos propuestos. Adicionalmente, se cuenta con distintos sistemas de información y servicios tecnológicos que soportan los procesos y por lo cual es necesario velar por la protección y seguridad de estos activos de información.

En el contexto interno, el DADEP definió el Plan Estratégico 2016 – 2020 el cual contempla 5 objetivos corporativos que permiten contribuir en la mejora de la calidad de vida de los ciudadanos, así como proteger por la integridad del espacio público y del patrimonio inmobiliario del distrito. En razón a esto, la gestión de riesgos de seguridad digital se alinean en función de velar por la disponibilidad, confidencialidad e integridad de los datos e información que se encuentran en el sistema de información misional **SIDEP**, el sistema de información geográfica **SIGDEP** y el sistema de gestión documental **ORFEO**. Logrando con esto, la consolidación del sistema de información misional de la entidad además de poder atender de forma ágil y oportuna los requerimientos de la ciudadanía.

De igual modo, con la definición del Plan Estratégico de Tecnologías de la Información **PETI** formulado para el DADEP, se propone un modelo integral de gestión de las Tecnologías de la Información desarrollado a partir de ocho componentes que se articulan para el logro de los objetivos corporativos formulados en el plan estratégico vigente en la entidad. En razón a esto, los esfuerzos para la administración de riesgos de seguridad digital están orientados hacia el logro de cada uno de estos componentes en donde las tecnologías de la información sean un agente de transformación digital estratégico en la entidad.

Durante los años 2016 y 2017 la entidad definió y adopto la Política de Seguridad de la Información y el manual de Gestión de Seguridad de la Información que forman parte del Subsistema de Gestión de Seguridad de la Información. Estos documentos describen lineamientos y directrices para la gestión de la seguridad de la información y sirven como mecanismos para la mitigación de riesgos asociados a los activos de información de la entidad.

5.1.2.2 **Contexto del Proceso**

El Plan de Gestión de Riesgos de Seguridad Digital hace parte del Plan de Seguridad y Privacidad de la Información definido por la entidad y los cuales hacen parte del proceso de soporte nombrado “GESTIÓN DE LA INFORMACÓN Y LA TECNOLOGÍA” que tiene como objetivo:” Garantizar la disponibilidad de las Tecnologías de la Información y Comunicaciones -TIC's, manteniendo la integridad y confidencialidad de la información”, así mismo, se han establecidos procedimientos, políticas, guías, manuales y formatos que dan soporte a la gestión de seguridad de la información.

5.1.3 Política de Gestión Riesgos

La Política de gestión de riesgos de seguridad digital GRSD definida para la entidad, se encuentra integrada en el documento titulado "Política de Operación del Riesgos del DADEP".

5.1.4 Roles y Responsabilidades

La gestión de riesgos de seguridad digital es una responsabilidad que se debe apropiar por las dependencias, funcionarios y/o contratistas al interior del DADEP. Por lo cual se debe contemplar las funciones establecidas en el documento de roles y responsabilidades **"127-GUIGI-02 Guía de Roles y Responsabilidades de Seguridad de la Información".**

5.1.5 Definición de Recursos para la Gestión de riesgos de seguridad digital.

Los recursos destinados para la gestión de riesgos de seguridad digital provienen del proyecto de inversión Fortalecimiento de la plataforma tecnológica del DADEP y del rubro de funcionamiento Gastos de Transporte y Comunicaciones. Donde parte de estos recursos son destinados a la adquisición de software e infraestructura tecnológica que coadyuve a la reducción de riesgos de seguridad digital y finalmente, contratación de personal con formación y conocimiento en gestión de seguridad de la información.

5.1.6 Identificación de los activos de seguridad digital.

El DADEP posee un inventario y clasificación de los activos de información valorados con su nivel de criticidad de acuerdo a los atributos de integridad, disponibilidad y confidencialidad, los cuales ayudan a determinar los controles y medidas que protejan y salvaguarden los activos de información son los más importantes y críticos dentro de los procesos y procedimientos de la entidad.

