ALCALDÍA DE BUCARAMANGA

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

ISABU e.s.e | INSTITUTO DE SALUD DE BUCARAMANGA

Marca Salud

Proceso: Gestión Tics

Subproceso: Seguridad de la información

Código: SEG- PL - 005

Versión: 04

Fecha de aprobación: 29/01/2026

TABLA DE CONTENIDO

1. OBJETIVO:

Fortalecer el Plan de tratamiento de riesgos de seguridad y privacidad de la información 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 y del modelo nacional de riesgos de seguridad Digital (MGRSD) del MINTIC.

2. ALCANCE:

El Plan de tratamiento de riesgos de seguridad y privacidad de la información inicia en fortalecer y definir acciones para la identificación y 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 realizará la entidad entorno a la seguridad digital para la mitigación de los riesgos, teniendo en cuenta la capacidad y recursos disponibles.

3. RESPONSABLE:

Profesional especializado de sistemas,
Profesional especializado de seguridad informática
Profesional especializado en infraestructura
profesional apoyo de sistemas de información.

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 esta (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.
- **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

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

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

5. DESARROLLO

5.1 AUTODIAGNÓSTICO

Durante los periodos 2023, 2024 y 2025 se ha logrado el cumplimiento del 100% de las actividades previstas en el marco del Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información de la E.S.E. ISABU. Estas acciones incluyeron la elaboración, publicación y actualización anual del plan, la sensibilización institucional sobre políticas de seguridad de la información y protección de datos personales, así como la ejecución de medidas técnicas y procedimentales orientadas a la mitigación de riesgos.

Entre las actividades más relevantes se destacan la realización de copias de seguridad del sistema de información CORE – PANACEA, la actualización de licenciamientos de seguridad en endpoints, la implementación de controles tecnológicos y procedimentales, y la documentación de informes de análisis y seguimiento. Estas medidas han permitido fortalecer la postura de seguridad digital de la entidad, garantizando la integridad, disponibilidad y confidencialidad de la información, en cumplimiento de los estándares normativos nacionales e internacionales.

La ejecución exitosa de los planes en los tres años evidencia un proceso de maduración progresiva, pasando de un enfoque inicial en seguridad digital hacia la integración de la ciberseguridad y la privacidad de la información, con indicadores de gestión y roles especializados. Este avance contribuye al fortalecimiento de la cultura institucional en seguridad, al aseguramiento de los activos tecnológicos y a la preparación frente a riesgos emergentes del entorno digital.

5.2 PLAN DE GESTIÓN DE RIESGOS DE SEGURIDAD DIGITAL

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

La E.S.E. ISABU 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:

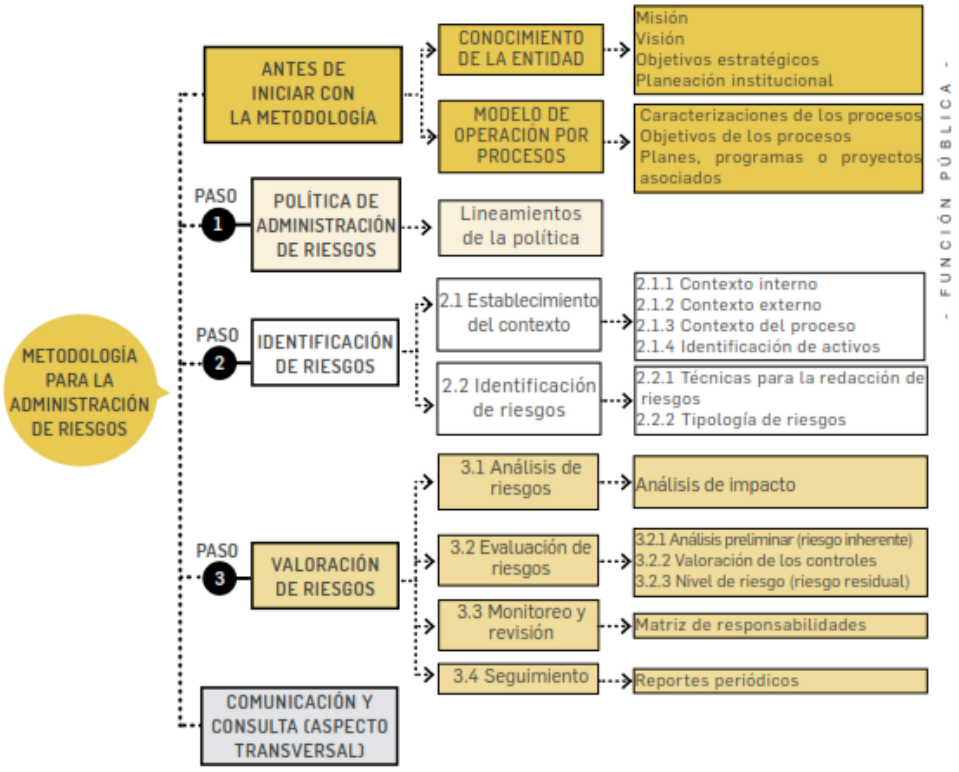
- Fase de planeación
- Fase de ejecución
- Fase de monitoreo y revisión
- Fase de mejoramiento continuo

