EMPRESA SOCIAL DEL ESTADO
HOSPITAL
SAN JUAN DE DIOS

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

EMPRESA SOCIAL DEL ESTADO HOSPITAL SAN JUAN DE DIOS DE CONCORDIA

Versión 03

CONCORDIA, ENERO 26 DE 2.026

"MAS Y MEJORES SERVICIOS"
Carrera 18 N. 16-05 Concordia -Antioquia
Teléfono: 8446161- 844 7722
hospitaldeconcordia@hospital-concordia.gov.co
Nit. 890907297-3

EMPRESA SOCIAL DEL ESTADO
HOSPITAL
SAN JUAN DE DIOS

COMITÉ DIRECTIVO.

DOCTOR MARIO ALEJANDRO CADAVID CADAVID.
Gerente Empresa Social del Estado.

SEÑOR JUAN CARLOS ÁLVAREZ ARANGO
Subgerente Administrativa.

SEÑOR LUBIN OCTAVIO GALLO ARANGO.
Jefe de la Oficina de Control Interno.

DOCTORA ANA MARÍA GONZÁLEZ ESCOBAR.
Odontólogo.

SEÑORA JULIANA ANDREA CADAVID MESA.
Enfermera.

SEÑORITA PAULINA ANDREA GARRO ORTIZ.
Enfermera.

SEÑORA GLORIA MARÍA LONDOÑO GIRALDO.
Profesional Universitaria Área Salud (Bacterióloga).

SEÑORA RAQUE ROMERO ANAYA.
Regente de Farmacia

SEÑORA ADRIANA MARIA JIMENEZ FRANCO.
Auxiliar Administrativa (Sistema de Información y Atención al Usuario).

SEÑORITA LUZ ALEIDA BETANCUR TOBON.
Secretaria.

EMPRESA SOCIAL DEL ESTADO
HOSPITAL
SAN JUAN DE DIOS

Contenido

EMPRESA SOCIAL DEL ESTADO
HOSPITAL
SAN JUAN DE DIOS

CUADRO DE CONTROL DE CAMBIOS

Versión	Fecha	Descripción Cambios
1.0	2021	Creación del documento.
2.0	23/01/2025	Se revisa la Versión 2.0 del Plan y se determina actualizar en alineación con el plan de desarrollo 2024-2028 Se actualiza los términos o definiciones Se actualiza el marco legal Se actualiza el objetivo general y objetivo especifico Se incluye la estrategia de seguridad digital y se incluye los ejes estratégicos Se actualiza el cronograma de gestión y actividades
3.0	26/01/2026	Lineamientos del Modelo Nacional de Gestión de Riesgo de Seguridad de la Información en Entidades Públicas dirigida a las entidades del Estado

INTRODUCCIÓN.

Mediante la definición del Plan de Tratamiento de Riesgos la ESE busca mitigar los riesgos presentes en el análisis de riesgos (Perdida de la Confidencialidad de los activos, Perdida de Integridad de los activos y Perdida de Disponibilidad de los activos) evitando aquellas situaciones que impidan el logro de los objetivos de la ESE.

El Plan de Tratamiento de Riesgo se define con el fin de evaluar las posibles acciones que se deben tomar para mitigar los riesgos existentes, estas acciones son organizadas en forma de medias de seguridad, y para cada una de ellas se define el nombre de la medida, objetivo, justificación, responsable de la medida y su prioridad.

Las anteriores medidas se definieron teniendo en cuenta la información del análisis de riesgos, el cual brindó información acerca de las necesidades de la ESE, en cuanto a la seguridad y privacidad de la información y proporcionó las herramientas necesarias para definir cada una de las características de las medidas y la definición de los pasos a seguir para su ejecución.

El plan de tratamiento de Riesgos de Seguridad y Privacidad de la información, Seguridad Digital y Continuidad de la Operación de los servicios de la ESE, se basa en una orientación estratégica que requiere el desarrollo de una cultura de carácter preventivo, de manera que, al comprender el concepto de riesgo, así como el contexto, se planean acciones que reduzcan la afectación a la entidad en caso de materialización, adicional se busca desarrollar estrategias para la identificación, análisis, tratamiento, evaluación y monitoreo de dichos riesgos con mayor objetividad, dando a conocer aquellas situaciones que pueden comprometer el cumplimiento de los objetivos trazados en el Entorno de la ESE para el Desarrollo Digital.

En cumplimiento de la Ley 1581 de 2012 (Art. 17 Lt. k y Art. 18 Lt. f) y del Decreto 1377 de 2013 (Art. 13.) mediante los cuales se dictan disposiciones para la protección de datos personales y en el desarrollo del derecho constitucional que tienen todas las personas a conocer, actualizar y rectificar la información que se haya recogido sobre ellas en bases de datos o archivos, la E.S.E. Hospital San Juan de Dios en calidad de responsable del tratamiento de los datos personales de sus grupos de interés conformado por los usuarios y sus familias, colaboradores, contratistas, estudiantes, entidades responsables de pago y las entidades de inspección, vigilancia y control, información que se ha obtenido en el desarrollo de su actividad misional de prestar servicios de salud, por lo cual se compromete con el cumplimiento de la normativa mencionada y la protección de los derechos de las personas e información a su grupo de interés que adopta las siguientes políticas sobre recolección, tratamiento y uso de datos personales.

Todas las referencias a los documentos del Modelo de Seguridad y Privacidad de la Información - MSPI, son derechos reservados por parte del Ministerio de Tecnologías de la Información y las Comunicaciones -MinTIC.

De igual forma, son derechos reservados por parte del MinTIC, todas las referencias a las políticas, definiciones o contenido relacionados con los documentos del MSPI publicadas en el compendio de las normas técnicas colombianas vigentes.

Las reproducciones, referencias o enunciaciones de estos documentos deberán ir siempre acompañadas por el nombre o seudónimo del titular de los derechos de autor (Ministerio de Tecnologías de la Información y las Comunicaciones).

Lo anterior, sin perjuicio de los derechos reservados por parte de entidades tales como la International Standard Organización (ISO), ICONTEC, entre otras, respecto de referencias, definiciones, documentos o contenido relacionado en el MGRSD y sus documentos o anexos que son de su autoría o propiedad.

1. DEFINICIONES

Para efectos de la ejecución de la presente política y de conformidad con la normatividad legal, serán aplicables las siguientes definiciones:

- **Autorización:** Consentimiento previo, expreso e informado del Titular para llevar a cabo el Tratamiento de datos personales.
- **Base de Datos:** Conjunto organizado de datos personales que sea objeto de Tratamiento.
- **Dato personal:** Cualquier información vinculada o que pueda asociarse a una o a varias personas naturales determinadas o determinables.
- **Dato personal semiprivado:** son aquellos datos que no tienen una naturaleza íntima, reservada, ni pública y cuyo conocimiento o divulgación puede interesar no solo a su titular, sino, a un grupo de personas o a la sociedad en general.
- En este caso, para su tratamiento se requiere la autorización expresa del Titular de la información. Por ejemplo: datos de carácter financiero, datos relativos a las relaciones con las entidades de seguridad social (EPS, AFP, ARL, Cajas de Compensación).
- **Dato personal sensible:** Son aquellos que afectan la intimidad del Titular o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición así como los datos relativos a la salud, a la vida sexual y los datos biométricos.
- **Dato personal privado:** es un dato personal que por su naturaleza íntima o reservada solo interesa a su Titular y para su tratamiento requiere de su autorización expresa. Por ejemplo: Nivel de escolaridad, libros de los comerciantes, entre otros.
- **Dato personal público:** es aquel tipo de dato personal que las normas y la Constitución han determinado expresamente como públicos y, para cuya recolección y tratamiento, no es necesaria la

autorización del Titular de la información. Por ejemplo: estado civil de las personas, datos contenidos del RUNT, datos contenidos en sentencias judiciales ejecutoriadas, entre otros.

- **Encargado del Tratamiento:** Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, realice el Tratamiento de datos personales por cuenta del Responsable del Tratamiento.
- **Responsable del Tratamiento:** Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, decida sobre la base de datos y/o el Tratamiento de los datos.
- **Titular:** Persona natural cuyos datos personales sean objeto de Tratamiento.
- **Tratamiento:** Cualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, almacenamiento, uso, circulación o supresión.
- **Riesgo:** es un escenario bajo el cual una amenaza puede explotar una vulnerabilidad generando un impacto negativo al negocio evitando cumplir con sus objetivos.
- **Amenaza:** es un ente o escenario interno o externo que puede hacer uso de una vulnerabilidad para generar un perjuicio o impacto negativo en la institución (materializar el riesgo).
- **Vulnerabilidad:** es una falencia o debilidad que puede estar presente en la tecnología, las personas o en las políticas y procedimientos.
- **Probabilidad:** es la posibilidad de la amenaza aproveche la vulnerabilidad para materializar el riesgo.
- **Impacto:** son las consecuencias que genera un riesgo una vez se materialice.
- **Control o Medida:** acciones o mecanismos definidos para prevenir o reducir el impacto de los eventos que ponen en riesgo, la adecuada ejecución de las actividades y tareas requeridas para el logro de objetivos de los procesos de una entidad.

2OBJETIVO GENERAL

El objetivo principal de este documento es orientar a todas las en el Hospital San Juan de Dios y en general, en la implementación de la Gestión de Riesgos de Seguridad de la información, que permita incrementar la confianza de las múltiples partes interesadas en el uso del entorno digital y del aseguramiento de los activos de información en la entidad.

3.OBJETIVOS ESPECIFICOS

- Otorgar una herramienta de orientación para la ejecución de la Gestión de Riesgos de Seguridad de la información.
- Estandarizar el proceso de Gestión de Riesgos de Seguridad de la información,

- Definir y aplicar los lineamientos para tratar de manera integral los riesgos de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación de los servicios que la ESE pueda estar expuesta, y de esta manera alcanzar los objetivos, la misión y la visión institucional, protegiendo y preservando la integridad, confidencialidad, disponibilidad y autenticidad de la información.
- Cumplir con los requisitos legales y reglamentarios pertinentes a la legislación colombiana.
- Gestionar riesgos de Seguridad y Privacidad de la información, Seguridad Digital y Continuidad de la Operación de los servicios, de acuerdo con los contextos establecidos en la Entidad.
- Fortalecer y apropiar conocimiento referente a la gestión de riesgos Seguridad y Privacidad de la información, Seguridad Digital y Continuidad de la Operación de los servicios de la ESE.

4. ALCANCE

Este documento tiene como objetivo ampliar y profundizar en los contenidos presentados en la "Guía para la Administración del Riesgo y el diseño de controles en entidades públicas" del Departamento Administrativo de la Función Pública. En particular, se enfoca en las secciones relacionadas con el análisis del contexto, con un énfasis especial en el entorno digital.

Además, aborda temas como la identificación de activos, la elaboración de catálogos de amenazas y vulnerabilidades para llevar a cabo un análisis exhaustivo de los riesgos de seguridad de la información, la implementación de controles diseñados para mitigar estos riesgos y el proceso de reporte de estos. También se abordan otros aspectos adicionales que desempeñan un papel fundamental en la gestión efectiva del riesgo de seguridad de la información en el ámbito de las entidades públicas.

Realizar una eficiente gestión de riesgos de Seguridad y Privacidad de la información, Seguridad Digital y Continuidad de la Operación de los servicios, que permita integrar en los procesos de la entidad, buenas prácticas que contribuyan a la toma de decisiones y prevenir incidentes que puedan afectar el logro de los objetivos. Junto con Guía de Gestión de Riesgos de Seguridad y Privacidad de la Información (MinTIC:2016)[1]: se dan los lineamientos para poder identificar, analizar, tratar, evaluar y monitorear los riesgos de seguridad y privacidad de la información en MINTIC.

El Plan de Tratamiento de Riesgo tendrá en cuenta los riesgos que se encuentren en los niveles Moderado, Alto y Extremo acorde con los lineamientos definidos por el Ministerio TIC, los riesgos que se encuentren en niveles inferiores serán aceptados por la Entidad.