5.1.7 Identificación de los Riesgos Inherentes de seguridad digital

La Entidad comprendiendo la necesidad de proteger los activos de información relacionados con los sistemas de información, redes de comunicaciones y servicios web, ha destinado recursos para la adquisición e implementación de controles de tipo tecnológicos, procedimentales y operacionales, mitigando de esta forma la exposición a riesgos en el ámbito cibernético que pueden afectar la integridad, confidencialidad y disponibilidad de los datos e información.

Sin embargo, una actividad previa que ayuda a la identificación de riesgos de seguridad digital consiste en tener consolidado y clasificado los activos de información de la entidad de acuerdo a los atributos de confidencialidad, integridad y disponibilidad que defina el grado o nivel de criticidad que poseen los activos para la entidad.

En esta etapa se identifica las fuentes que originan el riesgo así como factores internos o externos por los cuales se presentan las vulnerabilidades, amenazas e impactos haciendo uso de métodos como lluvia de ideas, juicios de expertos y análisis de escenarios entre otro. Es necesario lograr identificar los agentes

generadores de causas, así como la descripción de los riesgos y las situaciones o consecuencias que se presentan producto de la materialización de los riesgos sobre los procesos del DADEP. En razón a esto, las actividades de esta etapa deben serán enfocadas a los riesgos potenciales que ocasionen una incidencia negativa sobre el desarrollo de los objetivos de los procesos estratégicos, misionales, de soporte, de verificación y mejora caracterizados en el Sistema Integrado de Gestión.

En la valoración de riesgos se identifican los controles existentes que el DADEP ha establecido a través de recursos tecnológicos, procesos y políticas para realizar el tratamiento de los riesgos. Sobre estos controles se verifica la efectividad y de acuerdo al análisis de riesgos realizado, se establecen cual son las prioridades que hay que atender de acuerdo al riesgo de y seguridad digital que pueda afectar los activos de información de la entidad.

5.1.8 Identificación y evaluación de los controles existentes.

En la actualidad la Oficina de Sistemas ha realizado algunas evaluaciones acerca de la efectividad de los controles, lo cual le ha permitido destinar recursos para la adquisición de soluciones tecnológicas de seguridad que mejoran la protección de los activos que se encuentran expuestos a diferentes niveles y perfiles de riesgos a través de Internet.

No obstante, en el análisis de riesgos se define la metodología de estimación del riesgo asignando valores y atributos a la probabilidad de que se materialice alguna amenaza afectando la seguridad de los activos de información, al igual que los valores y atributos sobre el impacto que puede afectar a la entidad producto de la materialización de los riesgos.

En esta etapa se debe especificar si el control es de tipo preventivo, detectivo o correctivo. El tiempo o periodicidad con que el control se implementará y los responsables de ejecutar el control. Adicionalmente, se realizará una evaluación a la efectividad de cada control para validar que el impacto de riesgo se logró minimizar alcanzando niveles deseados de aceptación del riesgo. Por lo tanto, resulta indispensable tener un tablero de control o un mapa de riesgos en donde se realice seguimiento y revisión a la efectividad de los controles implementados y de esta manera determinar acciones sobre el riesgos residual

Para realizar el análisis de riesgos de seguridad digital este plan adopta los criterios para la evaluación de riesgos que se encuentran definidos en el documento **Guía de Administración de Riesgos 127-GUIDE-05** que hace parte del sistema de gestión de calidad del **DADEP.**