5.3 FASE DE PLANIFICACIÓN

5.3.1 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

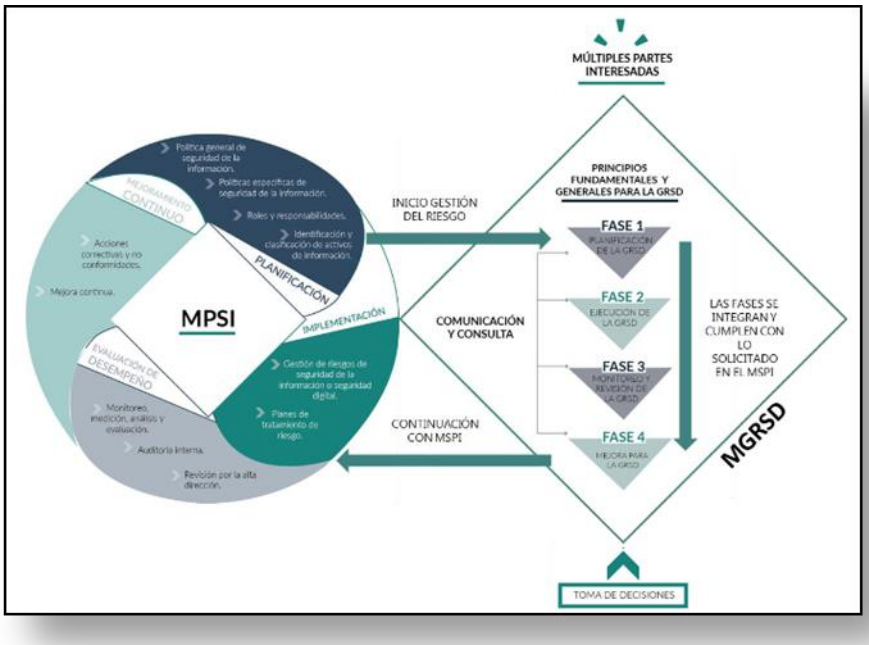


Fuente: Guía Para la administración de riesgos y el diseño de controles en entidades públicas.

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

5.3.2 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.

5.3.3 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.

5.3.4 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 (SIG), que permiten realizar la identificación, tratamiento, monitoreo y revisión de los riesgos de seguridad digital más críticos de la entidad, los cuales pueden impactar de manera considerable el desarrollo de funciones y el logro de los objetivos institucionales.

Adicionalmente, la entidad cuenta con diversos sistemas de información y servicios tecnológicos que soportan los procesos asistenciales, administrativos y financieros, razón por la cual resulta indispensable velar por la protección y seguridad de estos activos de información frente a amenazas internas y externas.

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 establecidos en el plan estratégico vigente. En consecuencia, los esfuerzos para la administración de riesgos de seguridad digital están orientados hacia el cumplimiento de cada uno de estos componentes, en donde las tecnologías de la información se consolidan como un agente de transformación digital estratégico en la entidad.

Durante los años 2016 y 2017, la entidad definió y adoptó la Política de Seguridad de la Información y el Manual de Gestión de Seguridad de la Información. Posteriormente, en un esfuerzo por mantenerse actualizada y alineada con las mejores prácticas, dicha política fue revisada y actualizada en el año 2023 mediante la Resolución 0552 del 28 de noviembre, ampliando su alcance para abarcar no solo la seguridad de la información, sino también la ciberseguridad y la protección de la privacidad, en plena alineación con los estándares más recientes, específicamente la NTC ISO 27001:2022.

