PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD DIGITAL

E.S.E. ISABU Instituto de Salud de Bucaramanga

2023

CONTENIDO

1. OBJETIVO: 3

2. ALCANCE: 3

3. RESPONSABLE: 3

4. DEFINICIONES 3

5. DESARROLLO: 4

5.1 PLAN DE GESTIÓN DE RIESGOS DE SEGURIDAD DIGITAL 4

5.2 FASE DE PLANIFICACIÓN 5

5.2.1 Metodología de gestión de riesgos de seguridad digital 5
5.2.2 Contexto Estratégico 7
5.2.3 Contexto Externo 7
5.2.4 Contexto Interno 8
5.2.5 Contexto del Proceso 8
5.2.6 Política de Gestión Riesgos 9
5.2.7 Roles y Responsabilidades 9
5.2.8 Definición de Recursos para la Gestión de riesgos de seguridad digital. 9
5.2.9 Identificación de los activos de seguridad digital. 9
5.2.10 Identificación de los Riesgos Inherentes de seguridad digital 9
5.2.11 Identificación y evaluación de los controles existentes. 10
5.2.12 Tratamiento de los riesgos de seguridad digital. 10
5.2.13 Plan de Tratamiento de los riesgos de seguridad digital e indicadores para la gestión del riesgo. 10

5.3 FASE DE EJECUCIÓN 11

5.4 FASE DE MONITOREO Y REVISIÓN 11

5.4.1 Registro y reportes de incidentes de seguridad digital 11
5.4.2 Reporte de la gestión de riesgos de seguridad digital al interior de la entidad. 11
5.4.3 Reportes de la gestión de riesgos de la seguridad digital a autoridades o entidades especiales. 12
5.4.4 Auditorías internas y externas 12
5.4.5 Medición del desempeño. 12

5.5 FASE DE MEJORAMIENTO CONTINUO DE LA GESTIÓN DE REISGOS DE SEGURIDAD DIGITAL. 12

5.6 SITUACIÓN ACTUAL. 13

6. DOCUMENTOS REFERENCIADOS 16

7. CONTROL DE MODIFICACIONES 16

1. OBJETIVO:

Establecer un Plan de tratamiento de riesgo de seguridad digital a través del cual se mitiguen las vulnerabilidades y amenazas asociados a los activos de información de la ESE ISABU, 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. ALCANCE:

El Plan de gestión de riesgos de seguridad digital inicia en fortalecer y definir acciones para el tratamiento de riesgos de seguridad digital de acuerdo a los lineamientos emitidos por el ministerio de tecnologías de la información, dando cubrimiento a los procesos estratégicos, misionales, de soporte, verificación y mejora; y concluye con la ejecución de acciones que realizara la entidad entorno a la seguridad digital para la mitigación de los riesgos, teniendo en cuenta la capacidad y recursos disponibles.

3. RESPONSABLE:

Líder Proceso de Gestión de la TI, Ingeniero Oficial de seguridad informática y protección de datos

4. DEFINICIONES

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

- **CSIRT:** Equipo de Respuesta a Incidentes de Seguridad Informática
- **RPO:** Sigla en inglés Recovery Point Objective, es el Punto de recuperación de información, que se espera, ante un evento de falla.
- **RTO:** Sigla en inglés Recovery Time Objective, es el Punto de restauración del Sistema, que se espera, ante un evento de falla.
- **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
- **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.

5. DESARROLLO:

5.1 PLAN DE GESTIÓN DE RIESGOS DE SEGURIDAD DIGITAL

El Instituto de Salud de Bucaramanga – ISABU E.S.E. entendiendo la Gestión de riesgos de seguridad digital, como una estrategia y siguiendo los lineamientos 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 para la prevención, contención y mitigación de amenazas a las que se encuentran expuestos los activos de información de la entidad.

El instituto de Salud de Bucaramanga fue creado mediante los decretos 665 y 668 de diciembre de 1989, siendo inicialmente un establecimiento público descentralizado del Orden Municipal. En 1997 mediante Decreto 1876 del 3 de agosto son reestructuradas las entidades descentralizadas prestadoras de Servicios de Salud y el ISABU obtiene así la modalidad de Empresa Social del Estado, con la categoría especial de Entidad Descentralizada, con personería Jurídica, Patrimonio Propio y Autonomía Administrativa, cuya función esencial es la Prestación de Servicios de Salud. 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.

El ISABU E.S.E. 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.