5.1.9 Tratamiento de los riesgos de seguridad digital

De acuerdo a la valoración de los riesgos de seguridad digital realizada, se determinan las opciones para tratar los riesgos a través de políticas que permitan controlar y hacer seguimiento sobre la gestión realizada a los riesgos con estrategias de tratamiento en donde se tome decisiones para mitigar, retener, transferir o asumir los riesgos. En razón a esto, la formulación de políticas deberán contemplan los objetivos a alcanzar, una estrategia de cómo se desarrollarán las políticas a corto, mediano y largo plazo, indicar qué riesgos se van a priorizar y controlar, estimar los recursos necesario y finalmente hacer seguimiento a la efectividad de las políticas de administración de riesgos de seguridad digital definidas. Por consiguiente, la política de administración del riesgo se articulará con lo establecido en el documento estratégico denominado **127-GUIDE-05 - Guía de Administración de Riesgos** con el propósito de integrar los objetivos, estrategias, la comunicación, la revisión y ciclo de control de los riesgos a los que se ve expuesta la entidad

5.1.10 Plan de Tratamiento de los riesgos de seguridad digital e indicadores para la gestión del riesgo.

La evaluación de riesgos realizada tendrá un mapa de riesgos inherente en cual de detalle la identificación de riesgos de los riesgos, las vulnerabilidades asociadas a los activos de información y los procesos, las eventuales y potenciales amenazas se seguridad digital y de la información y por último, un listado de controles que mediante su implementación se logre reducir el nivel de riesgo a un estado tolerable o de aceptación por parte de los gestores o dueños de proceso y la dirección del DADEP. Posteriormente se contará con un mapa de riesgo residual que determinará la probabilidad de ocurrencia e impacto de la materialización de los riesgos producto de la implementación de controles.

5.2 FASE DE EJECUCIÓN

Actualmente al interior del DADEP ya se cuenta con controles y procesos que se pueden definir como **AD Hoc** y estos han logrado que exista una reducción en la exposición de los activos de información frente a riesgos inherentes del entorno cibernético.

Ahora bien, en esta fase se seguirá la ruta definida para la aplicación de controles, los cuales estarán a cargo de su implementación en los tiempos definidos, los responsables o líderes de proceso con el apoyo de la Oficina de Sistemas en lo concerniente a controles tecnológicos e informáticos, también será necesario contar con el apoyo y compromiso del responsable de la seguridad digital que brinde conocimiento, apoyo y experticia en la aplicación de los controles.

5.3 FASE DE MONITOREO Y REVISIÓN

Dado que el origen y tipos de riesgos son variables, el monitoreo constante será necesario para detectar cambios respecto a nuevos activos de información, nuevos procesos o procedimientos, nuevos factores o amenazas que afecten los activos de información, nuevas vulnerabilidades, incremento del impacto e incluso la materialización de incidentes de seguridad digital.

5.3.1 Registro y reportes de incidentes de seguridad digital

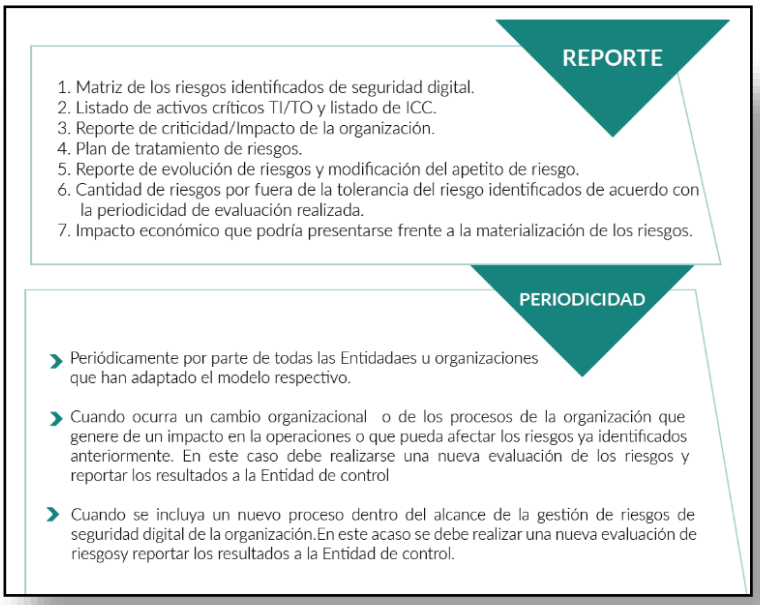
A la fecha, la Oficina de Sistemas ha gestionado eventos e incidentes que han afectado la seguridad digital en la entidad con un impacto bajo por lo que no ha sido necesario aún realizar reporte al Centro Cibernético Policial y al Equipo de Respuesta a Incidentes de Seguridad Informática **CSIRT.** Sin embargo, durante esta etapa se trabajará de forma proactiva para para poder detectar la materialización de incidentes de seguridad digital de manera oportuna, será necesario poder realizar un diagnósticos preciso de la materialización de los incidentes, desarrollar e implementar estrategias para la gestión, contención y mitigación de los daños causados por los incidentes. Se trabajará de manera eficaz con usuarios, gestores de proceso y la Oficina de Sistemas para la restauración de los activos de información afectados por el incidente y como acciones de mejora para prevenir futuras recurrencias del incidentes, se trabajará en la identificación de causa raíz e implementación de mejoras y controles que ayuden a la protección de los distintos activos de información.