Finalmente, en el año 2025, la política institucional fue reforzada con la inclusión de estrategias de seguridad desde el diseño, gestión integral de riesgos digitales, protección de la privacidad con roles especializados, cultura de seguridad digital y medición mediante indicadores de cumplimiento, incidentes gestionados y personal capacitado.
Esta evolución demuestra el compromiso continuo del ISABU E.S.E. con la seguridad y la adaptabilidad frente a las cambiantes dinámicas del entorno digital, garantizando la vigencia y eficacia de sus prácticas de gestión de la información. Los documentos normativos y directrices institucionales constituyen mecanismos fundamentales para la

mitigación de riesgos asociados a los activos de información de la entidad, consolidando una cultura organizacional orientada a la confianza, la resiliencia y la mejora continua

5.3.5 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 TIC" 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.

5.3.6 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.".

5.3.7 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 contemplan las siguientes funciones:

Tabla 1 Roles y Responsables

ROLES	ACTIVIDADES
Alta dirección	▪ Aprobar los recursos financieros y humanos necesarios para la gestión de riesgos. ▪ Proporcionar el liderazgo y apoyo a la estrategia de seguridad de la información. ▪ Asegurarse de que los riesgos de seguridad de la información estén alineados con los objetivos comerciales
Profesional especializado en Gestión Tic	▪ Aprobar la política de seguridad de la información y los objetivos estratégicos. ▪ Revisar y aprobar las estrategias de gestión de riesgos. ▪ Tomar decisiones sobre riesgos significativos. ▪ Monitorear el progreso y resultados de la gestión de riesgos. ▪ Aprobar las estrategias según los resultados y cambios en el entorno.
Profesional especializado en Seguridad de la información	▪ Liderar y coordinar la implementación de la metodología de gestión de riesgos. ▪ Identificar y evaluar las amenazas y vulnerabilidades en la infraestructura y los sistemas de la organización. ▪ Diseñar plan de tratamientos de riesgos y hacer respectivo seguimiento. ▪ Colaborar con las partes interesadas para definir los criterios de evaluación de riesgos. ▪ Proporcionar recomendaciones técnicas y estratégicas para abordar los riesgos. ▪ Monitorear la eficacia de los controles de seguridad implementados. ▪ Informar a la Alta Dirección sobre el estado de riesgos y la efectividad de las estrategias.
Profesional especializado en sistemas de información	▪ Evaluar riesgos en sistemas y aplicaciones. ▪ Coordinar implementación de controles de seguridad en sistemas. ▪ Supervisar pruebas de seguridad y auditorías de sistemas. ▪ Mantenerse informado sobre vulnerabilidades y amenazas en TI. ▪ Colaborar con el equipo de desarrollo en estándares de seguridad.
Profesional especializado en infraestructura	▪ Evaluar y evaluar riesgos de infraestructura y operaciones. ▪ Implementar y mantener controles técnicos de seguridad. ▪ Supervisar la seguridad física de activos tecnológicos. ▪ Colaborar en garantizar que las soluciones cumplan con estándares de seguridad. ▪ Participar en la mejora continua de procesos de seguridad.
Usuarios	▪ Participar en la identificación y valoración de los riesgos de seguridad de la información, ciberseguridad y protección de la privacidad que pueden afectar las actividades definidas dentro del alcance del Sistema

ROLES	ACTIVIDADES
Alta dirección	▪ Aprobar los recursos financieros y humanos necesarios para la gestión de riesgos. ▪ Proporcionar el liderazgo y apoyo a la estrategia de seguridad de la información. ▪ Asegurarse de que los riesgos de seguridad de la información estén alineados con los objetivos comerciales
	de gestión de Seguridad de la Información - SGSI. ▪ Aplicar los controles para mitigar los riesgos identificados y proponer mejoras a la gestión del riesgo en su proceso. ▪ Participar en los ejercicios de autoevaluación de riesgos para establecer la eficiencia, eficacia y efectividad de los controles implementados para el tratamiento de los riesgos de seguridad de la información, ciberseguridad y protección de la privacidad. ▪ Participar en las actividades de formulación de las acciones correctivas, preventivas y de mejora, cuando se materializan los riesgos de seguridad de la información, ciberseguridad y protección de la privacidad. ▪ Reportar al Oficial de Seguridad de la Información la materialización de riesgos de seguridad de la información, ciberseguridad y protección de la privacidad.