De igual modo, con la definición del Plan Estratégico de Tecnologías de la Información **PETI formulado** para el ISABU E.S.E., se propone un modelo integral de gestión de las Tecnologías de la Información desarrollado para el logro de los objetivos corporativos formulados en el plan de desarrollo 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 y estratégico en la entidad.

Para la construcción del plan de tratamiento de riesgos de seguridad digital se identifican las siguientes fases:

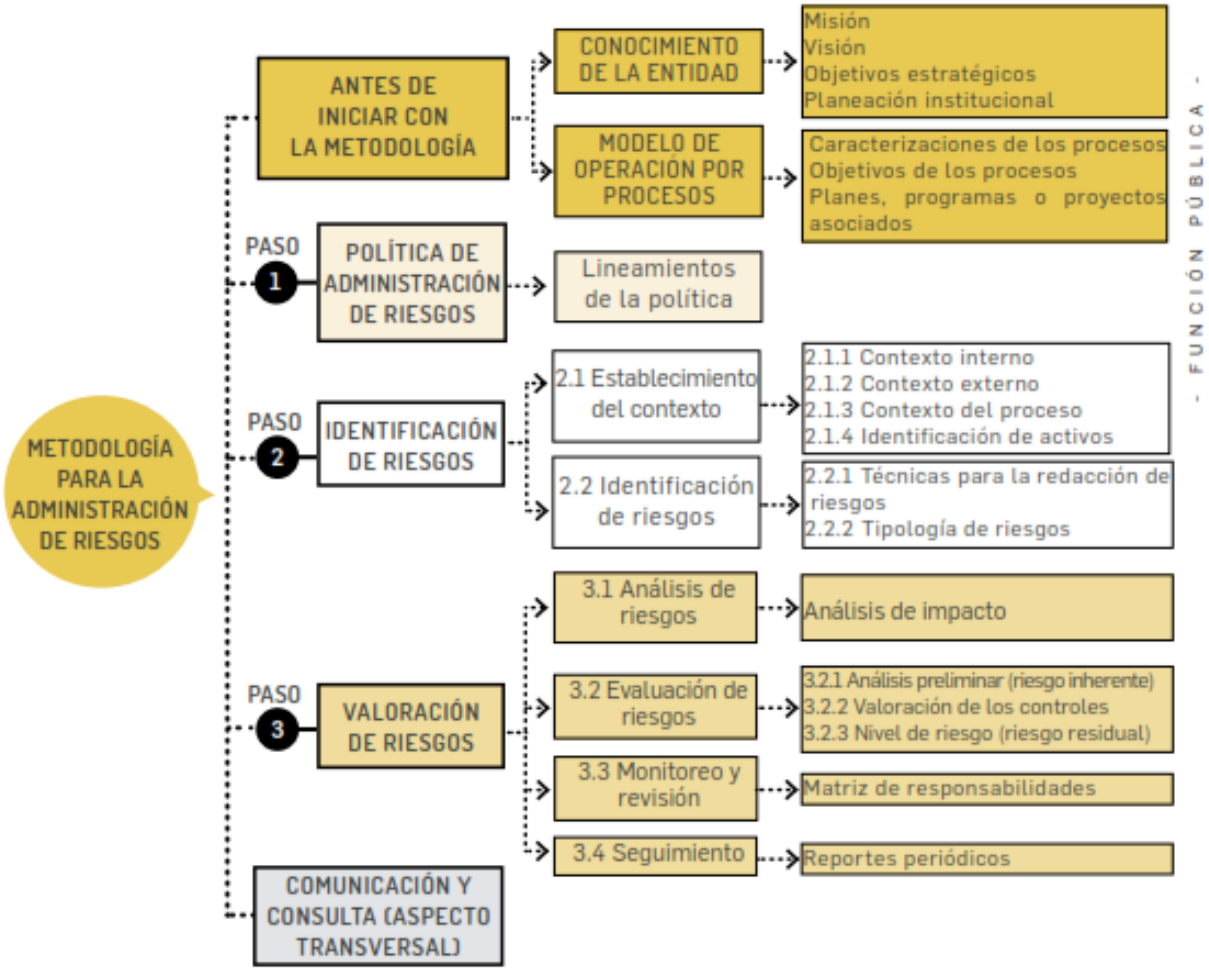
- Fase de planeación
- Fase de ejecución
- Fase de monitoreo y revisión
- Fase de mejoramiento continuo

