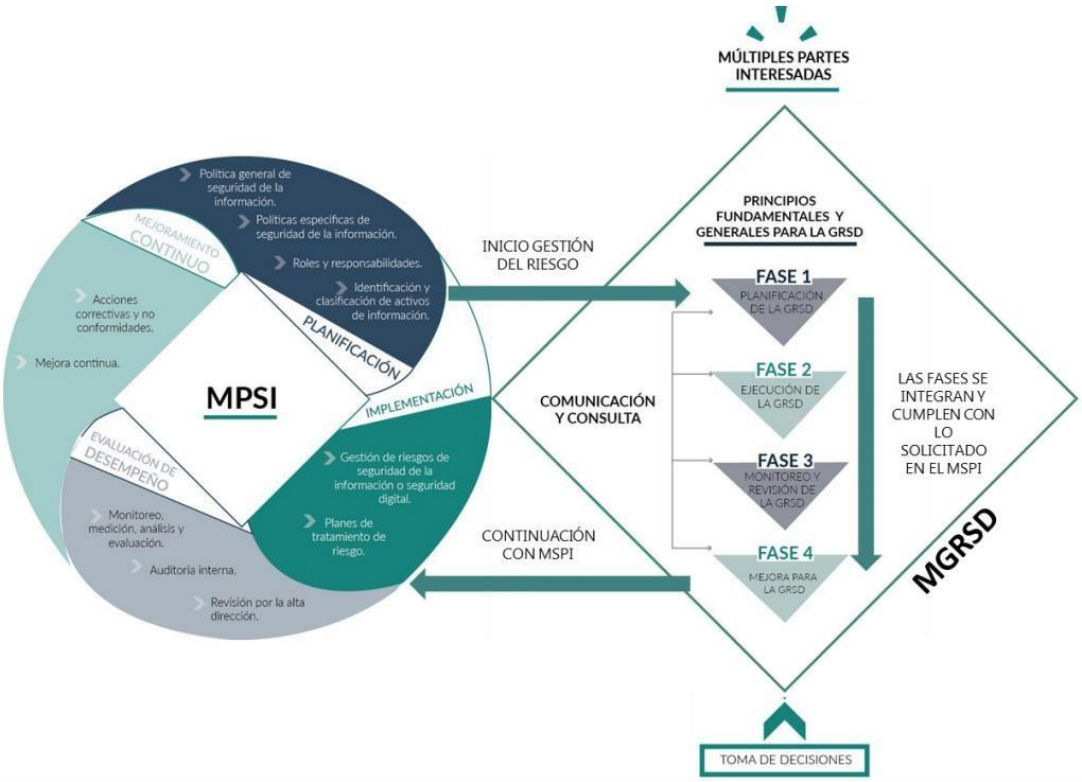
2021

Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información



Gobernación de Boyacá | Secretaría de TIC y Gobierno Abierto | Boyacá Avanza

Fecha del plan:	_20_/_01_/_2021_	Año de vigencia del plan:	2021

1 INTRODUCCIÓN

Entendiendo la Gestión de riesgos de seguridad digital como una estrategia que se diseña enmarcada en un conjunto de principios generales y operativos de seguridad digital en todos los niveles de gobierno y de las organizaciones públicas y un conjunto de procesos críticos para gestionar el riesgo de las actividades económicas y sociales.

Los principios generales propuestos por la OCDE: Conocimiento, capacidades y empoderamiento, responsabilidad, derechos humanos y valores fundamentales, cooperación. Los principios operativos dirigidos a los líderes o tomadores de decisiones, quienes por su alto nivel en las organizaciones deben enfocar sus acciones hacia la adopción del marco general de gestión del riesgo de seguridad digital.

Así que, este documento permite dar a conocer el modelo de gestión sistemática y cíclica del riesgo de seguridad digital y estructurar las condiciones para que las múltiples partes interesadas puedan gestionar la seguridad digital. Entonces, se integran el Modelo nacional de gestión de riesgos de seguridad digital GRSD y el modelo interno de Administración del riesgo según lineamientos establecidos por el Departamento Administrativo de la Función Pública (DAFP).