5.Integración del modelo de seguridad y privacidad de la Información (MSPI)

Conforme al ámbito de aplicación del Decreto 1078 de 2015, en lo relacionado con la Estrategia de Gobierno Digital, y a la Resolución 500 del 10 de marzo de 2021, mediante la cual el MinTIC establece los lineamientos y estándares para la estrategia de seguridad digital y adopta el Modelo de Seguridad y Privacidad de la Información (MSPI) como habilitador de dicha política, las entidades públicas deben implementar el MSPI con el fin de establecer un Sistema de Gestión de Seguridad de la Información (SGSI) dentro de su organización.

El MSPI incorpora, en cada una de sus fases, actividades orientadas a la gestión de riesgos de seguridad de la información, ya que esta constituye su eje central. Para ello, la Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas, junto con este Anexo, proporcionan las directrices necesarias para cumplir con los requerimientos de gestión del riesgo establecidos en el modelo.

En esencia, la interacción entre el modelo de seguridad y privacidad de la información y el modelo nacional de gestión de riesgos de seguridad de la información puede resumirse de la siguiente manera:

1. Las actividades de identificación de activos, identificación, análisis, evaluación y tratamiento de los riesgos se alinean con la fase de PLANIFICACIÓN del MSPI.

2. Las actividades de implementación de los planes de tratamiento de riesgos se alinean con la fase de IMPLEMENTACIÓN del MSPI.

3. Las actividades de monitoreo y revisión, revisión de los riesgos residuales, efectividad de los planes de tratamiento o los controles implementados y auditorías se alinean con la fase de EVALUACIÓN DEL DESEMPEÑO del MSPI.

4. Las actividades de MEJORAMIENTO CONTINUO en ambos modelos son similares y trabajan simultáneamente, ya que dependerán de las fases de Medición del desempeño para identificar aspectos a mejorar en la aplicación de ambos modelos.

A continuación, se ilustra en que acciones del MSPI tendrán interacción directa con el Modelo de Gestión de Riesgos de Seguridad de la información

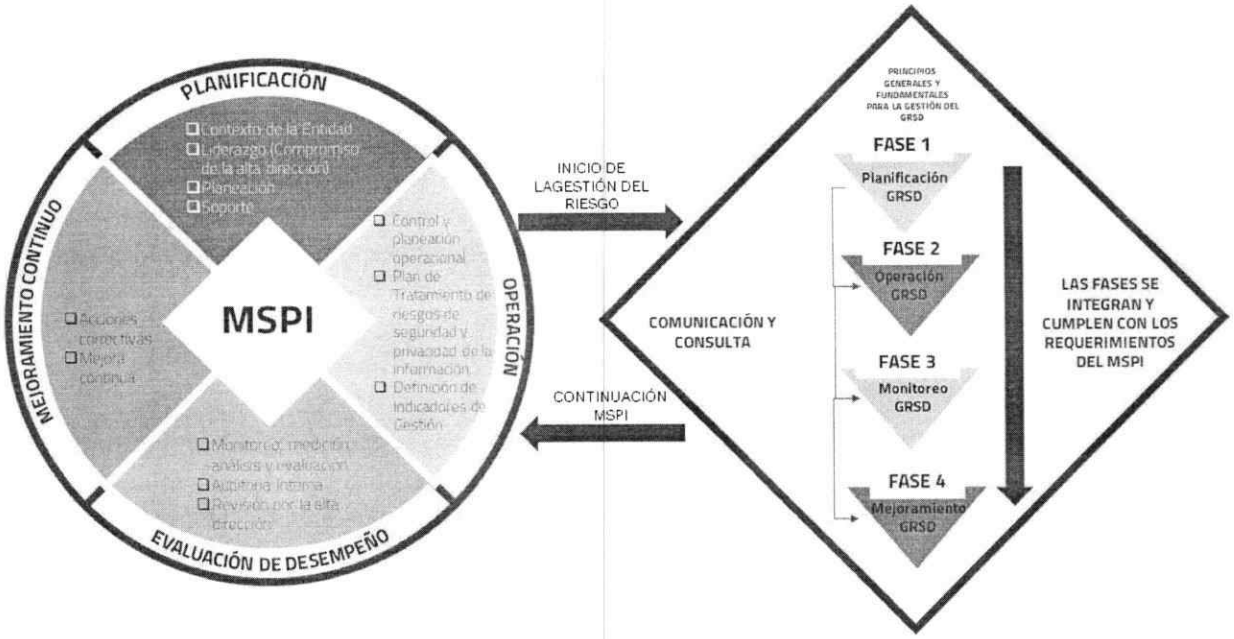


Ilustración 1 Interacción MSPI - Modelo Gestión de Riesgo de seguridad de la información

Fuente: Ministerio de Tecnologías de la Información y las Comunicaciones

6. MARCO REFERENCIAL

6.1. POLÍTICA DE ADMINISTRACION DE RIESGOS

La ESE, a través de su Modelo Integrado de Gestión, se orienta hacia una cultura de la gestión del riesgo asociados en el desarrollo de sus procesos, en aras de cumplir con su responsabilidad de diseñar, adoptar y promover las políticas, planes, programas y proyectos que contribuyan al desarrollo social y económico de la población, al desarrollo integral de los ciudadanos y la mejora en su calidad de vida.

El objetivo de la política es establecer los parámetros necesarios para una adecuada gestión de los riesgos de gestión, corrupción, Seguridad y Privacidad de la información, Seguridad Digital y Continuidad de los servicios del Ministerio/Fondo único de Tecnologías de la Información y las comunicaciones procurando que no se materialicen, atendiendo los lineamientos establecidos en Guía para la administración del riesgo y el diseño de controles en entidades públicas del DAFP, orientando a la toma de decisiones oportunas y minimizando efectos adversos al interior de la Entidad, con el fin de dar continuidad a la gestión institucional y asegurar el cumplimiento de los compromisos con los Grupos de interés.

El tratamiento de riesgos es la respuesta establecida por la primera línea de defensa, es decir, el líder o responsable del proceso junto con su equipo de trabajo para la mitigación de los diferentes riesgos.

El tratamiento o respuesta dada al riesgo, se enmarca en las siguientes categorías:

- **Aceptar el riesgo:** No se adopta ninguna medida que afecte la probabilidad o el impacto del riesgo. (Ningún riesgo de corrupción es aceptado). La aceptación del riesgo puede ser una opción viable en la entidad, para los riesgos bajos, pero también pueden existir escenarios de riesgos a los que no se les puedan aplicar controles y por ende, se acepta el riesgo. En ambos escenarios debe existir un seguimiento continuo del riesgo.

- **Reducir el riesgo:** Se adoptan medidas para reducir la probabilidad o el impacto del riesgo, o ambos; por lo general conlleva a la implementación de controles. Deben seleccionarse controles apropiados y con una adecuada segregación de funciones, de manera que el tratamiento al riesgo adoptado logre la reducción prevista sobre este.

- Evitar el riesgo: Se abandonan las actividades que dan lugar al riesgo, es decir, no iniciar o no continuar con la actividad que lo provoca.

- **Compartir el riesgo:** Se reduce la probabilidad o el impacto del riesgo transfiriendo o compartiendo una parte de este. Los riesgos de corrupción se pueden compartir, pero no se puede transferir su responsabilidad. Los dos principales métodos de compartir o transferir parte del riesgo son: seguros y tercerización.

La gestión de riesgos de Seguridad y privacidad de la Información, seguridad digital y continuidad de la operación de los servicios le permite a la ESE realizar una identificación, análisis y tratamiento de los riesgos que puedan generar afectación al cumplimiento de los objetivos de sus procesos, contribuyendo en la toma de decisiones, y en la prevención de la materialización de estos. La administración de riesgos de seguridad y privacidad de la información se encuentra enfocada en identificar, analizar, valorar y tratar las amenazas y vulnerabilidades de los activos de información de la entidad, teniendo presente su criticidad y protección. Las etapas presentes en la gestión de riesgos permiten alinearlas con los objetivos, estrategias y políticas corporativas, logrando un nivel de riesgo que pueda aceptar o asumir la Alta Dirección.

1. Política de tratamiento de datos

La E.S.E. Hospital San Juan de Dios, está comprometida en dar un correcto uso y tratamiento de los datos personales y datos personales sensibles de sus titulares, evitando el acceso no autorizado a terceros que permita conocer, vulnerar, modificar, divulgar y/o destruir la información, para lo cual cuenta con políticas de seguridad de la información que incluyen medidas de control de obligatorio cumplimiento.

La Entidad, solicita a los titulares de la información los datos necesarios para prestar los servicios de salud cumpliendo con las funciones asignadas por la normativa vigente. La información sensible requerida será de libre y voluntaria entrega por parte del respectivo Titular.

Salvo las excepciones previstas en la ley, el tratamiento de los datos personales sólo podrá realizarse con el consentimiento previo, expreso e informado de sus titulares manifestado de forma oral o mediante conductas inequívocas del Titular que permitan concluir de forma razonable que otorgó la autorización.

La E.S.E. Hospital San Juan de Dios, solicitará a las entidades responsables de pago, colaboradores, estudiantes y contratistas, los datos personales necesarios para establecer la respectiva relación y/o vinculación (civil, laboral, comercial o educativa). La información sensible requerida será de libre y voluntaria entrega por parte del respectivo Titular, quien deberá otorgar su consentimiento y autorización para su respectivo tratamiento.

2. Finalidad con la que se efectúa la recolección de datos personales y tratamiento de los mismos:

El tratamiento de los datos personales proporcionados por los usuarios y sus familias tendrá la siguiente finalidad:

- Para la prestación de los servicios asistenciales de sus usuarios y familias.
- Actualización de datos entregados por el Titular.
- Caracterización de la población atendida basada en RIPS
- Entrega de reportes de Salud Pública de obligatorio cumplimiento.

- Dar respuesta a requerimientos a entidades de control.
- Evaluación de indicadores de oportunidad y calidad de los servicios.
- Ejercer acciones legales y en la defensa de las mismas.
- Suministro de información a las autoridades competentes en caso de ser requerida.
- En general para cualquier otra finalidad que se derive de la naturaleza jurídica de la E.S.E. Hospital San Juan de Dios.

El tratamiento de los datos personales proporcionados por los colaboradores tendrá la siguiente finalidad:

Establecer una relación contractual.

Evaluaciones de desempeño, satisfacción laboral, crecimiento personal, bienestar, seguridad y salud en el trabajo.

Cumplir el proceso de afiliación al Sistema General de Seguridad Social Integral (Entidades Promotoras de Salud, Administradoras de riesgos laborales, Fondos de pensiones y cesantías, Caja de Compensación)

Efectuar el proceso de Remuneración.

Ejercer acciones legales y en la defensa de las mismas.

Cumplir con exigencias judiciales.

Suministro de información a las autoridades competentes en caso de ser requerida.

En general para cualquier otra finalidad que se derive de la vinculación contractual.

El tratamiento de los datos personales proporcionados por las entidades responsables de pago y contratistas, sean personas naturales o jurídicas, tendrá la siguiente finalidad:

Realizar la vinculación contractual.

Efectuar el reconocimiento económico por la prestación del servicio.

Suministro de información a las autoridades competentes en caso de ser requerida.

Ejercer acciones legales y en la defensa de las mismas.

Cumplir con exigencias judiciales.

3. Deberes de la E.S.E. Hospital San Juan de Dios.

- Garantizar al usuario el pleno y efectivo derecho constitucional de habeas data.
- Mantener la información en condiciones de seguridad y privacidad.
- Hacer uso de la información para los fines misionales y previstos en la ley.
- Tramitar de manera oportuna los reclamos que tengan los usuarios frente a la información consignada en la base de datos.
- No vender, circular o intercambiar la base de datos de sus usuarios, sin causa legal o contractual que lo justifique.