Se realizará la comunicación respectiva para reportar a las entidades competentes la afectación causada por los incidentes de modo que se pueda recibir colaboración por parte de dichas entidad en la solución de los incidentes.

5.3.2 Reporte de la gestión de riesgos de seguridad digital al interior de la entidad.

En esta actividad el DADEP desarrollará planes de comunicación y administración de los riesgos de seguridad digital asignando responsables, acciones, medidas de control y orientación detallada sobre los riesgos priorizados que se van a tratar.

Ilustración 3 Reporte de Información



Fuente: Ministerio de Tecnologías de la Información y las Comunicaciones

La ilustración 3 detalla las actividades necearías para realizar el reporte y la periodicidad con que se deberá llevar a cabo el reportes de información.

5.3.3 Reportes de la gestión de riesgos de la seguridad digital a autoridades o entidades especiales.

Toda la administración y gestión de riesgos de seguridad digital realizada por el DADEP será reportada a las entidades competentes de manera proactiva con el ánimo de que esta información pueda contribuir al Gobierno Nacional a mejorar la seguridad de la información en el ámbito cibernético y digital.

5.3.4 Auditorías internas y externas

La Oficina Asesora de Control Interno se encargará de identificar las acciones de mejora necesarias para lograr una efectiva gestión de riesgos de seguridad digital y permita esto salvaguardar los activos de información de la entidad.

5.3.5 Medición del desempeño.

Se formularán métrica e indicadores que resalten el trabajo realizado sobre la gestión de riesgos de seguridad digital, evaluando la eficiencia y efectividad de los controles dispuestos a fin de poder tomar decisiones a nivel directivo sobre el cumplimiento de los objetivos propuestos.

5.4 FASE DE MEJORAMIENTO CONTINUO DE LA GESTION DE REISGOS DE SEGURIDAD DIGITAL.

El DADEP trabajará en la mejora continua de la gestión de riesgos de seguridad digital velando por la mitigación de vulnerabilidades, amenazas, riesgos, eventos e incidentes que atenten contra la disponibilidad, integridad y confidencialidad de los datos e información asociada a los distintos activos de información como parte de los procesos de la entidad y se llevaran a cabo las acciones necesarias para atender los hallazgos o no conformidades producto de auditorías internas y externas.

6 PLAN DE TRABAJO

Las actividades formuladas en el plan de gestión de riesgos de seguridad digital se encuentran en el documento anexo Plan de trabajo.xlsx:

CONTROL DE CAMBIOS		
VERSIÓN	**FECHA**	**DESCRIPCIÓN DE MODIFICACIÓN**
2.0	**30/01/2018**	**Ajuste en la definición de actividades que hacen parte del plan de trabajo**

AUTORIZACION		
Elaboró: Carlos Rojas Villamil Contratista Oficina de Sistemas	**Revisó:**	**Aprobó:** Julio Alexander Hernández Martínez Jefe Oficina de sistemas