2 OBJETIVOS

2.1. Objetivo general

Establecer un marco de trabajo integral de la gestión de riesgos de seguridad digital a través del cual se mitiguen las vulnerabilidades y amenazas asociadas a los activos de información de la gobernación de Boyacá, 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 y así maximizar los beneficios de un entorno digital abierto para impulsar la prosperidad económica y social.

2.2 Objetivos específicos

- Ser una metodología lógica y sistemática para identificar los riesgos de seguridad de la información y los datos, evaluar, tratar, controlar y proteger los recursos del

[1] Es el año de última actualización dentro del horizonte estratégico o período de gobierno.

estado, resguardándolos contra la materialización de los riesgos.

- Introducir dentro de los procesos y procedimientos de la entidad las acciones de mitigación resultado de la administración del riesgo de seguridad de la información para prevenir, generar recomendaciones y regular los incidentes o emergencias cibernéticas desarrollando una base confiable para la toma de decisiones y la planificación institucional.

- Definir el plan de tratamiento del riesgo residual de seguridad y privacidad de la información de la entidad.

3 ALCANCE

El alcance del plan de gestión de tratamiento de riesgos de seguridad y privacidad de la información inicia con la fase de planificación; y concluye con la fase de mejoramiento continuo de la gestión de riesgos de seguridad digital y el plan de acción mediante el cual se realizará el tratamiento, monitoreo y revisión de los riesgos de seguridad digital identificados.

4 ÁMBITO DE APLICACIÓN

Aplica a todas las dependencias y procesos de la Gobernación de Boyacá; así mismo a las partes interesadas quienes dependen del entorno digital para todas o algunas de sus actividades, económicas y sociales que genera la entidad.

5 DEFINICIONES

Activo: Se refiere a elementos de hardware y de software de procesamiento, almacenamiento y comunicaciones, bases de datos y procesos, procedimientos y recursos humanos asociados con el manejo de los datos y la información misional, operativa y administrativa de cada entidad, órgano u organismo.

Activo de información: Es cualquier cosa que tiene valor para la organización. Se refiere a todos aquellos recursos (físicos, de información, software, documentos, procesos, procedimientos, servicios, personas, instalaciones, comunicaciones etc) que necesiten ser protegidos de riesgos potenciales.

Gestión de riesgos de seguridad digital: es el conjunto de actividades coordinadas dentro de una organización o entre organizaciones, para abordar el riesgo de seguridad digital, mientras se maximizan oportunidades. Es una parte integral de la toma de decisiones y de un marco de trabajo integral para gestionar el riesgo de las actividades

[1] Es el año de última actualización dentro del horizonte estratégico o período de gobierno.

económicas y sociales. Se basa en un conjunto flexible y sistemático de procesos cíclicos lo más transparente y lo más explícito posible. Este conjunto de procesos ayuda a asegurar que las medidas de gestión de riesgos de seguridad digital (medidas de seguridad) sean apropiadas para el riesgo y los objetivos económicos y sociales en juego.

Evaluación de riesgos y ciclo de tratamiento: En este principio operativo la evaluación de riesgos debe llevarse a cabo de manera sistemática y continua, evaluando las posibles consecuencias de las amenazas y las vulnerabilidades digitales en las actividades económicas y sociales en juego. El tratamiento del riesgo debería tener como objetivo reducir el riesgo a un nivel aceptable en relación con los beneficios económicos y sociales.

Innovación: Un principio operativo donde los líderes y tomadores de decisiones deben asegurarse de que la innovación sea considerada como parte integral de la reducción del riesgo de seguridad digital. Esta debe fomentarse tanto en el diseño y funcionamiento de la economía, y de las actividades sociales basadas en el entorno digital, como en el diseño y el desarrollo de las medidas de seguridad.

Medidas de seguridad: Este principio operativo donde los líderes y tomadores de decisiones deben asegurarse de que las medidas de seguridad sean apropiadas y proporcionales al riesgo, y deben tener en cuenta su potencial impacto, negativo o positivo, sobre las actividades económicas y sociales que tienen por objeto proteger. La evaluación de riesgos de seguridad digital debe guiar la selección, operación y mejora de las medidas de seguridad para reducir el riesgo a niveles aceptables.