5.2 FASE DE PLANIFICACIÓN

5.2.1 Metodología de gestión de riesgos de seguridad digital

El Instituto de Salud de Bucaramanga –ESE ISABU 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

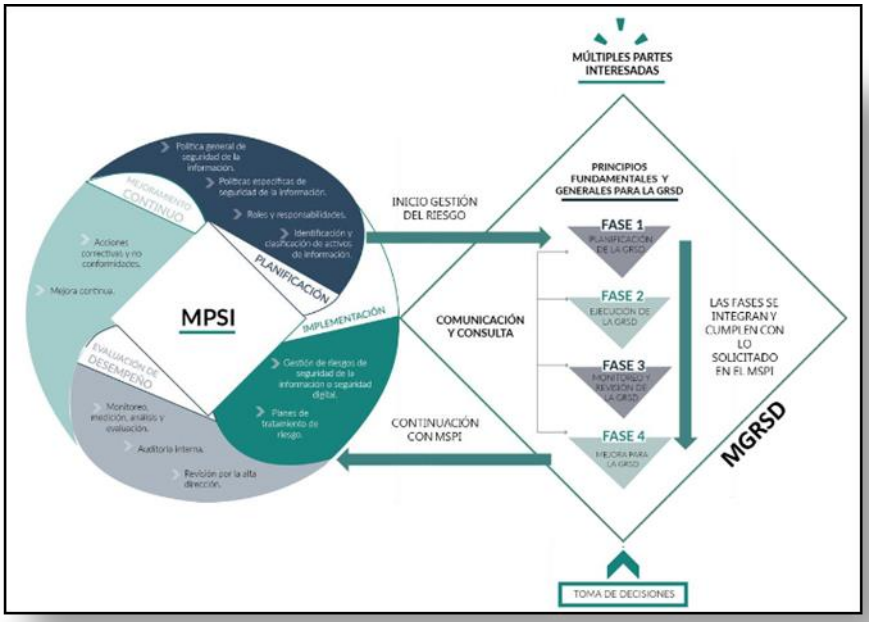


Fuente: Guía Para la administración de riesgos y el diseño de controles en entidades públicas.

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 ISABU E.S.E.

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

5.2.2 Contexto Estratégico

El instituto de Salud de Bucaramanga fue creado mediante los decretos 665 y 668 de diciembre de 1989, siendo inicialmente un establecimiento público descentralizado del Orden Municipal. En 1997 mediante Decreto 1876 del 3 de agosto son reestructuradas las entidades descentralizadas prestadoras de Servicios de Salud y el ISABU obtiene así la modalidad de Empresa Social del Estado, con la categoría especial de Entidad Descentralizada, con personería Jurídica, Patrimonio Propio y Autonomía Administrativa, cuya función esencial es la Prestación de Servicios de Salud. 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.

5.2.3 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 ISABU E.S.E., 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 persona 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, ISABU E.S.E. 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.

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 ISABU E.S.E. 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.

5.2.4 Contexto Interno

El ISABU E.S.E. 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.

De igual modo, con la definición del Plan Estratégico de Tecnologías de la Información **PETI** formulado para el ISABU E.S.E., 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. 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.

5.2.5 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.

5.2.6 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 Riesgos de Seguridad digital del ISABU E.S.E.".

5.2.7 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 ISABU E.S.E. Por lo cual se debe contemplar las funciones establecidas en el documento de roles y responsabilidades "**Catálogo de servicios TIC – Roles y responsabilidades".**

5.2.8 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 ISABU E.S.E. y del rubro de funcionamiento Gastos de mantenimiento 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.

5.2.9 Identificación de los activos de seguridad digital.

El ISABU E.S.E. debe tener 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, que permitan determinar los controles y medidas que protejan y salvaguarden los activos de información, cuáles son los más importantes y críticos dentro de los procesos y procedimientos de la entidad. Para esto se requiere utilizar el "FORMATO ÚNICO DE INVENTARIO DE ACTIVOS DE INFORMACIÓN PARA SEGURIDAD INFORMATICA", y que sea diligenciado con datos actualizados por los líderes de los diversos procesos de la Institución.

5.2.10 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 ISABU E.S.E. 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 ISABU E.S.E. 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.

5.2.11 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 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 riesgo residual

5.2.12 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, las formulaciones 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 necesarios 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 "**Guía para la Administración de los Riesgos de Gestión, Corrupción y Seguridad Digital y el Diseño de Controles en Entidades Públicas"** 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

5.2.13 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 ISABU E.S.E.. 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.