4. Derechos de los Titulares

El Titular de los datos personales y datos personales sensibles tendrá los siguientes derechos:

- Conocer, actualizar y rectificar los datos que aparezcan en la misma. Este derecho se podrá ejercer, entre otros frente a datos parciales, inexactos, incompletos, fraccionados, que induzcan a error, o aquellos cuyo tratamiento esté expresamente prohibido o no haya sido autorizado.
- Conocer por qué y para qué la E.S.E. Hospital San Juan de Dios, recolecta información en base de datos.
- Revocar en cualquier momento la autorización dada para contener información personal en las bases de datos de la institución.
- Revocar la autorización y/o solicitar la supresión del dato cuando en el tratamiento considere que no se respetan los principios, derechos y garantías constitucionales y legales. La revocatoria y/o supresión procederá cuando la Superintendencia de Industria y Comercio haya determinado que en el tratamiento el responsable o encargado han incurrido en conductas contrarias a esta ley y a la constitución.
- Poner queja ante la Superintendencia de Industria y Comercio, cuando considere que le ha sido violado por parte de la institución su derecho al Habeas Data.
- Derecho a solicitar prueba de la autorización: salvo en los eventos en los cuales, según las normas legales vigentes, no se requiera de la autorización para realizar el tratamiento.

5. Casos que no requieren autorización para el tratamiento de datos

La autorización del Titular no será necesaria cuando se trate de:

- Información requerida por una entidad pública o administrativa en ejercicio de sus funciones legales o por orden judicial.
- Datos de naturaleza pública.
- Casos de urgencia médica o sanitaria.

- Tratamiento de información autorizado por la ley para fines históricos, estadísticos o científicos.
- Datos relacionados con el Registro Civil de las Personas.

6. Entrega de información

La información que reúna las condiciones establecidas en el Art. 13 de la Ley 1581 de 2012, podrá suministrarse a las siguientes personas:

- A los Titulares, sus causahabientes o sus representantes legales.
- A las entidades públicas o administrativas en ejercicio de sus funciones legales o por orden judicial.
- A los terceros autorizados por el Titular o por la ley.

7. Área responsable de la atención de peticiones, consultas y reclamos.

El área responsable de la atención de peticiones, consultas y reclamos será SIAU de la E.S.E. Hospital San Juan de Dios", la cual una vez reciba la solicitud de acuerdo con el capítulo siguiente la remitirá al área responsable del tratamiento de los datos.

8. Procedimiento para la atención de peticiones, consulta y reclamos

- El Titular de la información contenida en la base de datos de la E.S.E. Hospital San Juan de Dios o por su representante legal, podrá ejercer su derecho de conocer, actualizar, rectificar, suprimir y revocar la información contenida en las mismas, mediante un correo electrónico hospitaldeconcordia@hospital-concordia.gov.co y en comunicación escrita a la dirección Cra 18 N° 16-05

- La solicitud debe ser clara en lo que se pretende, ya sea conocer, actualizar, rectificar, suprimir y/o revocar la información que se encuentra contenida en una base de datos. Además, deberá contener los datos de contacto del peticionario para poder darle una respuesta.

- Independientemente del mecanismo utilizado para la radicación de solicitudes de consulta, las mismas serán atendidas en un término máximo de diez (10) días hábiles contados a partir de la fecha de su recibo. Cuando no fuere posible atender la consulta dentro de dicho término, se informará al interesado, expresando los motivos de la demora y señalando la fecha en que se atenderá su consulta, la cual en ningún caso podrá superar los cinco (5) días hábiles siguientes al vencimiento del primer término.

- Los reclamos para corrección, actualización o supresión de datos serán contestados dentro de los quince (15) días hábiles siguientes, contados a partir del día siguiente a la fecha de su recibo. Cuando no fuere posible atenderlo dentro de dicho término se informará al interesado antes del

vencimiento del referido plazo los motivos de la demora y la fecha en que se atenderá su reclamo, la cual en ningún caso podrá superar los ocho (8) días hábiles siguientes al vencimiento del primer término.

- Si el reclamo resulta incompleto, se requerirá al interesado dentro de los cinco (5) días siguientes a la recepción del reclamo para que subsane las fallas. Una vez recibido el reclamo completo, se incluirá en la base de datos una leyenda que diga "reclamo en trámite" y el motivo del mismo, en un término no mayor a dos (2) días hábiles. Dicha leyenda deberá mantenerse hasta que el reclamo sea decidido. De igual forma, si Transcurridos dos (2) meses desde la fecha del requerimiento, sin que el solicitante presente la información requerida, se entenderá que ha desistido del reclamo.

- La primera instancia de la reclamación será la E.S.E. Hospital San Juan de Dios, y una vez agotada esta sin respuesta satisfactoria, podrá el Titular recurrir a la Superintendencia de Industria y Comercio.

7. METODOLOGÍA

El Plan de Tratamiento de Riesgos contempla la definición de las actividades a desarrollar en aras de mitigar los riesgos sobre los activos, estas actividades se estructuraron de la siguiente manera, siguiendo las recomendaciones de la Guía de Gestión de Riesgos de Seguridad y Privacidad de la Información (MinTIC:2016)[2]:

Gestión	Actividad	Tarea	Responsable	Fechas Inicio	Fecha fin
Gestión de riesgos	Actualización de lineamientos de riesgos	Actualización de políticas y metodologías de gestión de riesgos	Equipo gestión de Riesgos	Marzo de 2026	Diciembre de 2026
	Sensibilización	Socialización Guía y Herramienta -Gestión de Riesgos de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación.	Equipo gestión de Riesgos	Abril de 2026	Diciembre de 2026
	Identificación de riesgos de seguridad y privacidad de la información, seguridad digital y	Identificación, Análisis y Evaluación de Riesgos-Seguridad y Privacidad en la Información, Seguridad Digital y Continuidad de la Operación.	Equipo gestión de Riesgos	Mayo de 2026	Diciembre de 2026

Gestión	Actividad	Tarea	Responsable	Fechas Inicio	Fecha fin
	continuidad de la operación	Realimentación, revisión y verificación de los riesgos identificados (Ajustes)	Equipo gestión de Riesgos	Mayo de 2026	Diciembre de 2026
	Aceptación de riesgos identificados	Aceptación, aprobación riesgos identificados y planes de tratamiento	Equipo gestión de Riesgos	Junio de 2026	Diciembre de 2026
	Publicación	Publicación matriz de riesgos	Equipo gestión de Riesgos	Junio de 2026	Diciembre de 2026
	Seguimiento fase de tratamiento	Seguimiento Estado Planes de Tratamiento de riesgos identificados y verificación de evidencias	Equipo gestión de Riesgos	Junio de 2026	Diciembre de 2026
	Evaluación de riesgos residual	Evaluación de riegos residuales	Equipo gestión de Riesgos	Junio de 2026	Diciembre de 2026
	Mejoramiento	Identificación de oportunidades de mejora acorde a los resultados obtenidos durante la evaluación de riesgos residuales	Equipo gestión de Riesgos	Junio de 2026	Diciembre de 2026
		Actualización Guía gestión de riesgos seguridad de la Información, de acuerdo a los cambios solicitados	Equipo gestión de Riesgos	Junio de 2026	Diciembre de 2026
	Monitoreo y revisión	Generación, presentación y reporte de indicadores	Equipo gestión de Riesgos	Junio de 2026	Diciembre de 2026

7.1. Desarrollo metodológico

- **Fase 1: Análisis de la información**

En esta etapa se evaluarán los resultados de las entrevistas con los colaboradores del proceso de TI, se desarrollarán las siguientes actividades:

- Aplicar las políticas de tratamiento de riesgos.
- Determinar los controles (se desprenden de las medidas) aplicados en el Ministerio TIC.
- Determinar los riesgos que van a ser incluidos en el Plan de Tratamiento de Riesgos.

- **Fase 2: Desarrollo de los proyectos**

En esta fase se realizarán las actividades que permitan la estructuración de las medidas.
- Determinar el nombre de la medida.
- Definir los responsables de cada medida.
- Establecer el objetivo de cada medida.
- Elaborar la justificación de la medida.
- Definir las actividades a realizar para el desarrollo de la medida.

- **Fase 3: Análisis de los proyectos**

- Definición de los controles relacionados con cada medida.
- Validar los riesgos mitigados por cada medida.
- Análisis de la aplicabilidad de las medidas.
- Priorización de las medidas.

- **Fase 4: Definición del organigrama de responsabilidad**

En esta fase se realizará un organigrama y se definirán responsabilidades respecto a la administración y gestión del riesgo, esta etapa deberá ser definida por el Ministerio teniendo en cuenta su estructura organizacional para la gestión de riesgos.
- Identificación de las funciones del Ministerio en materia de seguridad de la información.
- Definición del grupo de trabajo de gestión de riesgo por parte del Ministerio.
- Definición de las funciones del grupo de trabajo referentes a la aplicación y gestión de las medidas.

- **Fase 5: Ciclo de vida del tratamiento de riesgos**

Definir las actividades a realizar por cada uno de los elementos del ciclo de vida del Plan de Tratamiento de Riesgos.

Planear: Dentro de esta etapa se desarrollan las actividades definidas en la fase 1 de la metodología de tratamiento de riesgos.

Hacer: En este paso del ciclo de vida se desarrollarán las actividades enmarcadas en la fase 2 de la metodología del tratamiento de riesgos.

Verificar: En esta etapa se desarrollarán las actividades que permiten hacer seguimiento o auditorías a la ejecución de cada una de las medidas.

Actuar: Dentro de esta etapa se realizarán las mejoras teniendo en cuenta el seguimiento y los resultados de las auditorías de la ejecución de los proyectos.

7.2. Oportunidad de Mejora

La ESE no sólo deberá centrarse en los riesgos identificados, sino que este análisis o apreciación del riesgo debe ser la base para identificar oportunidades. Por lo anterior la oportunidad deberá entenderse como la consecuencia positiva frente al resultado del tratamiento del Riesgo.

8. RECURSOS

La ESE, en el marco de la gestión de riesgos de Seguridad y Privacidad de la información, Seguridad Digital y Continuidad de la Operación de los servicios, dispone de los siguientes recursos.

RECURSOS	VARIABLE
Humanos	El líder Tecnologías de la información a través de seguridad de la información es responsable de coordinar, implementar, modificar y realizar seguimiento a las políticas, estrategias y procedimientos en la Entidad en lo concerniente a la seguridad y privacidad de la información lo cual contribuye a la mejora continua.
Técnicos	Guía de Guía para la administración del riesgo y el diseño de controles en entidades públicas - Lineamientos del Modelo Nacional de Gestión de Riesgo de Seguridad de la Información en Entidades Públicas Dirigida a las entidades del Estado
Logísticos	Gestión de recursos para realizar socializaciones, transferencia de conocimientos y seguimiento a la gestión de riesgos.
Financieros	Recursos para la adquisición de conocimiento, recursos humanos, técnicos, y desarrollo de auditorías

9. PRESUPUESTO

La estimación y asignación del presupuesto para el plan de tratamiento de riesgos de Seguridad y Privacidad de la información, Seguridad Digital y Continuidad de la Operación de los servicios identificados en la entidad, corresponderá al dueño del riesgo, quien es el responsable de contribuir con el seguimiento y control de la gestión, además de la implementación de los controles definidos en el plan de tratamiento.

10. MEDICIÓN DEL MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

La medición se realiza con un indicador de gestión que está orientada principalmente en la medición de eficacia de los componentes de implementación y gestión definidos en el modelo de operación del marco de seguridad y privacidad de la información, indicador que se alimenta de indicadores internos en el marco de la implementación del Eje de Seguridad de la Información y que servirán como insumo para el componente de mejora continua permitiendo adoptar decisiones de mejora sobre Seguridad de la informa.

9. MEDICIÓN

La medición se realiza con un indicador de gestión que está orientado principalmente a determinar el porcentaje de implementación de los controles definidos en el tratamiento de riesgos de seguridad y privacidad de la información.

Dimensión: Entorno del ecosistema digital

Objetivo: Consolidar a la ESE como una organización donde existe la innovación basada en procesos transversales y orientados al desarrollo potencial de su personal.

Proceso: Gestión de tecnologías de la información.

Datos del indicador

Nombre del indicador: nivel de implementación de los controles para los riesgos de seguridad y privacidad de la información, Seguridad digital y continuidad de la operación.

Objetivo del indicador: Medir el nivel de implementación de los controles para los riesgos de seguridad y privacidad de la información, Seguridad digital y continuidad de la operación.