Múltiples partes interesadas: el Gobierno nacional y los territoriales, las organizaciones públicas y privadas, la Fuerza Pública, los propietarios u operadores de las infraestructuras críticas cibernéticas nacionales, la academia y la sociedad civil, quienes dependen del entorno digital para todas o algunas de sus actividades, económicas y sociales, y quienes pueden ejercer distintos roles y tener distintas responsabilidades.

Infraestructura crítica cibernética nacional: aquella soportada por las TIC y por las tecnologías de operación, cuyo funcionamiento es indispensable para la prestación de servicios esenciales para los ciudadanos y para el Estado. Su afectación, suspensión o destrucción puede generar consecuencias negativas en el bienestar económico de los ciudadanos, o en el eficaz funcionamiento de las organizaciones e instituciones, así como de la administración pública.

Preparación y continuidad: Este principio operativo con el fin de reducir los efectos adversos de los incidentes de seguridad, y apoyar la continuidad y la capacidad de recuperación de las actividades económicas y sociales, deben adoptarse preparaciones y planes de continuidad. El plan debe identificar las medidas para prevenir, detectar, responder y recuperarse de los incidentes y proporcionar mecanismos claros de

[1] Es el año de última actualización dentro del horizonte estratégico o período de gobierno.

escalamiento.

Riesgo: es el efecto de incertidumbres sobre objetivos y puede resultar de eventos en donde las amenazas cibernéticas se combinan con vulnerabilidades generando consecuencias económicas.

Riesgo de seguridad digital: es la expresión usada para describir una categoría de riesgo relacionada con el desarrollo de cualquier actividad en el entorno digital. Este riesgo puede resultar de la combinación de amenazas y vulnerabilidades en el ambiente digital. Puede debilitar el logro de objetivos económicos y sociales, así como afectar la soberanía nacional, la integridad territorial, el orden constitucional y los intereses nacionales. El riesgo de seguridad digital es de naturaleza dinámica. Incluye aspectos relacionados con el ambiente físico y digital, las personas involucradas en las actividades y los procesos organizacionales que las soportan.

Seguridad digital: es la situación de normalidad y de tranquilidad en el entorno digital (ciberespacio), derivada de la realización de los fines esenciales del Estado mediante (i) la gestión del riesgo de seguridad digital; (ii) la implementación efectiva de medidas de ciberseguridad; y (iii) el uso efectivo de las capacidades de ciberdefensa; que demanda la voluntad social y política de las múltiples partes interesadas y de los ciudadanos del país.

Definiciones establecidas por la OCDE, y otras tomadas del documento CONPES 3854 de 2016

6 FASE DE PLANIFICACIÓN

La Gobernación de Boyacá siguiendo los lineamiento trazados por el Gobierno Nacional con lo expuesto en la Ley de transparencia 1712 de 2014, las Políticas de Gobierno Digital y de Seguridad digital: establece un plan de tratamiento de riesgos de seguridad y privacidad de la información en el cual se identifiquen las amenazas, las vulnerabilidades, el impacto y el nivel de riesgo asociados a los activos de información.

6.1 Roles y responsabilidades frente a la administración del riesgo de seguridad digital

Para la Gestión de Riesgos de Seguridad digital, se establecen las siguientes líneas de defensa:

- **1ª línea defensa.** En esta se ejerce el Autocontrol con los líderes de proceso que son los Secretarios y Directores, quienes a su vez son dueños de los activos, que los identifican y valoran, realizan la gestión de riesgos y ejecutan planes de

[1] Es el año de última actualización dentro del horizonte estratégico o período de gobierno.

tratamiento.

- **2ª línea defensa.** A través de la cual se hace Autogestión donde el responsable es el Director de Sistemas de Información quien lidera y hace monitoreo el desarrollo de la política de seguridad digital y diseña el plan de tratamiento de riesgos de seguridad y privacidad de la información de acuerdo a modelos establecidos por el Gobierno Nacional.
- **3ª línea defensa.** En la cual se hace Aseguramiento independiente por parte de control Interno de Gestión a través del proceso de Auditoría interna para realizar seguimiento y evaluar la efectividad de la política y el plan de riesgos.
- **Línea estratégica.** Corresponde la autorregulación por parte del Comité Institucional de Gestión y Desempeño, y del Comité institucional de Coordinación de Control Interno.