5.3 FASE DE EJECUCIÓN

Actualmente al interior del E.S.E. ISABU 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.

5.4 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.

5.4.1 Registro y reportes de incidentes de seguridad digital

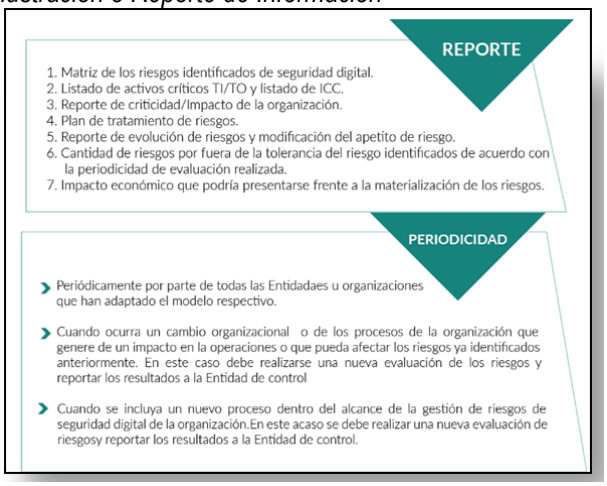
A la fecha, la Oficina de Sistemas ha gestionado eventos e incidentes que han afectado la seguridad digital en la entidad con un impacto bajo por lo que no ha sido necesario aún realizar reporte al Centro Cibernético Policial y al Equipo de Respuesta a Incidentes de Seguridad Informática **CSIRT.** Sin 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 diagnóstico 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 incidente, 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 dicha entidad en la solución de los incidentes.

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

En esta actividad el ISABU E.S.E. 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 reporte de información.

5.4.3 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 E.S.E. ISABU 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.

5.4.4 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.

5.4.5 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.

5.5 FASE DE MEJORAMIENTO CONTINUO DE LA GESTIÓN DE REISGOS DE SEGURIDAD DIGITAL.

La E.S.E. ISABU 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.

5.6 SITUACIÓN ACTUAL.

Durante el año 2020 la entidad adoptó la nueva Política de Seguridad de la información. Este documento describe 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.

El Plan de gestión de riesgos de seguridad digital junto con la política hacen parte del proceso para la mitigación de los mismos, los cuales tienen como objeto Garantizar la disponibilidad de las tecnologías de la información, manteniendo la integridad y confidencialidad de la información.

La E.S.E ISABU ha priorizado abordar la gestión de riesgos de seguridad informática sobre los activos de tecnologías de información frente a ciberamenazas, en atención a los procesos que realizan sus actividades apoyadas en el uso de tecnologías de información. Actualmente la institución cuenta con un sistema de información y una base de Datos principal como activos de tecnologías de información de interés para el análisis y gestión para la toma de decisiones, así como equipos tecnológicos que incluye: Computadores, servidores y dispositivos de red.
Una de las acciones relevantes es la identificación de riesgos sobre los activos de tecnología de la información frente a la ciberamenazas que tienen lugar en el entorno digital, a partir de lo cual se define la siguiente matriz de riesgos:

Id	Escenario De Riesgo	Amenaza	Vulnerabilidad
1	Afectación de la disponibilidad, integridad o confidencialidad de los servidores, por acción de Spyware/Malware, debido a una falta o deficiencia en controles sobre la detección, prevención, recuperación para proteger contra códigos maliciosos.	Spyware/Malware	Falta o deficiencia en controles sobre la detección, prevención, recuperación para proteger contra códigos maliciosos
2	Compromiso de la disponibilidad, integridad o confidencialidad de los PC de escritorio, portátiles, por acción de Spyware/Malware, debido a una falta o deficiencia en controles sobre la detección, prevención, recuperación para proteger contra códigos maliciosos	Spyware/Malware	Falta o deficiencia en controles sobre la detección, prevención, recuperación para proteger contra códigos maliciosos
3	Afectación de la disponibilidad, integridad o confidencialidad de los servidores, por acción hackers, debido a una falta o deficiencia en controles de seguridad informática en la gestión de las redes	Hackers	Falta o deficiencia en controles de seguridad informática en la gestión de las redes
4	Afectación de la disponibilidad, integridad o confidencialidad de los servidores, por acción hackers, debido a una falta o deficiencia en controles sobre el acceso a redes y servicios en red	Hackers	Falta o deficiencia en controles sobre el acceso a redes y servicios en red
5	Afectación de la disponibilidad, integridad o confidencialidad de los sistemas de información web, por acción de hackers, debido a una falta o deficiencia en controles que garanticen el adecuado análisis y especificación de requisitos de seguridad informática en los sistemas de información	Grupos criminales	Falta o deficiencia en controles que garanticen el adecuado análisis y especificación de requisitos de seguridad informática en los sistemas de información
6	Afectación de la integridad, disponibilidad y confidencialidad de los servidores de bases de datos, por acción de atacante interno, debido a una falta o deficiencia en controles sobre el acceso a redes y servicios en red	Amenazas internas (Insider)	Falta o deficiencia en controles sobre el acceso a redes y servicios en red