Tipo de indicador: Eficacia
Frecuencia de la información: Mensual
Responsable del análisis: Líder encargado de coordinar el tema de seguridad Digital.
Frecuencia del análisis: Trimestral
Fuentes de la información: Informe de seguimiento al desarrollo y mantenimiento de sistemas información / Formatos de acuerdos de desarrollo y de requerimiento acordados.
Metas:
Desde 0% a 59% - Bajo
Desde 60% a 84 - medio
Desde 85% a 100 Alto

11. Gestión De riesgos De Seguridad De La Información Para Entidades Publicas

En los siguientes numerales se indican los aspectos complementarios a lo expuesto en el documento "Guía para la administración del riesgo y el diseño de controles en entidades públicas"[10], donde se incluyen los riesgos de seguridad de la información.

12 Fase 1. Planificación de la GRSD

La fase de planificación comprende todo lo expuesto en los Pasos 1, 2 y 3 de la "Guía para la administración del riesgo y el diseño de controles en entidades públicas", emitida por el Departamento Administrativo de la Función Pública, es decir, comprende todo lo relacionado con las siguientes actividades:

Definición del contexto interno, externo y de los procesos de la entidad pública.

- Definición de la política de administración de riesgo.
- Designación de roles y responsabilidades.}
- Definición de criterios de probabilidad, impacto y zonas de riesgo aceptable.
- Identificación de activos de información.
- Identificación de riesgos.
- Valoración de riesgos.
- Definición del tratamiento de los riesgos.

Respecto a estas actividades, el presente documento busca profundizar en lo concerniente a riesgos de seguridad de la información, en cada una de ellas, siendo el documento del Departamento Administrativo de la Función Pública -DAFP-, el documento metodológico principal.

13. Contexto interno y externo de la entidad pública

Conforme lo indica el DAFP, las entidades públicas deben realizar la identificación del contexto interno y externo de la entidad, sin embargo, es necesario profundizar en este análisis relacionado con seguridad de la información, por lo tanto, a continuación, se dan unas directrices adicionales para realizar la actividad adecuadamente.

Las entidades deben revisar los ecosistemas digitales desde la óptica de los daños colaterales que pueden presentarse dentro de la organización, y que pueden impactar en la afectación del principio de disponibilidad, sin que necesariamente el evento inicial sea considerado como de orden digital.

Establecimiento del contexto externo: Para determinar el contexto externo, la entidad pública debe considerar, sin limitarse, los siguientes factores relacionados con el entorno digital:

CONTEXTO EXTERNO

- Clientes, proveedores de servicios y empresas que sean competencia directa y/o se relacionen con la misión de la entidad pública analizada.
- Normativas o aspectos jurídicos que apliquen directa o indirectamente a la entidad pública; ejemplo, la Ley 1581 de 2012 o la Ley 1712 de 2014, circulares o regulaciones emitidas por superintendencias o ministerios, como el Decreto 1078 de 2015 o el Decreto número 1083 de 2015, modificado por el Decreto 1499 de 2017.
- Dependencias económicas y financieras por parte de otras empresas.
- Entorno cultural.
- Cualquier otro factor externo de tipo internacional, nacional (gobierno), regional o local.
- Cantidad de ciudadanos a los cuales la entidad pública brinda u ofrece servicios a través del entorno digital como trámites a través de páginas web.
- Aspectos externos que pueden verse afectados con los riesgos de seguridad

Fuente: Ministerio de Tecnologías de la Información y las Comunicaciones.

Establecimiento del contexto interno: Para esto se considera factores que impactan directamente a:

- La entidad pública, en general, su organización, sistemas de información o servicios, reglamentación interna, número de sedes, empleados, entre otros aspectos.

- Cada uno de los procesos sobre los cuales están soportadas sus operaciones.

Para determinar los factores de la entidad pública y los procesos se debe considerar, sin limitarse, los siguientes factores relacionados con el entorno digital:

PARA LA ENTIDAD PÚBLICA	PARA LOS PROCESOS
• Recursos económicos, sociales, ambientales, físicos, tecnológicos, financieros, jurídicos, entre otros • Flujos de información y los procesos de toma de decisiones • Empleados, contratistas • Objetivos estratégicos y la forma de alcanzarlos • La misión, visión, valores y cultura de la organización • Sus políticas, procesos y procedimientos • Sistemas de gestión (calidad, seguridad en el trabajo, seguridad de la información, riesgos, entre otros) • Toda la estructura organizacional • Roles y responsabilidades • Sistemas de información o servicios. • Infraestructuras físicas, servicios y sistemas de información de apoyo y servicios logísticos transversales.	• Identificación de los procesos y su respectiva caracterización • Detalle de las actividades que se llevan a cabo en el proceso • Flujos de información • Identificación y actualización de los activos en la cadena de valor de la entidad pública • Recursos • Alcance del proceso • Relaciones con otros procesos de la entidad pública • Cantidad de ciudadanos afectados por el proceso • Procesos de gestión de riesgos que se tienen actualmente implementados • Personal involucrado en la toma de decisiones

Tabla 1 Factores del entorno digital

Fuente: Ministerio de Tecnologías de la Información y las Comunicaciones.

Para llevar a cabo esta actividad se sugiere hacer una lista en la que estén enumeradas las partes interesadas externas e internas que tengan relación con la entidad pública y con sus objetivos, misión o visión.

14. Alcance para aplicar la gestión de riesgos de seguridad de la información

El alcance de la administración del riesgo de seguridad de la información debe ser extensible y aplicable a los procesos de la entidad pública, así como a los grupos de valor que indiquen los criterios diferenciales del Modelo de Seguridad y Privacidad de la Información[11] , habilitador de la Estrategia de Gobierno Digital expedida por el MINTIC.

11 http://www.mintic.gov.co/gestionti/615/articles-5482_Modelo_de_Seguridad_Privacidad.pdf

Alineación o creación de la política de gestión de riesgo de seguridad de la información

Es necesario que la entidad pública establezca una política de gestión de riesgo integral, donde se incluya el compromiso en la gestión de los riesgos de seguridad de la información en todos sus niveles. Esta debe crearse como lo indica la guía para la Administración del Riesgo y el diseño de controles en entidades públicas del DAFP en el Paso 1, incluyendo la gestión de riesgos de seguridad de la información. Esta actividad es responsabilidad de la Línea estratégica dispuesta por el MIPG.

Definición de roles y responsabilidades

Además de las líneas de defensa y las responsabilidades designadas en la Guía para la Administración del Riesgo y el diseño de controles en entidades públicas" del DAFP, es necesario indicar o profundizar en las responsabilidades que deberá tener designadas el responsable de Seguridad digital:

Responsable de seguridad de la información

Cada entidad pública debe designar una persona o grupo responsable de Seguridad Digital que también es el responsable de la Seguridad de la Información, el cual debe pertenecer a un área que haga parte de la Alta Dirección o Línea Estratégica, como lo establece el Manual Operativo del MIPG en el numeral 3.2.1.4 Política de Seguridad de la información, se recomienda que este responsable pertenezca a un área diferente a la de tecnología con el fin de evitar conflicto de intereses. Las responsabilidades que deberá cumplir respecto a la gestión del riesgo de seguridad de la información serán las siguientes:

RESPONSABLE DE SEGURIDAD DE LA INFORMACIÓN
•Actualizar el procedimiento para la Identificación y Valoración de Activos de la Entidad, de acuerdo a los criterios de seguridad de la información (Confidencialidad, integridad y disponibilidad).
•Adoptar o adecuar el procedimiento formal para la gestión de riesgos de seguridad de la información (Identificación, Análisis, Evaluación y Tratamiento).
•Asesorar y acompañar a la primera línea de defensa en la realización de la gestión de riesgos de seguridad de la información y en la recomendación de controles para mitigar los riesgos.
•Apoyar en el seguimiento a los planes de tratamiento de riesgo definidos.
•Informar a la línea estratégica sobre cualquier variación importante en los niveles o valoraciones de los riesgos de seguridad de la información.

Fuente: Ministerio de Tecnologías de la Información y las Comunicaciones

Nota: Como complemento de esta actividad, la entidad pública debe tomar como

referencia lo definido en el documento de Lineamientos de Roles y responsabilidades del MSPI de la Estrategia de Gobierno Digital del MINTIC, en complemento a lo anterior.

Definición de recursos para la Gestión de riesgos de seguridad de la información

La entidad pública debe disponer los recursos suficientes para el desarrollo de la gestión de riesgos de seguridad de la información, (capital, tiempo, personal, procesos, sistemas y tecnologías), con el fin de apoyar a los responsables en la implementación de controles y seguimiento de los riesgos de seguridad de la información.

La línea estratégica o alta dirección debe asignar entre otros, recursos tales como:

- Personal capacitado e idóneo para la gestión del riesgo de seguridad de la información.
- Recursos económicos para la implementación de controles para la mitigación de riesgos (con base al análisis de riesgo realizado, teniendo en cuenta el alcance de la política de riesgos de la entidad en cuanto a seguridad de la información), que permita ser incluido dentro de la gestión presupuestal y eficiencia del gasto público de la entidad.
- Recursos para los aspectos de mejora continua, monitoreo y auditorías.

Identificación de activos de información

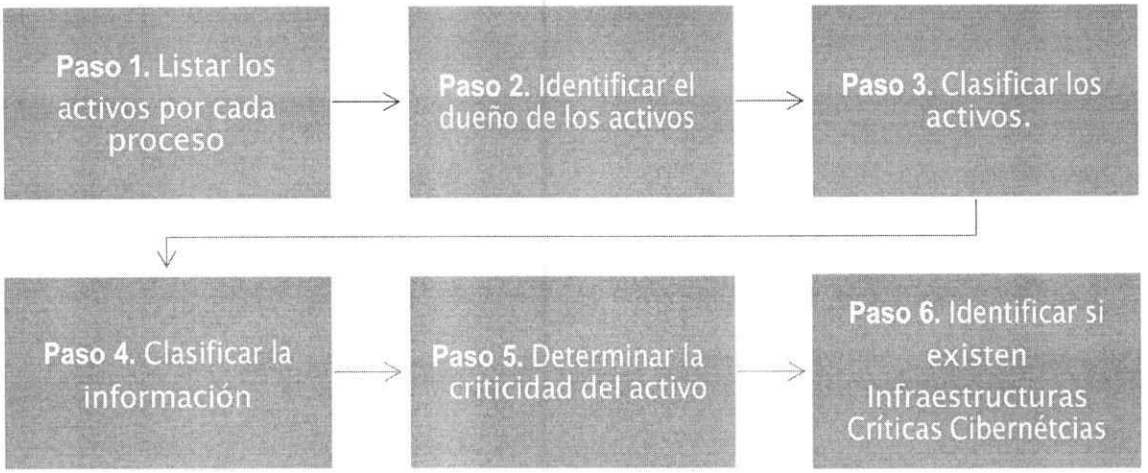
Un activo de información es cualquier elemento que participe en el tratamiento de información que tenga valor para la organización, sin embargo, en el contexto de seguridad de la información son activos elementos tales como: hardware, software, aplicaciones de la entidad pública, servicios Web, redes, información digital, personal, ubicación, organización, Tecnologías de la Información -TI- o Tecnologías de la Operación -TO-) que utiliza la organización para su funcionamiento y que por afectación operativa, se afecte el principio de disponibilidad.

Es necesario que la entidad pública identifique los activos de información y documente un inventario de activos, así podrá saber lo que se debe proteger para garantizar tanto su funcionamiento interno (BackOffice) como su funcionamiento de cara al ciudadano (Front Office), aumentando así su confianza en el uso del entorno digital para interactuar con las partes interesadas.

La identificación y valoración de activos debe ser realizada por la Primera Línea de Defensa – Líderes de Proceso, en cada proceso donde aplique la gestión del riesgo de seguridad de la información, siendo debidamente orientados por el responsable de seguridad digital o de seguridad de la información de la entidad pública.

Para la generación de este inventario, la entidad pública debe tener en cuenta los

siguientes pasos:



Fuente: Ministerio de Tecnologías de la Información y las Comunicaciones

A continuación, se especifica lo que deberá tenerse en cuenta para la realización de cada uno de los pasos mencionados para la identificación y valoración de activos.