Los Comités institucionales actúan basándose en lineamientos regulaciones de orden nacional y territorial, en lo particular definen y aprueban la política y el plan de seguridad y privacidad de la información de la entidad; así como el plan de tratamiento de riesgos de seguridad digital.

Al Comité institucional de gestión y desempeño hace parte la mesa técnica de gobierno y seguridad digital, entre las funciones relativas de esta mesa se encuentran:

- Proponer mecanismos, metodologías, lineamientos y procesos específicos para dar cumplimiento a la normatividad y lineamientos relacionados con seguridad y privacidad de la información
- Coordinar la formulación y actualización de la política general de seguridad y privacidad de la información, planes y manuales correspondientes para preservar la seguridad digital de la entidad.

Cada proceso debe realizar la identificación de sus activos de información teniendo presente que en cada activo se establezca un dueño del riesgo del activo y su responsable, en el entendido que el dueño del riesgo estará encargado en un rol operativo y el responsable del activo en un rol directivo.

6.2 Política de administración del riesgo de seguridad digital

La administración de riesgos de seguridad digital para los Activos de Tecnologías de Información en producción se debe realizar de manera permanente y con monitoreos cuatrimestrales.

Todas las mejoras, actualizaciones, conversiones y cambios relativos asociados con estos Activos de TI deben ser precedidos por una evaluación del riesgo.

Los funcionarios públicos, contratistas y responsables de proceso de la Gobernación de

[1] Es el año de última actualización dentro del horizonte estratégico o período de gobierno.

Boyacá que realizan las labores de administración de los activos de información son responsables por la implementación, permanencia y monitoreo de los controles sobre dichos activos.

La implementación de medidas de seguridad debe ser consistente con las directrices establecidas por la Dirección de Sistemas de Información siguiendo lineamientos nacionales, objetivos de control de mejores prácticas y de estándares internacionales.

Esta política se incluye en el manual de políticas de seguridad y privacidad de la información de código interno No. A-AD-TI-M-001.

6.3. Identificación y valoración de activos de TI

Es importante para la entidad establecer los lineamientos para la identificación, clasificación, valoración y actualización de los activos de TI con el propósito de gestionarlos a través de su ciclo de vida para asegurar que su uso aporta valor, que se mantendrán en funcionamiento, que están protegidos físicamente, y que los activos que son fundamentales para apoyar la capacidad del servicio son fiables y están disponibles.

Se ha definido la Gestión de activos de TI como un procedimiento previo para poder establecer la Gestión de los riesgos de seguridad digital. Este último incorporándose a la administración de riesgos de la entidad.

El procedimiento correspondiente se encuentra en el documento Gestión de activos de Tecnologías de la Información con código interno No. A-AD-TI-P-008.

6.4. Metodología para la administración del riesgo de seguridad digital

Se establece una metodología integral aplicando el Modelo nacional de gestión de riesgos de seguridad digital (MGRSD) articulado al Modelo de Seguridad y Privacidad de la Información (MSPI) y al modelo interno de Administración del riesgo según lineamientos establecidos por el Departamento Administrativo de la Función Pública (DAFP).