De acuerdo con los posibles riesgos, se realiza la valoración de los mismos de acuerdo a la escala propuesta por el departamento administrativo de la Función Pública, A partir del cual se obtiene el Plan de acción para el tratamiento

de riesgos. Para ello se crea como anexo el Mapa de Riesgo de seguridad TI para la aplicación y seguimiento de los controles de riesgos inherentes y residuales, en el que se identifican y prioriza el conjunto de riesgos frente a la probabilidad de ocurrencia y el impacto de la materialización.

5.2 PLAN DE ACCIÓN DEL TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN.

El tratamiento de riesgos de seguridad y privacidad de la información se enfoca en la seguridad informática frente a las ciberamenazas, para lo cual se realizan unas actividades durante la vigencia, con el fin de implementar los controles requeridos y priorizados.

MAPA DE RUTA PARA LA VIGENCIA 2020-2023

ANEXO 1: PLAN DE TRABAJO RIESGO DE SEGURIDAD DIGITAL							
FASE	**OBJETIVO**	**ACTIVIDAD**	**2020**	**2021**	**2022**	**2023**	**MEDICIÓN Y SEGUIMIENTO**
PLANIFICACIÓN	Establecer las actividades y procesos necesarios para cumplir con los requisitos de seguridad y privacidad de la información establecidos en el MSPI	Establecer Política de Seguridad de la Información					Actividades ejecutadas / Actividades Programadas
		Actualizar la política de seguridad de la información del ISABU					
		Establecer roles y responsabilidades al interior del ISABU (Acta Constitución de Gobierno ISABU)					
		Realizar levantamiento y clasificación de activos de información					
		Identificar riesgos de seguridad de la información (se Priorizan 6 riesgos de gestión para el 2022 - y se actualizan para el 2023)					
		Realizar análisis de riesgos de seguridad de la información					
		Realizar Mapa de Riesgos de Gestión de las TIC					
		Realizar seguimiento al Mapa de Riesgo de Gestión de las Tic					
		Realizar evaluación de los riesgos de seguridad de la información					
		Diseñar el programa de sensibilización y capacitación (Cronograma de trabajo FERSACO)					
		Implementar el programa de sensibilización y capacitación en seguridad de la información					
IMPLEMENTACIÓN	Ejecutar actividades, controles y medidas de protección que permitan la mitigación de riesgos de seguridad de la información.	Creación Política de Seguridad de la Información y Política de Protección de datos Personales					Actividades ejecutadas / Actividades Programadas
		Aprobación y publicación de Políticas en Pág. Web.					
		Realizar Seguimiento del sistema de protección de datos personales por medio de capacitaciones y sensibilización a personal de la institución.					
		Realizar informe donde se evidencie la custodia de la información (copias de seguridad)					
		Revisión periódica de las alarmas generadas por el software de integral de protección contra virus, Malware entre otros.					

MEJORA CONTINUA	Determinar los factores y/o aspectos a mejorar que hacen parte del MSPI	Desarrollar plan de mejora continua					Actividades ejecutadas / Actividades Programadas
		Gestionar las comunicaciones					

El desarrollo de las actividades, estará sujeto a la disponibilidad de recursos (humanos, técnicos, tecnológicos y financieros), que faciliten el cumplimiento de las actividades de acuerdo con la disponibilidad presupuestal.