Paso 1. Listar los activos por cada proceso:

En cada proceso, deberán listarse los activos, indicando algún consecutivo, nombre y descripción breve de cada uno.

Ejemplo:

PROCESO	ACTIVO	DESCRIPCION
Gestión Financiera	Base de datos de nómina	Base de datos con información de nómina de la entidad
Gestión Financiera	Aplicativo de Nómina	Sistema que permite gestionar la nómina y los pagos
Gestión Financiera	Cuentas de Cobro	Formatos de cobro diligenciados

Fuente: Ministerio de Tecnologías de la Información y las Comunicaciones

NOTA: Las entidades públicas pueden adicionar identificadores o nemónicos para complementar la identificación de los activos.

Paso 2. Identificar el dueño de los activos:

Cada uno de los activos identificados deberá tener un dueño designado, Si un activo no posee un dueño, nadie se hará responsable ni lo protegerá debidamente.

Ejemplo:

ACTIVO	DESCRIPCION	DUEÑO DEL ACTIVO
Base de datos de nómina	Base de datos con información de nómina de la entidad	Jefe Oficina de Nómina
Aplicativo de Nómina	Sistema que permite gestionar la nómina y los pagos	Jefe Oficina de Nómina
Cuentas de Cobro	Formatos de cobro diligenciados	Jefe Oficina de Nómina

Fuente: Ministerio de Tecnologías de la Información y las Comunicaciones

NOTA: Generalmente el dueño del activo es el líder del proceso o el jefe de una de las áreas pertenecientes al proceso.

Paso 3. Clasificar los activos:

Cada activo debe tener una clasificación o pertenecer a un determinado grupo de activos según su naturaleza cómo, por ejemplo: Información, Software, Hardware, Componentes de Red entre otros.

La siguiente tabla presenta una propuesta de tipología de activos con el fin de hacer la clasificación mencionada.

Tipo de activo	Descripción
Información	Información almacenada en formatos físicos (papel, carpetas, CD, DVD) o en formatos digitales o electrónicos (ficheros en bases de datos, correos electrónicos, archivos o servidores), teniendo en cuenta lo anterior, se puede distinguir como información: Contratos, acuerdos de confidencialidad, manuales de usuario, procedimientos operativos o de soporte, planes para la continuidad del negocio, registros contables, estados financieros, archivos ofimáticos, documentos y registros del sistema integrado de gestión, bases de datos con información personal o con información relevante para algún proceso (bases de datos de nóminas, estados financieros) entre otros.
Software	Activo informático lógico como programas, herramientas ofimáticas o sistemas lógicos para la ejecución de las actividades
Hardware	Equipos físicos de cómputo y de comunicaciones como, servidores, biométricos que por su criticidad son considerados activos de información
Servicios	Servicio brindado por parte de la entidad para el apoyo de las actividades de los procesos, tales como: Servicios WEB, intranet, CRM, ERP, Portales organizacionales, Aplicaciones entre otros (Pueden estar compuestos por hardware y software)
Intangibles	Se consideran intangibles aquellos activos inmateriales que otorgan a la entidad una ventaja competitiva relevante, uno de ellos es la imagen corporativa, reputación o el *'good will'*, entre otros

Infraestructura crítica cibernética nacional	Se entiende por aquella infraestructura 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.

Tipo de activo	Descripción
	Medios necesarios para realizar la conexión de los elementos de hardware y software en una red, por ejemplo, el cableado estructurado y tarjetas de red, routers, switches, entre otros
Recursos Humanos	Aquellos roles que, por su conocimiento, experiencia y criticidad para el proceso, son considerados activos de información, por ejemplo: personal con experiencia y capacitado para realizar una tarea específica en la ejecución de las actividades
Instalaciones y Otros Servicios	Espacio o área asignada para alojar y salvaguardar los datos considerados como activos críticos para la empresa

Fuente: Ministerio de Tecnologías de la Información y las Comunicaciones

Ejemplo:

ACTIVO	TIPO DE ACTIVO
Base de datos de nómina	Información
Aplicativo de Nómina	Software
Cuentas de Cobro	Información

Fuente: Ministerio de Tecnologías de la Información y las Comunicaciones

Paso 4. Clasificar la información:

Realizar la clasificación de la información conforme lo indican las leyes 1712 de 2014, 1581 de 2012, el Modelo de Seguridad y Privacidad en su Guía de Gestión de Activos, los controles de la norma ISO27001:2022 y demás normatividad aplicable. Esto adicionalmente ayudará a dilucidar la importancia de los activos de información en el siguiente Paso 5.

Ejemplo:

ACTIVO	*TIPO DE ACTIVO*	*Ley 1712 de 2014*	*Ley 1581 de 2012*
Base de datos de nómina	Información	Información Reservada	Contiene datos personales
Aplicativo de Nómina	Software	N/A	N/A
Factura de venta	Información	Información Pública	No contiene datos personales

Fuente: Ministerio de Tecnologías de la Información y las Comunicaciones

NOTA: Al realizar la identificación del contexto externo, la entidad pública debería tener plenamente identificados los aspectos regulatorios y normativos con los que deberá cumplir, las leyes enunciadas (1712 de 2014 y 1581 de 2012) pueden ser de cumplimiento para la mayoría de las entidades públicas sin embargo es tarea de la entidad pública determinar si hay más o menos aspectos regulatorios para tener en cuenta respecto a la información. El **área jurídica** de Las entidades debe colaborar en esta tarea específica.

En este paso la entidad pública debe definir las escalas (que significa criticidad ALTA, MEDIA y BAJA) para valorar los activos respecto a la confidencialidad, integridad y disponibilidad e identificar su nivel de importancia o criticidad para el proceso. Para definir estas escalas puede tomar como referencia el documento de Lineamentos para el Inventario de Activos de Información del Modelo de Seguridad y Privacidad de la Información (MSPI)12, estas escalas deberán ser definidas y documentadas en un procedimiento de gestión de activos que debe ser aprobado por parte de la línea estratégica de la entidad pública.

ACTIVO	TIPO DE ACTIVO	Criticidad respecto a su confidencialidad	Criticidad respecto a su completitud o integridad	Criticidad respecto a su disponibilidad	Nivel de Criticidad
Base de datos de nómina	Información	ALTA	ALTA	ALTA	ALTA

Aplicativo de Nómina	software	BAJA	MEDIA	BAJA	MEDIA
Listas de asistencia	Información	BAJA	BAJA	BAJA	BAJA

Fuente: Ministerio de Tecnologías de la Información y las Comunicaciones

Una vez se ejecute la identificación de los activos, la entidad pública debe definir si gestionará los riesgos en todos los activos del inventario o solo en aquellos que tengan un nivel de criticidad Alto o altos y medios, esto debe estar debidamente documentando y aprobado por la **Línea Estratégica — Alta dirección**.

Paso 6. Identificar si existen Infraestructuras Críticas Cibernéticas Nacionales -ICCN-

Se invita a que las entidades públicas identifiquen si poseen ICC. Un activo se caracteriza y es considerado infraestructura crítica si su impacto o afectación podría cumplir alguno de los criterios establecidos por el COLCERT en sus LINEAMIENTOS EN CIBERSEGURIDAD

Si la entidad pública determina que tiene ICC, es importante que se identifiquen los componentes que conforman dicha infraestructura. Por ejemplo, dicha ICC puede tener componentes de TI (como servidores) o de TO (como sistemas de control industrial o sensores).

Las entidades deberán consultar y aplicar los criterios y la metodología de identificación de infraestructura critica cibernética que esté vigente, cada vez que realicen el inventario de activos de información o una actualización a este, estos criterios y metodología serán actualizados por el ColCERT.

Con base a los seis (6) pasos vistos previamente, la entidad pública podría generar un formato como el siguiente (ejemplo de referencia) para generar tanto su procedimiento de identificación e inventario de activos como el formato para hacer su levantamiento. El formato puede variar en cada entidad según la necesidad y normatividad aplicable o si desea integrar otra información.

Proceso	Activo	Descripción	Dueño del Activo	Tipo de Activo	Clasificación de información (Ley 1581 de 2012 / Ley 1712 de 2014)	Criticidad del Activo (De acuerdo con su confidencialidad, integridad y disponibilidad)
Ver Paso 1	Ver Paso 1	Ver Paso 1	Ver Paso 2	Ver Paso 3	Ver Paso 4	Ver Paso 5
Gestión Financiera	Base de datos de nómina	Base de datos con información de nómina de la entidad	Jefe oficina de nómina	Información	Ley 1712 Información reservada Ley 1581 Contiene datos personales Otras normas que apliquen	ALTA

Fuente: Ministerio de Tecnologías de la Información y las Comunicaciones

Recomendaciones adicionales para la identificación de activos:

Para identificar los activos, realizar su inventario y clasificación, las entidades públicas pueden emplear los siguientes métodos:

- Revisión de los flujos o diagramas del proceso.
- Revisión de inventarios de activos previos o de otras áreas.
- Entrevistas o lluvia de ideas dentro de cada proceso.

Nota: adicional a lo anterior, el documento de **Lineamientos para el Inventario y Clasificación de Activos de Información e Infraestructura Critica Cibernética Nacional del Modelo de Seguridad y Privacidad de la Información** de la Estrategia Gobierno

Digital de MINTIC, también brinda una orientación para clasificar los activos de información.

Importante:

La entidad pública puede decidir si realiza la gestión de riesgos en todos los activos identificados en este punto o si desea hacerlo a los activos más críticos. Esta decisión debe estar debidamente formalizada en el procedimiento de gestión de activos que solicita el **Modelo de Seguridad y Privacidad de la Información**. Adicionalmente, debe quedar explícita en la Política de Administración de Riesgos de la entidad pública, debidamente aprobada por el Comité Institucional de Coordinación de Control Interno.

Identificar los riesgos inherentes de seguridad de la información

Como lo indica el Paso 2 de la "Guía para la Administración del Riesgo en la Gestión, Corrupción y Seguridad de la información. Diseño de Controles en Entidades Públicas " emitida por el DAFP, para efectos del presente modelo se podrán identificar los siguientes tres (3) riesgos inherentes de seguridad de la información:

- Pérdida de la confidencialidad.
- Pérdida de la integridad.
- Pérdida de la disponibilidad.

Para cada riesgo, se deben asociar el grupo de activos o activos específicos del proceso o su ecosistema digital operativo, y conjuntamente analizar las posibles amenazas y vulnerabilidades que podrían causar su materialización. A continuación, se mencionan un listado de amenazas y vulnerabilidades que podrían materializar los tres (3) riesgos previamente mencionados:

a) Identificación de Amenazas:

Se plantean los siguientes listados de amenazas, que representan situaciones o fuentes que pueden hacer daño a los activos y materializar los riesgos. A manera de ejemplo se citan las siguientes amenazas:

Ejemplos de amenazas clásicas

Categoría	N°	Descripción de la amenaza	Tipo de fuente de riesgo *
Amenazas físicas	TP01	Fuego	A, D, E
	TP02	Agua	A, D, E
	TP03	Contaminación, radiación nociva	A, D, E
	TP04	Accidente grave	A, D, E
	TP05	Explosión	A, D, E
	TP06	Polvo, corrosión, heladas	A, D, E
Amenazas naturales	TN01	Fenómeno climático	E
	TN02	Fenómeno sísmico	E
	TN03	Fenómeno volcánico	E
	TN04	Fenómeno meteorológico	E
	TN05	Inundación	E
	TN06	Fenómeno de pandemia/epidemia	E
Fallas en las infraestructuras	TI01	Fallas en un sistema de suministro	A, D
	TI02	Falla del sistema de refrigeración o ventilación	A, D
	TI03	Pérdida del suministro eléctrico	A, D, E
	TI04	Falla de una red de telecomunicaciones	A, D, E
	TI05	Falla del equipo de telecomunicaciones	A, D
	TI06	Radiación electromagnética	A, D, E
	TI07	Radiación térmica	A, D, E
	TI08	Impulsos electromagnéticos	A, D, E
Fallas técnicas	TT01	Falla de dispositivos o sistemas	A
	TT02	Saturación del sistema de información	A, D
	TT03	Vulneración del mantenimiento del sistema de información	A, D
Acciones huma	TH01	Atentado terrorista, sabotaje	D
	TH02	Ingeniería social	D
	TH03	Interceptación de la radiación de un dispositivo	D
	TH04	Espionaje remoto	D
	TH05	Escucha clandestina	D
	TH06	Robo de medios o documentos	D
	TH07	Robo de equipos	D
	TH08	Robo de identidad digital o de credenciales	D
	TH09	Recuperación de medios reciclados o descartados	D
	TH10	Divulgación de información	A, D
	TH11	Entrada de datos de fuentes no fiables	A, D

nas	TH12	Manipulación con hardware	D
	TH13	Manipulación con software	A, D
	TH14	Ataque de descarga oculta a través de internet	D
	TH15	Ataque de repetición, ataque de intermediario	D
	TH16	Tratamiento no autorizado de datos personales	A, D
	TH17	Entrada no autorizada en instalaciones	D
	TH18	Uso no autorizado de dispositivos	D
	TH19	Uso incorrecto de dispositivos	A, D
	TH20	Daño de dispositivos o medios	A, D
	TH21	Copia ilícita de software	D
	TH22	Uso de software falsificado o copiado	A, D
	TH23	Corrupción de datos	D
	TH24	Tratamiento ilegal de datos	D
	TH25	Envío o distribución de malware	A, D, E
	TH26	Detección de posición	D
Compromiso de funciones o servicios	TC01	Error en el uso	A
	TC02	Abuso de derechos o permisos	A, D
	TC03	Falsificación de derechos o permisos	D
	TC04	Denegación de acciones	D
Amenazas a la organización	TO01	Falta de personal	A, E
	TO02	Falta de recursos	A, E
	TO03	Falla de los proveedores de servicios	A, E
	TO04	Violación de la legislación o la normativa	A, D
* D : deliberado; A : accidental; E : medioambiental			

Tabla 2 Tabla de amenazas Fuente: ISO/IEC 27005:202209

- Deliberadas (D), fortuitas (F) o ambientales (A).
    - Amenazas dirigidas por el hombre: empleados con o sin intención, proveedores y piratas informáticos, entre otros.

Fuente de amenaza	Motivación	Acciones amenazantes

Pirata informático, intruso ilegal	• Reto • Ego • Rebelión • Estatus • Dinero	• Piratería • Ingeniería Social • Intrusión, acceso s forzados al sistema • Acceso no autorizado
Criminal de la computación	• Destrucción de la información • Divulgación ilegal de la información • Ganancia monetaria • Alteración no autorizada de los datos	• Crimen por computador • Acto fraudulento • Soborno de la información • Suplantación de identidad • Intrusión en el sistema

Fuente de amenaza	Motivación	Acciones amenazantes
Terrorismo	• Chantaje • Destrucción • Explotación • Venganza • Ganancia política • Cubrimiento de los medios de comunicación	• Bomba/Terrorismo • Guerra de la información • Ataques contra el sistema DDoS • Penetración en el sistema • Manipulación en el sistema
Espionaje industrial (inteligencia, empresas, gobiernos extranjeros, otros intereses)	• Ventaja competitiva • Espionaje económico	• Ventaja de defensa • Ventaja política • Explotación económica • Hurto de información • Intrusión en privacidad personal • Ingeniería social • Penetración en el sistema • Acceso no autorizado al sistema

Intrusos (Empleados con entrenamiento deficiente, descontentos, malintencionados, negligentes, deshonestos o despedidos)	• Curiosidad • Ego • Inteligencia • Ganancia monetaria • Venganza • Errores y omisiones no intencionales (ej. Error en el ingreso de datos, error de programación)	• Asalto a un empleado • Chantaje • Observar información reservada • Uso inadecuado del computador • Fraude y hurto • Soborno de información • Ingreso de datos falsos o corruptos • Interceptación • Código malicioso • Venta de información personal • Errores en el sistema • Intrusión al sistema • Sabotaje del sistema

Fuente de amenaza	Motivación	Acciones amenazantes
		• Acceso no autorizado al sistema.

Tabla 3 Tabla de amenazas dirigida por el hombre Fuente: ISO/IEC 27005:2022

b) Identificación de vulnerabilidades:
la entidad pública puede identificar vulnerabilidades (debilidades) en las siguientes áreas:

Ejemplos de vulnerabilidades clásicas

Categoría	N°	Ejemplos de vulnerabilidades
	VH01	Mantenimiento insuficiente/instalación defectuosa de los medios de almacenamiento
	VH02	Programas insuficientes para el reemplazo periódico de equipos
	VH03	Susceptibilidad a la humedad, al polvo y a la suciedad

Hardware	VH04	Sensibilidad a la radiación electromagnética
	VH05	Control insuficiente de los cambios de configuración
	VH06	Susceptibilidad a las variaciones de tensión
	VH07	Susceptibilidad a las variaciones de temperatura
	VH08	Almacenamiento sin protección
	VH09	Falta de protección a la disposición final
	VH10	Copia no controlada
Software	VS01	Pruebas de software inexistentes o insuficientes
	VS02	Defectos conocidos en el software
	VS03	No se cierra la sesión al abandonar el puesto de trabajo
	VS04	Disposición o reutilización de medios de almacenamiento sin un borrado adecuado
	VS05	Configuración insuficiente de los registros para fines de auditoría
	VS06	Asignación errónea de derechos de acceso
	VS07	Software ampliamente distribuido
	VS08	Aplicación de programas de aplicación a datos erróneos desde el punto de vista cronológico
	VS09	Interfaz de usuario complicada
	VS10	Documentación insuficiente o inexistente
	VS11	Configuración incorrecta de los parámetros
	VS12	Fechas incorrectas
	VS13	Mecanismos insuficientes de identificación y autenticación (por ejemplo, para la autenticación de usuarios)
	VS14	Tablas de contraseñas desprotegidas
	VS15	Gestión deficiente de contraseñas
	VS16	Activación de servicios innecesarios
	VS17	Programas informáticos nuevos o inmaduros
	VS18	Especificaciones poco claras o incompletas para los desarrolladores
	VS19	Control ineficiente de los cambios
	VS20	Descarga y uso de programas informáticos incontrolados
	VS21	Copias de seguridad inexistentes o incompletas
	VS22	Incumplimiento de la elaboración de informes de gestión
	VN01	Mecanismos insuficientes para la prueba de envío o recepción de un mensaje
	VN02	líneas de comunicación sin protección
	VN03	Tráfico sensible sin protección
	VN04	Cableado de empalme deficiente
	VN04	Un solo punto de falla
	VN06	Ineficacia o falta de mecanismos para la identificación y autenticación del remitente y el destinatario

Red	VN07	Arquitectura de red insegura
	VN08	Transferencia de contraseñas en claro
	VN09	Gestión inadecuada de la red (resiliencia del enrutamiento)
	VN10	Conexiones a redes públicas sin protección
Personal	VP01	Ausencia de personal
	VP02	Procedimientos inadecuados de contratación
	VP03	Formación insuficiente sobre seguridad
	VP04	Uso incorrecto de software y hardware
	VP05	Escasa concienciación en materia de seguridad
	VP06	Mecanismos de monitoreo insuficientes o inexistentes
	VP07	Trabajo de personal externo o de limpieza sin supervisión
	VP08	Ineficacia o falta de políticas para el uso correcto de los medios de telecomunicación y mensajería
Instalaci on es	VS01	Uso inadecuado o descuidado del control de acceso físico a edificios y salas
	VS02	Ubicación en una zona susceptible de inundación
	VS03	Red de energía inestable
	VS04	Protección física insuficiente del edificio, puertas y ventanas
Organiza ció n	VO01	No se ha creado un procedimiento formal para el registro y la cancelación de usuarios, o su aplicación es ineficaz
	VO02	No se ha creado un proceso formal de revisión (supervisión) de los derechos de acceso, o su aplicación es ineficaz
	VO03	Disposiciones insuficientes (en materia de seguridad) en los contratos con clientes y/o con terceros
	VO04	No se ha creado un procedimiento de monitoreo de las instalaciones de tratamiento de la información, o su aplicación es ineficaz
	VO05	Las auditorías (supervisión) no se realizan con regularidad
	VO06	No se han creado procedimientos de identificación y evaluación de riesgos, o su aplicación es ineficaz
	VO07	Insuficiencia o falta de informes de averías grabados en los registros del administrador y del operador
	VO08	Respuesta inadecuada del servicio de mantenimiento
	VO09	Acuerdo de nivel de servicio insuficiente o inexistente
	VO10	No se ha creado un procedimiento de control de cambios, o su aplicación es ineficaz
	VO11	No se ha creado un procedimiento formal para el control de la documentación del SGSI, o su implementación es ineficaz
	VO12	No se ha creado un procedimiento formal para la supervisión de los registros del SGSI, o su implementación es ineficaz
	VO13	No se ha creado un procedimiento formal para la autorización de información pública, o su implementación es ineficaz
	VO14	Asignación inadecuada de responsabilidades en materia de seguridad de la información

	VO15	Los planes de continuidad no existen, están incompletos o son obsoletos
	VO16	No se ha creado una política de uso del correo electrónico, o su aplicación es ineficaz
	VO17	No se han creado procedimientos para introducir software en los sistemas operativos, o su aplicación es ineficaz
	VO18	No se han creado procedimientos para el tratamiento de información clasificada, o su aplicación es ineficaz
	VO19	Las responsabilidades con respecto a la seguridad de la información no están presentes en las descripciones de los cargos
	VO20	Insuficiencia o falta de disposiciones (respecto a la seguridad de la información) en los contratos con los empleados
	VO21	No se ha definido el proceso disciplinario en caso de incidentes de seguridad de la información, o no funciona correctamente
	VO22	No se ha creado una política formal sobre el uso de computadores móviles, o su aplicación es ineficaz
	VO23	Control insuficiente de los activos fuera de las instalaciones
	VO24	Insuficiencia o falta de una política de "escritorio y pantalla limpios"
	VO25	Autorización de instalaciones de tratamiento de la información no implementada o que no funciona correctamente
	VO26	Los mecanismos de monitoreo de las infracciones de seguridad no se implementan correctamente
	VO27	No se han creado procedimientos para notificar las deficiencias de seguridad, o su aplicación es ineficaz
	VO28	No se han creado procedimientos de conformidad con las disposiciones en materia de derechos intelectuales, o su aplicación es ineficaz

Tabla 4 Tabla de Vulnerabilidades

Comunes Fuente: ISO/IEC

27005:2022

NOTA: La sola presencia de una vulnerabilidad no causa daños por sí misma, ya que representa únicamente una debilidad de un activo o un control, para que la vulnerabilidad pueda causar daño, es necesario que una amenaza pueda explotar esa debilidad. Una vulnerabilidad que no tiene una amenaza puede no requerir la implementación de un control.

A continuación, se presentan ejemplos de relación entre vulnerabilidades de acuerdo con el tipo de activos y las amenazas.