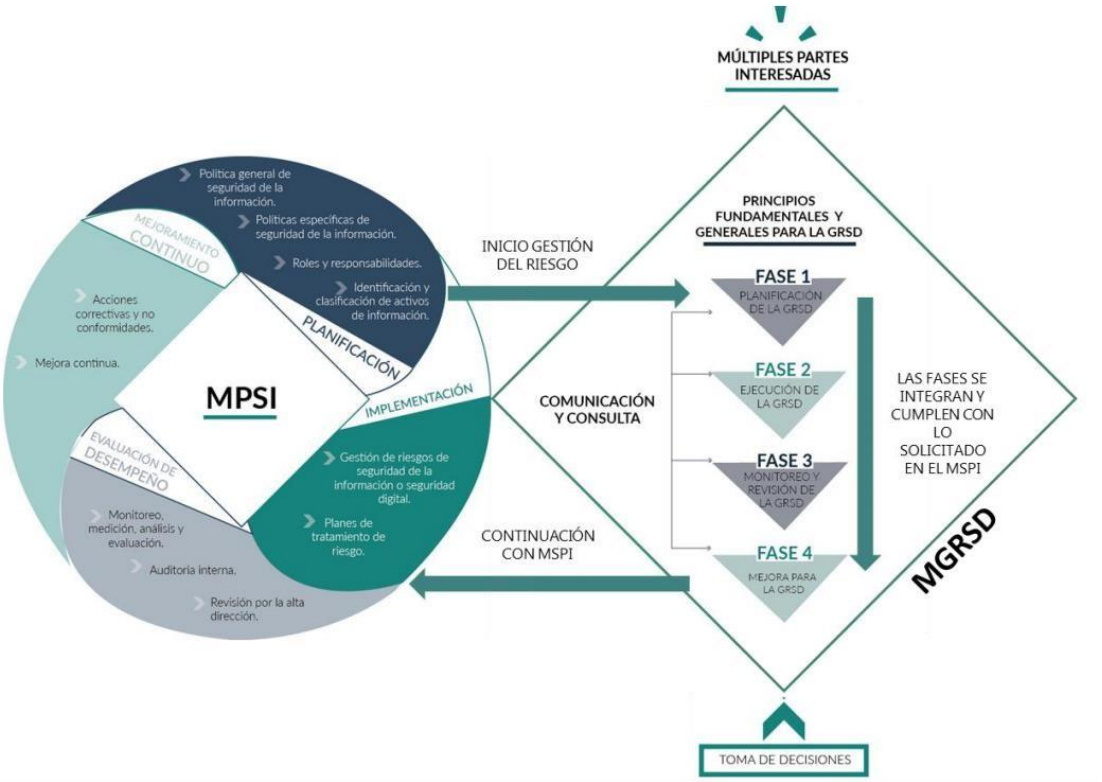
Para el diseño de la metodología se ha tenido en cuenta la Guía para la administración del riesgo y el diseño de controles en entidades públicas, en su versión 4, que trata lo relativo a riesgos de gestión, corrupción y seguridad digital. Así mismo, los lineamientos para la gestión de riesgos de seguridad digital en entidades públicas establecidos por el MinTIC.

En la figura 1 se observa la interacción de los dos modelos, donde las actividades de

[1] Es el año de última actualización dentro del horizonte estratégico o período de gobierno.

identificación de activos, identificación, análisis, evaluación y tratamiento de los riesgos del MGRSD se alinean con la fase de planificación del MSPI.

Figura 1. Esquema de Seguridad y privacidad – MSPI y MGRSD



Fuente: Tomado de (MinTIC, 2018)

En la figura 2 se observa la metodología integral que se adopta para la Gestión de riesgos de seguridad digital del Proceso Gestión de las Tecnologías de Información en la Gobernación de Boyacá, que articula el procedimiento Gestión de activos de Tecnologías de la Información de código interno No. A-AD-TI-P-008, con el Procedimiento Administración de Riesgos de Código: E-DO-DM-P-002 del Proceso Direccionamiento y Mejoramiento de Métodos y Sistemas de Gestión.

Figura 2. Metodología Administración de riesgos de seguridad digital

[1] Es el año de última actualización dentro del horizonte estratégico o período de gobierno.

Fuente: Elaboración propia

7. FASE DE EJECUCIÓN

7.1. Análisis contexto estratégico

- **Contexto externo:**

A nivel nacional, la Ley 1581 de 2012 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 de la Gobernación de Boyacá, 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, la Ley 1712 de 2014 "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.

[1] Es el año de última actualización dentro del horizonte estratégico o período de gobierno.

En razón a esto, la gobernación de Boyacá está comprometida 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.

Por su parte, el decreto 1008 de 2018 "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 la Gobernación de Boyacá desempeña un papel importante con la implementación de servicios tecnológicos que le permita alcanzar los propósitos que dispone esta ley, gestionando los riesgos y amenazas que traigan consigo la implementación de avances tecnológicos.