5.3.8 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.

5.3.9 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 con 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 "GIF-F-022 Matriz de identificación, gestión y clasificación de activos de información e infraestructura critica de TI", y que sea diligenciado con datos actualizados por los líderes de los diversos procesos de la Institución.

5.3.10 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 con 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 con el análisis de riesgos realizado, se establecen cual son las prioridades que hay que atender de acuerdo con el riesgo de y seguridad digital que pueda afectar los activos de información de la entidad.

5.3.11 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

5.3.12 Tratamiento de los riesgos de seguridad digital

De acuerdo con 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.

5.3.13 Plan de Tratamiento de los riesgos de seguridad Y privacidad de la información e indicadores para la gestión del riesgo.

La evaluación de riesgos realizada tendrá un mapa de riesgos inherente en cual se detalle la identificación de 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.

5.4 FASE DE EJECUCIÓN

Actualmente al interior del E.S.E. ISABU ya se cuenta con controles tecnológicos, procedimentales y operativos qué permiten mitigar la materialización de riesgos de seguridad de la información, ciberseguridad y protección de la privacidad.

Esta fase seguirá la ruta definida para la aplicación de controles, los cuales estarán a cargo de su implementación en los tiempos definidos, por 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.

5.5 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.

5.5.1 Registro y reportes de incidentes de seguridad digital

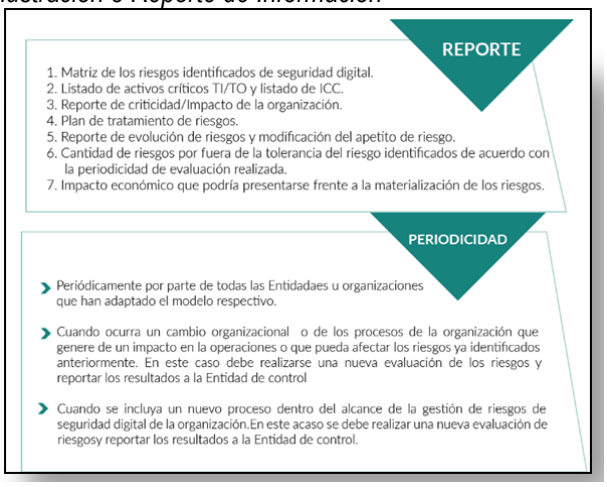
A la fecha, la Oficina de Sistemas ha gestionado eventos e incidentes que han afectado la seguridad digital en la entidad con un impacto bajo por lo que no ha sido necesario aún realizar reporte al Centro Cibernético Policial y al Equipo de Respuesta a Incidentes de Seguridad Informática **CSIRT.** Sin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

5.5.2 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.

5.5.3 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.

5.5.4 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. De igual forma el proceso de gestión de las TICS cuenta con un procedimiento de monitoreo en seguridad de la información, ciberseguridad y protección de la privacidad el cual ejecutara dos veces al año

5.5.5 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.

5.6 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.

5.7 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.