Tipo de activo	Ejemplos de vulnerabilidades	Ejemplos de amenazas

HARDWARE	Mantenimiento insuficiente/instalación fallida de los medios de almacenamiento	Incumplimiento en el mantenimiento del sistema de Información.
	Ausencia de esquemas de reemplazo periódico	Destrucción de equipos o medios.
	Susceptibilidad a la humedad, el polvo y la suciedad	Polvo, corrosión y congelamiento
	Sensibilidad a la radiación electromagnética	Radiación electromagnética
	Ausencia de un eficiente control de cambios en la configuración	Error en el uso

Tipo de activo	Ejemplos de vulnerabilidades	Ejemplos de amenazas
	Susceptibilidad a las variaciones de voltaje	Perdida del suministro de energía
	Susceptibilidad a las variaciones de temperatura	Fenómenos meteorológicos
	Almacenamiento sin protección física	Hurtos medios o documentos.
	Falta de cuidado en la disposición final	Hurtos medios o documentos.
	Copia no controlada	Hurtos medios o documentos.
	Ausencia o insuficiencia de pruebas de software	Abuso de los derechos
	Defectos bien conocidos en el software	Abuso de los derechos
	Ausencia de "terminación de sesión" cuando se abandona la estación de trabajo	Abuso de los derechos
	Disposición o reutilización de los medios de almacenamiento sin borrado adecuado	Abuso de los derechos
	Ausencias de pistas de auditoria	Abuso de los derechos
	Asignación errada de los derechos de acceso	Abuso de los derechos
	Software ampliamente distribuido	Corrupción de datos

SOFTWARE	En términos de tiempo utilización de datos errados en los programas de aplicación	Corrupción de datos
	Interfaz de usuario compleja	Error en el uso
	Ausencia de documentación	Error en el uso
	Configuración incorrecta de parámetros	Error en el uso
	Fechas incorrectas	Error en el uso
	Ausencia de mecanismos de identificación y autentificación, como la autentificación de usuario	Falsificación de derechos
	Tablas de contraseñas sin protección	Falsificación de derechos
	Gestión deficiente de las contraseñas	Falsificación de derechos

Tipo de activo	Ejemplos de vulnerabilidades	Ejemplos de amenazas
	Habilitación de servicios innecesarios	Procesamiento ilegal de datos
	Software nuevo o inmaduro	Mal funcionamiento del software
	Especificaciones incompletas o no claras para los desarrolladores	Mal funcionamiento del software
	Ausencia de control de cambios eficaz	Mal funcionamiento del software
	Descarga y uso no controlado de software	Manipulación con software
	Ausencia de copias de respaldo	Manipulación con software
	Ausencia de protección física de la edificación, puertas y ventanas	Hurto de medios o documentos
	Fallas en la producción de informes de gestión	Uso no autorizado del equipo
INFRAESTRUCTURA CRITICA CIBERNETICA	Ausencia de pruebas de envío o recepción de mensajes	Negación de acciones
	Líneas de comunicación sin protección	Escucha encubierta
	Tráfico sensible sin protección	Escucha encubierta

	Conexión deficiente de los cables	Fallas del equipo de telecomunicaciones
	Punto único de fallas	Fallas del equipo de telecomunicaciones
	Ausencia de identificación y autentificación de emisor y receptor	Falsificación de derechos
	Arquitectura insegura de la red	Espionaje remoto
	Transferencia de contraseñas en claro	Espionaje remoto
	Gestión inadecuada de la red (tolerancia a fallas en el enrutamiento)	Saturación del sistema de información
	Conexiones de red pública sin protección	Uso no autorizado del equipo
RECURSO HUMANOS	Ausencia del personal	Incumplimiento en la disponibilidad del personal
	Procedimientos inadecuados de contratación	Destrucción de equipos y medios

Tipo de activo	Ejemplos de vulnerabilidades	Ejemplos de amenazas
	Entrenamiento insuficiente en seguridad	Error en el uso
	Uso incorrecto de software y hardware	Error en el uso
	Falta de conciencia acerca de la seguridad	Error en el uso
	Ausencia de mecanismos de monitoreo	Procesamiento ilegal de los datos
	Trabajo no supervisado del personal externo o de limpieza	Hurto de medios o documentos.
	Ausencia de políticas para el uso correcto de los medios de telecomunicaciones y mensajería	Uso no autorizado del equipo
INSTALACIONES	Uso inadecuado o descuidado del control de acceso físico a las edificaciones y los recintos	Hurto de medios o documentos
	Ubicación en área susceptible de inundación	Destrucción de equipos o medios

	Red energética inestable	Falla en equipo de telecomunicaciones
	Ausencia de protección física de la edificación (Puertas y ventanas)	Hurto de medios o documentos
SERVICIOS	Ausencia de procedimiento formal para el registro y retiro de usuarios	Abuso de los derechos
	Ausencia de proceso formal para la revisión de los derechos de acceso	Abuso de los derechos
	Ausencia de disposición en los contratos con clientes o terceras partes (con respecto a la seguridad)	Abuso de los derechos
	Ausencia de procedimientos de monitoreo de los recursos de procesamiento de la información	Abuso de los derechos
	Ausencia de auditorias	Abuso de los derechos
	Ausencia de procedimientos de identificación y valoración de riesgos	Abuso de los derechos

Tipo de activo	Ejemplos de vulnerabilidades	Ejemplos de amenazas
	Ausencia de reportes de fallas en los registros de administradores y operadores	Abuso de los derechos
	Respuesta inadecuada de mantenimiento del servicio	Incumplimiento en el mantenimiento del sistema de información
	Ausencia de acuerdos de nivel de servicio o insuficiencia de estos	Incumplimiento en el mantenimiento del sistema de información
	Ausencia de procedimientos de control de cambios	Incumplimiento en el mantenimiento del sistema de información

	Ausencia de procedimiento formal para la documentación del MSPI	Corrupción de datos
	Ausencia de procedimiento formal para la supervisión del registro del MSPI	Corrupción de datos
	Ausencia de procedimiento formal para la autorización de la información disponible al publico	Datos provenientes de fuentes no confiables
	Ausencia de asignación adecuada de responsabilidades en seguridad de la información	Negación de acciones
	Ausencia de planes de continuidad	Falla del equipo
	Ausencia de políticas sobre el uso de correo electrónico	Error en el uso
	Ausencia de procedimientos para introducción del software en los sistemas operativos	Error en el uso
	Ausencia de registros en bitácoras	Error en el uso
	Ausencia de procedimientos para el manejo de información clasificada	Error en el uso
	Ausencia de responsabilidad en seguridad de la información en la descripción de los cargos	Error en el uso

Tipo de activo	Ejemplos de vulnerabilidades	Ejemplos de amenazas
	Ausencia de los procesos disciplinarios definidos en caso de incidentes de seguridad de la información	Hurto de equipo
	Ausencia de política formal sobre la utilización de computadores portátiles	Hurto de equipo
	Ausencia de control de los activos que se encuentran fuera de las instalaciones	Hurto de equipo
	Ausencia de política sobre limpieza de escritorio y pantalla	Hurto de medios o documentos
	Ausencia de autorización de los recursos de procesamiento de información	Hurto de medios o documentos
	Ausencia de mecanismos de monitoreo establecidos para las brechas en seguridad	Hurto de medios o documentos
	Ausencia de revisiones regulares por parte de la gerencia	Uso no autorizado de equipo
	Ausencia de procedimientos para la presentación de informes sobre las debilidades en la seguridad	Uso no autorizado de equipo
	Ausencia de procedimientos del cumplimiento de las disposiciones con los derechos intelectuales.	Uso de software falsificado o copiado

Tabla 5 Tabla de Amenazas y Vulnerabilidades

Fuente: Ministerio de Tecnologías de la Información y las Comunicaciones

c) Descripción de los riesgos de seguridad de la información:

Para cada tipo de activo o grupo de activos pueden existir una serie de riesgos, los cuales la entidad pública debe identificar, valorar y posteriormente tratar si el nivel de dicho riesgo lo amerita.

Adicionalmente, se debe identificar el dueño del riesgo, es decir, "quien tiene que rendir cuentas sobre el riesgo o quien tiene la autoridad para gestionar el riesgo"[13].

La identificación de riesgos, amenazas y vulnerabilidades puede ser realizada a través de diferentes metodologías. Como ejemplo, se citan las siguientes:

- **Lluvia de ideas:** mediante esta opción se busca animar a los participantes a que indiquen qué situaciones adversas asociadas al manejo de la información digital y los activos de información se pueden presentar o casos ocurridos que los participantes conozcan que se hayan dado en la entidad pública o en el sector. Deben existir un orden de la sesión, un líder y personas que ayuden con la captura de las memorias.

- **Juicio de expertos:** a través de este esquema se reúnen las personas con mayor conocimiento sobre la materia de análisis e indican cuáles aspectos negativos o riesgos de seguridad de la información se pueden presentar. Para emplear esta técnica, se requiere disponer de una agenda con un orden de temas, establecer reglas claras y contar con la participación de un orientador o moderador, así como personas que tomen notas de los principales conceptos expuestos. Al finalizar, se retoman los principales riesgos identificados y se procede a hacer una valoración.

- **Análisis de escenarios**: en este esquema también se busca que un grupo de personas asociadas al proceso determinen situaciones potenciales que pueden llegar a presentarse: explosión de un pozo, sobrecarga de un nodo, pérdida de control de una unidad operada remotamente; y con base en estas posibilidades, se determina qué puede llegar a suceder, desde la perspectiva digital, a los activos de información y las consecuencias de la afectación.

- **Otras técnicas que pueden ser empleadas** son: entrevistas estructuradas, encuestas o listas de chequeo.

Posterior a la identificación de los riesgos de seguridad de la información con sus respectivas amenazas y vulnerabilidades enunciadas en este documento, se deberá continuar con el Paso de Valoración del Riesgo, de la "Guía para la Administración del Riesgo y el diseño de controles en entidades públicas" del DAFP.

2 Identificación del nivel de confianza para la autenticación digital

Se deben identificar aquellos trámites y servicios ciudadanos digitales que deben contar con autenticación digital de acuerdo con lo señalado en la guía de lineamientos para los Servicios Ciudadanos Digitales, en la que se establece que inicialmente, para el acceso al servicio de Autenticación Digital, las entidades deben identificar y determinar el grado de confianza requerido para los procesos relacionados con el trámite acorde con la siguiente clasificación:

- Bajo: Ofrece un nivel de confianza mínimo en el proceso de Autenticación Digital. Se emplea cuando el riesgo que conlleva una autentificación errónea es mínimo.

- Medio: Ofrece cierto nivel de confianza en el proceso de Autenticación Digital. Se emplea cuando el riesgo que conlleva una autentificación errónea es moderado.

- Alto: Ofrece una gran confianza en el proceso de Autenticación Digital. Se emplea cuando el riesgo que conlleva una autentificación errónea implica un riesgo alto.

- Muy alto: Ofrece más confianza en el proceso de Autenticación Digital. Se emplea cuando el riesgo que conlleva una autentificación errónea implica un riesgo extremo.

Para la definición del nivel de confianza y establecer el nivel de garantía requerido para el sistema de información asociado al trámite que usará el servicio de Autenticación Digital, se debe realizar el proceso para la valoración de riesgos de Seguridad de la información, señalado en la Guía para la administración de riesgos y diseño de controles de la Función Pública, en el capítulo 5. Lineamientos riesgos de seguridad de la información y lo establecido en el catálogo y metodología de Infraestructuras Criticas Cibernéticas del Ministerio de Tecnologías de la Información y las Comunicaciones.

En este sentido, es necesario identificar dentro del inventario de activos de información aquellos activos de tipo software que requieren autenticación digital, especialmente si los trámites o servicios digitales asociados solo pueden ser realizados por el titular de la información. En estos casos, debe establecerse un control de autenticación digital adecuado, cuyo nivel se determinará a partir del análisis del impacto por pérdida de confidencialidad, integridad y disponibilidad. Este análisis debe considerar la vulnerabilidad asociada a la ausencia de mecanismos de identificación y autenticación (como el inicio de sesión de usuario), así como la amenaza de falsificación de derechos sobre dichos activos de software.

Posteriormente, se debe realizar el análisis de probabilidad e impacto de materialización de los riesgos identificados, con el fin de determinar su nivel conforme a la Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas (niveles: extremo, alto, moderado o bajo). A partir de este resultado, se establecerá el grado de confianza requerido para la autenticación digital (muy alto, alto, medio o bajo). Una vez definido el nivel de confianza, se deben aplicar los lineamientos de la Guía para la Vinculación y Uso de los Servicios Ciudadanos Digitales, con el fin de adelantar el proceso de vinculación al servicio de autenticación digital.

3. Valoración del riesgo

Para realizar la valoración de los riesgos de seguridad de la información se debe llevar a cabo: el análisis de riesgo, la evaluación del riesgo, las estrategias para combatir el riesgo, las herramientas para la gestión del riesgo y finalmente el monitoreo y revisión tal como se establece en la "Guía para la administración del riesgo y el diseño de controles en entidades públicas" del Departamento Administrativo de la función Pública (DAFP).

4. Identificación y evaluación de los controles existentes

Como lo indica la Guía de DAFP, arriba mencionada, una vez establecidos y valorados los riesgos inherentes se procede a la identificación y evaluación de los controles existentes para evitar trabajo o costos innecesarios.