PLAN DE ACCIÓN TRATAMIENTO DE RIESGOS DE SEGURIDAD DIGITAL PARA LA VIGENCIA 2023

No.	Actividad	Descripción de la actividad	Responsable	Formato
1	Elaborar Plan de tratamiento de riesgos de seguridad digital para la vigencia 2023	Definir los lineamientos para la ejecución de las actividades del plan de tratamiento de riesgos de seguridad digital	Ing. de Seguridad Informática y Protección de Datos.	Plan de seguridad y privacidad de la información
2	Publicar en página web institucional y socializar el Plan de tratamiento de riesgos de seguridad digital por correo electrónico.	Dar a conocer a la comunidad, colaboradores, entes de control el Plan de tratamiento de riesgos de seguridad digital de la ESE ISABU para la vigencia 2023	Ing. de Seguridad Informática y Protección de Datos.	Correo electrónico y link de página web institucional
3	Establecer las actividades y procesos necesarios para cumplir con los requisitos de seguridad y privacidad de la información establecidos en el MSPI	Realizar Seguimiento del sistema de tratamiento de riesgo de seguridad y privacidad de la información y protección de datos personales	Ingeniero de seguridad informática y protección de datos	* Un cronograma de sensibilización y capacitación en seguridad de la información * Dos informes como evidencia a la implementación del programa de sensibilización y capacitación en seguridad de la información
4	Ejecutar actividades, controles y medidas de protección que permitan la mitigación de riesgos de seguridad de la información	Realizar informe donde se evidencie la custodia de la información, copias de seguridad de la información a servidores y bases de datos de la institución	Líder de Sistemas de información / Líder de Infraestructura	* Informe semestral de seguimiento de copias de seguridad a la base de datos y servidores
5	Ejecutar actividades, controles y medidas de protección que permitan la mitigación de riesgos de seguridad de la información	Realizar Actualización de licencia del antivirus e Informe de riesgos reportados por software de control de intrusos. (Antivirus) con una periosidad trimestral (4)	Ingeniero de seguridad informática y protección de datos / Líder de Infraestructura	* Informe de seguimiento de antivirus con periocidad trimestral para la vigencia 2023, se programan 4 entregables en el año
6	Determinar los factores y/o aspectos a mejorar que hacen parte del MSPI	Actualización del Plan de tratamiento de riesgos de seguridad y privacidad de la información (1)	Ingeniero de seguridad informática y protección de datos	* Documento - plan actualizado para siguiente vigencia.

Anexo.

- **Formato inventario de activos de información**

En el cual se identifican los activos de Información, Identificación de Riesgos, Roles y Responsabilidades, Controles de Riesgos, Tratamiento, seguimiento e indicadores para la gestión del riesgo de seguridad de la información.

- **Formato Plan de Acción Estratégico Institucional Código: PLA-F-012**

6. DOCUMENTOS REFERENCIADOS

- Concepto, E. (2013-2021). *Concepto.de*. Obtenido de https://concepto.de/sistema-de-informacion/
- MinTIC, G. d. (s.f.). *G.ES.06 Guía PETI - MinTIC.* Bogota.
- Publica, F. (s.f.). *Plan de tratamiento de riesgos de seguridad de la nformación*. Obtenido de https://www.funcionpublica.gov.co/documents/418537/38169866/2021-01-30_Plan_tratamiento_riesgos_seguridad_informacion_v3.pdf/91994a8c-eda2-02b2-8c02-4c5dde38a3d6?t=1612127235836
- Ley 527 de 1999. Por la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales y se establecen las entidades de certificación y se dictan otras disposiciones.
- Ley 594 de 2000. Por medio de la cual se expide la Ley General de Archivos.
- Ley 1266 de 2008. Por la cual se dictan las disposiciones generales del Hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones
- Ley 1273 de 2009. Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones
- Ley 1341 de 2009. Por la cual se definen principios y conceptos sobre la sociedad de la información y la organización de las tecnologías de la información y las comunicaciones - TIC- Se crea la agencia Nacional de espectro y se dictan otras disposiciones
- Ley 1978 de 2019. Por la cual se moderniza el sector de las Tecnologías de la Información y las Comunicaciones TIC), se distribuyen competencias, se crea un regulador único y se dictan otras disposiciones.
- Decreto 1008 del 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.
- CONPES 3854 de 2016. Política Nacional de Seguridad digital
- CONPES 3905 de 2020. Política Nacional de Confianza y Seguridad Digital

7. CONTROL DE MODIFICACIONES

VERSIÓN	FECHA	DESCRIPCIÓN DE LA MODIFICACIÓN	RELIZADA POR
1	2701/2023	Documento modificado de manual a Plan de Tratamiento de riesgos de seguridad Digital	Ingeniera de Sistemas apoyo al proceso de las TIC´s Líderes del proceso de Gestión de las TIC´s