- **Contexto Interno:**

A nivel interno, el Decreto 601/2018, Decreto 187/2018 “Por medio del cual se adopta el Modelo Integrado de Planeación y Gestión, se crean algunas instancias administrativas al interior de la Gobernación de Boyacá, y se dictan otras disposiciones”, y Decreto 318 de 2019 “por medio del cual se unifican y modifican los decretos de operación del Modelo MIPG al interior de la Gobernación de Boyacá, y se dictan otras disposiciones”. Allí se han definido las instancias que en una gestión y desempeño institucional son responsables de liderar la implementación de las políticas de gestión de la entidad, y con ellas los planes estratégicos y operativos, entre los que se mencionan el plan de seguridad y privacidad de la información y el plan de tratamiento de riesgos de seguridad digital y la incorporación de acciones relacionadas en el plan de acción institucional.

Así mismo, con la Ordenanza 049 de 2018 "Por la cual se determina la estructura orgánica para la administración departamental; las funciones de sus dependencias y se dictan otras disposiciones"; allí se crea la Secretaría de TIC y Gobierno abierto y las direcciones de apropiación TIC y de Sistemas de Información, donde se designan funciones relativas a coordinar la gestión de activos de información, la continuidad del negocio, gestión de seguridad y privacidad de la información y los servicios tecnológicos de la administración departamental, adelantar estudios que permitan establecer mecanismos de control y planes de contingencia como garantía para la preservación, oportunidad, integralidad y confiabilidad de la información.

En el plan departamental de desarrollo 2016-2019 se estableció que era necesario fortalecer el plan anticorrupción, implementando de manera oportuna las acciones

establecidas en el plan de manejo de riesgos de cada uno de los procesos de la entidad con el fin de minimizar la probabilidad y el impacto en caso de materializarse alguno de

[1] Es el año de última actualización dentro del horizonte estratégico o período de gobierno.

los riesgos; además, que era necesario propender la entrega oportuna de los informes de monitoreo y seguimiento de riesgos por parte de los responsables de los procesos y poder cumplir con los términos establecidos en el Decreto 2641 de 2012. El mismo plan plantea que la mayor dificultad que se tiene con respecto a la Gestión del riesgo es el no considerarse una herramienta de gestión para la toma de decisiones orientadas a prevenir la materialización de los riesgos, además que no se exige cuentas a los responsables de proceso sobre su gestión para mejorar la efectividad de los controles adoptados. Aunque no se menciona de manera explícita, aquí se entienden incorporados los riesgos de seguridad digital.

El plan departamental de desarrollo 2016-2019 menciona que es importante implementar medidas que aseguren la integridad de la información de la entidad y que garanticen la continuidad del negocio frente a los diversos riesgos detectados.

El manual de operaciones del sistema de gestión de la entidad incorpora un objetivo del sistema de gestión que da alcance a la Gestión de riesgos, definido así: Implementar los controles establecidos y priorizados por medio de la identificación de los peligros, evaluación y valoración de los riesgos de acuerdo a la metodología adoptada por la Gobernación de Boyacá.

Por su parte, el PETI menciona que el habilitador transversal de seguridad y privacidad dentro de la política de gobierno digital se desarrollará a partir de los lineamientos emitidos por el MinTIC establecidos en dos modelos: Modelo de seguridad y privacidad de la información (MSPI) y Modelo de gestión de riesgos de seguridad digital (MGRSD), en atención a la política de seguridad digital Conpes 3854 de 2016. Así mismo, incorpora en la visión del Gobierno de TI un proceso dentro de la cadena de valor de TI denominado: Gestión del riesgo y la seguridad.

7.2. Identificación de riesgos de seguridad digital

Se incorporará el consolidado de la identificación de riesgos de seguridad digital de la entidad una vez los procesos de negocio hayan realizado la Identificación y valoración de activos de TI y basado en ello hayan realizado la identificación de riesgos en función de la gestión de riesgos digitales.

7.3. Valoración de riesgos de seguridad digital

Se incorporará el consolidado de la valoración de riesgos de seguridad digital de la entidad una vez los procesos de negocio hayan realizado la Identificación y valoración

[1] Es el año de última actualización dentro del horizonte estratégico o período de gobierno.

de activos de TI y basado en ello hayan realizado la valoración de riesgos en función de la gestión de riesgos digitales.