Nota: Para determinar si existen uno o varios controles asociados a los riesgos inherentes identificados se puede consultar la sección **4. OBJETIVOS DE CONTROL Y CONTROLES DE REFERENCIA** (*Tomados del Anexo A de la Norma ISO/IEC 27001:2022* como un insumo base y determinar si ya posee alguno de los controles orientados a seguridad de la información que están enunciados en dicho anexo.

5. Tratamiento de los riesgos de seguridad de la información

Una vez se han identificado los riesgos, la entidad pública debe definir el tratamiento para cada uno de los riesgos analizados y evaluados, conforme a los criterios y al apetito de riesgo definidos previamente en la Política de Administración de Riesgos Institucional.

El tratamiento de los riesgos es un proceso cíclico, el cual involucra una selección de opciones para modificarlos, por lo tanto, la entidad pública puede tener en cuenta las opciones planteadas en la "Guía para la administración del riesgo y el diseño de controles en entidades públicas" del DAFP: **aceptar, reducir, evitar, compartir el riesgo.**

Importante:

Si la entidad pública decide **mitigar o tratar el riesgo** mediante la selección de controles que permitan disminuir la probabilidad o el impacto del riesgo, deberá tener en cuenta la **Sección 4. OBJETIVOS DE CONTROL Y CONTROLES DE REFERENCIA**, basados en la norma ISO/IEC 27001:2022 en su Anexo A, como un insumo base para mitigar los riesgos de seguridad de la información, sin embargo, la entidad pública puede implementar nuevos controles de seguridad que no estén incluidos dentro del Anexo, siempre y cuando sean efectivos y eficaces para disminuir la probabilidad o el impacto del riesgo.

6. Planes de Tratamiento de Riesgos de Seguridad de la información e Indicadores para la

Los planes de tratamiento de riesgos y los indicadores para medir la eficacia o la efectividad se deberán generar como lo indica el **Esquema 9. Consolidación de los Planes de Tratamiento de Riesgos,** de la *"Guía para la Administración del Riesgo en la Gestión, Corrupción y Seguridad de la información. Diseño de Controles en Entidades Públicas Versión 4 - 2018 "* emitida por el DAFP.

Nota: Tenga en cuenta para el diseño de controles, los parámetros señalados en la versión 4 de la Guía para la administración del riesgo y el diseño de controles en entidades públicas, de 2018, continúan vigentes, por lo tanto, se sugiere remitirse a dicho documento.

Fase 2. Ejecución

Esta fase se centra en la implementación de los planes de tratamiento de riesgos definidos en la fase anterior, en esencia es seguir la ruta crítica definida y llevar a cabo todo lo planeado en la Fase 1.

Aquí la Línea Estratégica debe cumplir con el compromiso de brindar los recursos necesarios para iniciar el tratamiento de los riesgos.

El responsable de seguridad digital deberá supervisar y acompañar el proceso de implementación de los planes de tratamiento, verificando que los responsables de los planes (Primer Línea de Defensa y la Oficina de Tecnologías de la Información -TI- generalmente) ejecuten las tareas en los tiempos pactados y que los recursos se estén ejecutando de acuerdo con lo planeado.

11.2 Fase 3. Monitoreo y revisión

La entidad pública a través de las Tres Líneas de defensa definidas en el MIPG en la Dimensión 7 Control Interno, Componente Actividades de control, debe hacer un seguimiento a los planes de tratamiento para determinar su efectividad, de acuerdo con lo definido a continuación:

- Realizar seguimiento y monitoreo al plan de acción en la etapa de implementación y finalización de los planes de acción.

- Revisar periódicamente las actividades de control para determinar su relevancia y actualizarlas de ser necesario.

- Realizar monitoreo de los riesgos y controles tecnológicos que contemple alertas y vulnerabilidades genéricas que puedan generar eventos o incidentes que posteriormente implique una materialización de riesgo.

- Efectuar la evaluación del plan de acción y realizar nuevamente la valoración de los riesgos de seguridad de la información para verificar su efectividad.

- Verificar que los controles están diseñados e implementados de manera efectiva y operen como se pretende para controlar los riesgos.

- Suministrar recomendaciones para mejorar la eficiencia y eficacia de los controles.

Nota 1: Una vez que el plan de tratamiento se haya ejecutado en las fechas y con las disposiciones de recursos previstas, la entidad pública debe valorar nuevamente el riesgo y verificar si el nivel disminuyó o no (es decir, si se desplazó de una zona mayor a una menor en el mapa de calor) y luego, compararlo con el ultimo nivel de riesgo residual.

En esta fase se deben evaluar periódicamente los riesgos residuales para determinar la efectividad de los planes de tratamiento y de los controles propuestos, de acuerdo con lo definido en la Política de Administración de Riesgos de la entidad pública. Así mismo, también deberán tenerse en cuenta los incidentes de seguridad de la información que hayan afectado a la entidad y también las métricas o indicadores definidos para hacer seguimiento a las medidas de seguridad implementadas. Todo lo anterior contribuye a la toma de decisiones en el proceso de revisión de riesgo por parte de la línea estratégica (Alta dirección y Comité Institucional de Coordinación de Control Interno) y las partes interesadas.

Nota 2: De conformidad con la implementación del presente lineamiento es importante tener en cuenta que, una vez se publique la metodología para la identificación de infraestructuras criticas cibernéticas establecida en el Decreto 338 de 2022, se actualizarán los lineamientos generados en el presente documento para realizar la identificación y evaluación mediante una nueva metodología de riesgos, la cual será de obligatorio cumplimiento para entidades del sector público.

a) Registro y reporte de incidentes de seguridad de la información

Es importante que la entidad pública cuente con el registro de los incidentes de seguridad de la información que se hayan materializado, con el fin de analizar las causas, las deficiencias de los controles implementados y las pérdidas que se pueden generar.

El propósito fundamental del registro de incidentes es garantizar que se tomen las acciones adecuadas para evitar o disminuir su ocurrencia, retroalimentar y fortalecer la identificación y gestión de dichos riesgos y enriquecer las estadísticas sobre amenazas y vulnerabilidades y, con esta información, adoptar nuevos controles.

Nota: El reporte de incidentes de seguridad de la información a terceros (entes de control, reguladores, superintendencias, instancias o autoridades en la materia, entre

otros), no es la misionalidad del presente documento, sin embargo, se recomienda realizar dichos reportes conforme lo estipulan los entes o las buenas prácticas en seguridad de la información.

1. Reporte de la gestión del riesgo de seguridad de la información al interior de la entidad pública.

El responsable de seguridad digital debería reportar periódicamente a la Línea Estratégica (Alta dirección y Comité Institucional de Coordinación de Control Interno) y a las partes interesadas la siguiente información:

REPO
1. Matriz de los riesgos identificados de seguridad de la información. 2. Listado de activos críticos TI/TO y listado de ICC. 3. Reporte de criticidad/impacto de la organización. 4. Plan de tratamiento de riesgos. 5. Reporte de evolución de riesgos y modificación del riesgo

PERIODI
> Periódicamente por parte de todas las Entidades u organizaciones que han adoptado el modelo respectivo. > Cuando ocurra un cambio organizacional o de procesos de la organización que genere un impacto en las operaciones o que pueda afectar los riesgos ya identificados anteriormente. En este caso debe realizarse una nueva evaluación de

Ilustración 2 Reportes de información por parte de la entidad.

Fuente: Ministerio de Tecnologías de la Información y las Comunicaciones

2. Reporte de la gestión del riesgo de seguridad de la información a autoridades o entidades especiales

Una vez la entidad pública obtenga los resultados de la gestión de riesgos de seguridad de la información, se debería consolidar información (previamente obtenida con la aplicación del modelo) con el fin de reportarla a futuro a las autoridades o instancias encargadas del tema y que el Gobierno defina.

La finalidad del reporte de esta información es que el Gobierno Nacional pueda identificar posibles oportunidades para la generación de política pública, generación de capacidades o asignación de recursos que permita ayudar a la mejora de la seguridad de la información.

Información por consolidar para generar el reporte de información:

Se propone que las entidades públicas consoliden la siguiente información puntual para poder llevar a cabo el reporte respectivo:

- Riesgos con nivel crítico.
- Amenazas críticas.
- Vulnerabilidades críticas.
- Tipos de Activos afectados por los riesgos críticos (incluyendo servicios digitales o que delimitan con internet).
- Planes de tratamiento propuestos para la mitigación y si han sido ejecutados.
- Servicios digitales críticos en la entidad pública (Servicios o trámites para los ciudadanos o sistemas de información críticos para la entidad).

Esta información tiene por objetivo permitir la construcción de un panorama de riesgos de seguridad de la información de todo el país, para poder tomar decisiones estratégicas para la construcción de política pública, generación de capacidades o planes de acción con base a la información que pueda analizarse.

Reportes relacionados con Infraestructuras Críticas Cibernéticas, cuando aplique:

Las infraestructuras críticas cibernéticas -ICC- que hayan sido identificadas deberían reportarse a las autoridades o instancias encargadas del tema en el Gobierno nacional.

Nota: Es importante indicar que los reportes de riesgos de seguridad de la información a las entidades de gobierno no implicarían o significarían el traslado de la responsabilidad sobre los riesgos o su tratamiento.

3. Auditorías internas y externas

Le corresponde a las Unidades de Control Interno (tercera línea de defensa), realizar evaluación (aseguramiento) independiente sobre la gestión del riesgo de seguridad de la información en la entidad pública, catalogándola como una unidad auditable más dentro de su Universo de Auditoría, conforme al Plan Anual de Auditoría aprobado por el Comité Institucional de Coordinación de Control Interno de la entidad.

4. Medición del desempeño

La entidad pública debe utilizar medidas de desempeño (indicadores[14]) para la gestión de los riesgos de seguridad de la información, las cuales deben reflejar el

14 Consultar en la *Guía de Administración del Riesgo de Gestión, Corrupción y Seguridad de la información* del DAFP – Sección Indicadores - Gestión del Riesgo de Seguridad de la información, para definir indicadores de seguimiento para la gestión del riesgo de seguridad de la información y cumplimiento de los objetivos propuestos. Estas deben ser evaluadas periódicamente alineadas con la revisión por la línea estratégica.

11.3 Fase 4. Mejoramiento continuo de la gestión del riesgo de seguridad de la información

La entidad pública debe garantizar la mejora continua de la gestión de riesgos de seguridad de la información, por lo tanto, debe establecer que cuando existan

hallazgos, falencias o incidentes de seguridad de la información se debe mitigar el impacto de su existencia y tomar acciones para controlarlos y prevenirlos. Adicionalmente, se debe establecer y hacer frente a las consecuencias propias de la no conformidad que llegó a materializarse.

Deben definirse las acciones para mejorar continuamente la gestión de riesgos de seguridad de la información de la siguiente forma:

- Revisar y evaluar los hallazgos encontrados en las auditorías internas, otras auditorías e informes de los entes de control realizadas.

- Establecer las posibles causas y consecuencias del hallazgo.

- Determinar si existen otros hallazgos similares para establecer acciones correctivas y evitar así que se lleguen a materializar.

- Emprender acciones de revisión continua, que permitan gestionar el riesgo a tiempo, disminuir el impacto y la probabilidad de ocurrencia del riesgo detectado, así como la aparición de nuevos riesgos que puedan afectar el desempeño de la entidad pública o de los servicios que presta al ciudadano.

Adicionalmente, se sugiere llevar un registro documentado del tratamiento realizado al hallazgo, así como las acciones realizadas para mitigar el impacto y ver el resultado para futuros hallazgos.

12 Controles de Referencia Para La Mitigación De Los Riesgos De Seguridad

Las entidades públicas podrán mitigar/tratar los riesgos de seguridad de la información empleando los controles, del numeral 11.1 Controles y objetivos de control, del documento maestro del Modelo de Seguridad y Privacidad de la Información – MSPI.

MARIO ALEJANDRO CADAVID CADAVID
Gerente

CÓDIGO DEL DOCUMENTO: MA-GIF-02	**VERSIÓN:** 2016 – 02	**PREPARADO POR:** Oficina de Control Interno.
APROBADO POR: Gerente Empresa Social del Estado.	**FECHA:** Enero 28 de 2026	**FIRMA:**