Tabla 2 PLAN DE ACCIÓN TRATAMIENTO DE RIESGOS DE SEGURIDAD DIGITAL PARA LA VIGENCIA 2026

No.	Ciclo PHVA	Meta	Actividad	Descripción de la actividad	Responsable
1	Planear	1	Actualizar el Plan de tratamiento de riesgos de Seguridad y Privacidad de la información para la vigencia 2026	Actualizar el Plan de tratamiento de riesgos de Seguridad y Privacidad de la información para la vigencia 2026	Profesional especializado de sistemas/ Profesional especializado en seguridad de la información
2	Hacer	1	Elaborar cronograma de las actividades a realizar en el Plan de tratamiento de riesgos de Seguridad y Privacidad de la información para la vigencia 2026	Cronograma elaborado de las actividades realizadas en el Plan de tratamiento de riesgos de Seguridad y Privacidad de la información	Profesional especializado de sistemas/ Profesional especializado en seguridad de la información
3	Hacer	1	Publicar en página web el Plan de tratamiento de riesgos de Seguridad y Privacidad de la información para la vigencia 2026	Publicar en página web el Plan de tratamiento de riesgos de Seguridad y Privacidad de la información para la vigencia 2026	Gestión TIC
4	Hacer	1	Socializar el Plan de tratamiento de riesgos de Seguridad y Privacidad de la información a través de correo electrónico con los líderes de procesos y su cronograma 2026	Correo electrónico de la socialización del Plan de tratamiento de riesgos de Seguridad y Privacidad de la información a los líderes de proceso.	Profesional especializado de sistemas/ Profesional especializado en seguridad de la información
5	Hacer	4	Ejecutar el cronograma de las actividades del Plan de tratamiento de riesgos de Seguridad y privacidad de la Información para la vigencia 2026	Excel con la ejecución de las actividades del Plan de tratamiento de riesgos de Seguridad y Privacidad de la información.	Profesional especializado de sistemas/ Profesional especializado en seguridad de la información
6	Verificar	100%	Medir y analizar trimestralmente el cumplimiento de la ejecución del cronograma del Plan de tratamiento de riesgos de Seguridad y privacidad de la información para la vigencia 2026	Ficha técnica del indicador Porcentaje de cumplimiento del plan de acción anual de Tratamiento de riesgos de Seguridad y privacidad de la información	Profesional especializado de sistemas/ Profesional especializado en seguridad de la información
7	Actuar	1	Actuar frente a las desviaciones encontradas en el plan de tratamiento de riesgos de Seguridad y privacidad de la información de la vigencia 2026	Informe final del Plan de tratamiento de riesgos de Seguridad y Privacidad de la información realizado	Profesional especializado de sistemas/ Profesional especializado en seguridad de la información

5.8 INDICADOR Y META

Gestión de Ejecución del Plan de Tratamiento de Riesgo de Seguridad Digital

Porcentaje de cumplimiento del plan de acción anual de TRSPI (No. de acciones ejecutadas / No. de acciones programadas) *100
Meta: 100%

5.9 ANEXO.

- SEG-F-040 Cronograma de las actividades a realizar en el Plan de tratamiento de riesgos de Seguridad y privacidad de la información para la vigencia 2026
- Formato Plan de Acción de los Planes Institucional y Estratégico, 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
2	30/01/2024	Modificación del numeral 3, en el cual se incluyeron los responsables de acuerdo a los roles actuales del área Inclusión de componente autodiagnóstico en el ítem 5.1-. Actualización del apartado 5.3.4 contexto interno, contextualizando la revisión de la política en el año 2023 y alineándola con la normativa NTC ISO 27001:2022. Actualización del apartado 5.3.7, roles y responsabilidades con la situación actual de la oficina de gestión de las TICS Actualización del apartado 5.4, dado que se complementa con el estado actual del proceso en materia de seguridad de la información Actualización del numeral 5.5.4 Auditorias externas e internas, se complementa con el programa de monitoreo que ejecuta. el proceso de gestión de las TICS Eliminación de la información situación actual. Eliminación del mapa de ruta para la vigencia 2020 – 2023 y actualización de actividades del plan de tratamiento de riesgos.	**Elaboró:** Ingeniero Oficial de Seguridad Informática y protección de datos. **Revisó:** Coordinador TI
3	30-01-2025	Actualización de las actividades del numeral 5.7 para el plan de tratamiento de riesgos. Inclusión de Formato Matriz De Riesgos De Seguridad De La Información, Ciberseguridad Y Protección De La Privacidad, y Formato de Reporte De Incidentes De Seguridad De La Información numeral 5.8 Actualización de cargos en el numeral 5.3.7 de roles y responsabilidades	**Elaboró:** profesional especializado en Seguridad de la información. **Revisó:** profesional especializado de sistemas

		Actualización de cargos en el numeral 3 de responsables	
4	29/01/2026	Actualización de los objetivos y alcance Actualización del autodiagnóstico en el ítem 5.1 Actualización del contexto interno en el ítem 5.3.4 Actualización de las actividades del numeral 5.7	**Elaboró:** profesional especializado en Seguridad de la información. **Revisó:** profesional especializado de sistemas