7.4. Controles para el tratamiento de riesgos

Se incorporará el consolidado de controles para el tratamiento de riesgos de seguridad digital de la entidad una vez los procesos de negocio hayan realizado la Identificación y valoración de activos de TI y basado en ello hayan realizado la valoración de controles existentes, y la identificación de nuevas medidas de seguridad en función de la gestión de riesgos digitales.

7.5. Plan de tratamiento de riesgos de seguridad digital

Se incorporará el mapa de riesgos de seguridad digital una vez los procesos de la entidad hayan realizado la Identificación y valoración de activos de TI y basado en ello hayan realizado la administración de riesgos de seguridad digital.

Se hace una consolidación de todos los tratamientos que hayan sido determinados por los procesos de negocio con las decisiones establecidas: si se optó por tomar el riesgo, si se va a reducir, se va a transferir o evitar el riesgo. En caso que la decisión sea reducirlo, se documenta aquí las medidas de seguridad digital que se van a seleccionar y aplicar, la innovación o las medidas de preparación para su tratamiento por parte de las sectoriales.

8. FASE DE MONITOREO Y REVISIÓN

Se monitorea y revisa los riesgos de manera permanente remitiendo al proceso de Direccionamiento y Mejoramiento de Métodos y Sistemas de Gestión, dentro de la tercera semana de los meses de Abril, Agosto y Diciembre, con el fin de dar cumplimiento a la periodicidad establecida en las políticas de operación y en la normatividad vigente.

Luego se verifica la publicación y socialización de Mapas de Riesgos de gestión, incluidos los de seguridad digital por proceso y/o subproceso en el sitio Web de la entidad y en la Herramienta Isolucion en el Módulo Riesgos DAFP.

Así mismo, se realiza el análisis y evaluación de riesgos atendiendo el cronograma establecido por la oficina asesora de control interno de gestión, siguiendo el Plan de

Manejo de Riesgos de los mapas de riesgos por proceso y/o subproceso, los parámetros de los formatos respectivos, y las políticas de operación del procedimiento Evaluación de riesgos.

[1] Es el año de última actualización dentro del horizonte estratégico o período de gobierno.

En la figura 2, se puede observar alineación de la gestión de riesgos de seguridad digital con el procedimiento de evaluación de riesgos de código interno No. V-EG-P-008 del proceso Evaluación de la Gestión.

9. FASE DE MEJORAMIENTO CONTINUO DE LA GESTIÓN DE RIESGOS

Conocidas las observaciones o no conformidades reportadas por parte de la oficina asesora de Control Interno de Gestión, se genera un plan de mejoramiento con acciones correctivas ingresando al módulo mejoramiento de la herramienta Isolucion.

Se realiza el análisis de causas y se formula las acciones que permiten mitigar el riesgo y se registra en la sección tratamiento, del módulo mejoramiento, las acciones necesarias para eliminar la no conformidad. Así mismo, se formulan las acciones correctivas necesarias para eliminar las causas de la no conformidad detectada.

Posteriormente, a medida que se va ejecutando el plan de acción en cada acción definida se registran las evidencias en la sección plan de mejoramiento del módulo de la herramienta.

Al finalizar, se evalúa la eficacia de las acciones correctivas realizadas en la medida que elimine las causas de la no conformidad. Si se ha dado cumplimiento a todas las acciones, se cierra la no conformidad en el módulo de la herramienta.

En la figura 2, se puede observar alineación de la gestión de riesgos de seguridad digital con el procedimiento de Acciones correctivas de código interno No. E-DO-DM-P-006 del proceso Direccionamiento y Mejoramiento de Métodos y Sistemas de Gestión.

10. PLAN DE TRABAJO

Las actividades formuladas en el plan de tratamiento de riesgos de seguridad digital se pueden observar en el siguiente cronograma:

[1] Es el año de última actualización dentro del horizonte estratégico o período de gobierno.

GOBERNACIÓN DE Boyacá	FORMATO	VERSION: 0
		CÓDIGO: A-AD-TI-F-029
PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION		FECHA: 16/Dic/2019

ACTIVIDAD	FASE	2021												2022												2023												MEDICIÓN Y SEGUIMIENTO	
		I CUATRIM				II CUATRIM				III CUATRIM				I CUATRIM				II CUATRIM				III CUATRIM				I CUATRIM				II CUATRIM				III CUATRIM				INDICADOR	% AVANCE
	MESES ===>	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4		
Actualización de la política de administración del riesgo de seguridad digital en el manual de políticas de seguridad y privacidad de la información por la Dirección de Sistemas de Información	PLANIFICACIÓN																																					Actividades ejecutadas / Actividades programadas	
Socialización del procedimiento A-AD-TI-P-008 Gestión de activos de Tecnologías de la información a los procesos de la Entidad por la Dirección de Sistemas de Información	PLANIFICACIÓN																																						
Socialización de la etodología para la administración del riesgo de seguridad digital a los procesos de la Entidad por la Dirección de Sistemas de Información	PLANIFICACIÓN																																						
Socialización del contexto estratégico a los procesos de la Entidad por la Dirección de Sistemas de Información	EJECUCIÓN																																						
Acompañamiento a los procesos en la identificación de riesgos de seguridad digital por por la Dirección de Sistemas de Información y la Oficina asesora de planeación y métodos de gestión	EJECUCIÓN																																						
Reporte de administración de riesgos de seguridad digital por parte de los procesos	EJECUCIÓN																																						
Reporte del mapa de riesgos de seguridad digital por parte de los procesos	EJECUCIÓN																																						
Consolidación del plan de tratamiento de riesgos de seguridad digital	EJECUCIÓN																																						
Monitoreo y revisión de riesgos de seguridad digital por parte de los procesos de la entidad	MONITOREO Y REVISIÓN																																					Actividades ejecutadas / Actividades programadas	
	MONITOREO Y																																						

GOBERNACIÓN DE Boyacá	FORMATO	VERSION: 0
		CÓDIGO: A-AD-TI-F-029
PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION		FECHA: 16/Dic/2019

ACTIVIDAD	FASE	2021												2022												2023												MEDICIÓN Y SEGUIMIENTO	
		I CUATRIM				II CUATRIM				III CUATRIM				I CUATRIM				II CUATRIM				III CUATRIM				I CUATRIM				II CUATRIM				III CUATRIM				INDICADOR	% AVANCE
	MESES ===>	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4		
Evaluación de riesgos de seguridad digital por parte de oficina asesora de Control interno de gestión	REVISIÓN																																						
Formulación del plan de mejoramiento continuo de la gestión de riesgos por parte de los procesos de la entidad	MEJORA																																						
Ejecución del plan de mejoramiento continuo de la gestión de riesgos por parte de los procesos de la entidad	MEJORA																																						

11. CONTROL DE CAMBIOS

Versión[1]	Fecha	Cambios introducidos
2020-I	20/Ene/2020	Emisión
2020-II	18/Dic/2020	Actualización fase de ejecución y plan de trabajo

Elaboró:

Versión	Nombre Autor (es)	Cargo o Profesión
2020-I	Mónica Orduz Valbuena	Profesional Universitario
2020-II	Mónica Orduz Valbuena	Profesional Universitario

Revisó:

Versión	Responsable	Cargo o Profesión
2020-I	Will Jhonathan Amaya Medina Mesa técnica de Gobierno y Seguridad Digital	Director de Sistemas de Información Profesionales Mesa técnica de Gobierno y Seguridad Digital
2020-II	Will Jhonathan Amaya Medina Mesa técnica de Gobierno y Seguridad Digital	Director de Sistemas de Información Profesionales Mesa técnica de Gobierno y Seguridad Digital

Aprobó:

Versión	Responsable	Cargo o Profesión
2020-I	John Amaya Rodríguez Comité institucional de Gestión y desempeño	Secretario de TIC y Gobierno Abierto Comité institucional de Gestión y desempeño
2020-II	John Amaya Rodríguez Comité institucional de Gestión y desempeño	Secretario de TIC y Gobierno Abierto Comité institucional de Gestión y desempeño

[1] Es el año de última actualización dentro del horizonte estratégico o período de gobierno.