2021

GUÍA METODOLÓGICA PARA LA GESTIÓN DE RIESGOS DE SEGURIDAD DIGITAL

Nerthink Mauricio Aguilar Hurtado

Gobernador de Santander

Ricardo Flórez Rueda

Secretario de TIC

METODOLOGÍA PARA LA GESTIÓN DE RIESGOS DE SEGURIDAD DIGITAL

Nerthink Mauricio Aguilar Hurtado

Gobernador de Santander

Ricardo Flórez Rueda

Secretario de TIC

Bucaramanga, Mayo de 2021

Tabla de contenido

Lista de Tablas

1. Introducción

La gestión de riesgos de seguridad digital (en adelante GRSD) permite identificar, comprender, evaluar y mitigar los riesgos, sus vulnerabilidades y el impacto en los activos de información de la Entidad; la GRSD permite la toma de decisiones al interior de la Entidad basada en información confiable y veraz, dando eficiencia en el uso de recursos y las prioridades necesarias para aplicar la gestión óptima de los riesgos digitales en relación a las necesidades de negocio.

La GRSD en la Gobernación de Santander establece procesos, procedimientos y actividades encaminados a lograr un equilibrio entre la operación y los riesgos que se generan asociados a los activos de información que apoyan y soportan la misión y visión de la Entidad.

La presente metodología inicia con el establecimiento del contexto acerca de la entidad, el cual es necesario para la GRSD, dando cubrimiento a los procesos estratégicos, misionales, de control y seguimiento, y de apoyo, pasando por la identificación de los activos de información, su valoración y la definición de amenazas y vulnerabilidades, obteniendo así los riesgos inherentes que afectan a dichos activos; concluyendo con su valoración, análisis y monitoreo desde el punto de vista de un proceso de mejora continua, en el cual se presenta un ciclo iterativo para la GRSD.

En Colombia, se cuenta con una cifra de más de treinta millones de conexiones a internet de banda ancha[1], lo que evidencia un aumento considerable en la economía digital del país. Así mismo, conscientes de que la seguridad digital es fundamental para el desarrollo del país, en los últimos años se ha puesto a la vanguardia la lucha contra las amenazas en el ámbito digital con estrategias tales como: la creación de lineamientos como la Política para Ciberseguridad y Ciberdefensa (CONPES 3701 y 3854), un modelo de seguridad y privacidad de la información (MSPI) y misiones de asistencia técnica internacional. Igualmente, el apoyo de diferentes organizaciones para la prevención y gestión de incidentes (MinTIC, Grupo de Respuestas a Emergencias Cibernéticas de Colombia ColCERT, Equipo de respuesta a incidentes de seguridad informática CSIRT (Centro Cibernético Policial de la Policía Nacional), los mecanismos de investigación (Fiscalía General de la Nación, Centro Cibernético Policial) y de judicialización (rama judicial). Con el conjunto de estas organizaciones se busca aumentar la capacidad de defensa ante las amenazas presentes en el medio digital.[2]

2. Objetivo General

Definir las acciones y métodos a seguir para tratar la GRSD de manera integral, identificando las necesidades de la entidad con respecto a los requisitos para la protección de la confidencialidad, integridad y disponibilidad de sus activos de información y apoyar la implementación del MSPI.

3. Objetivos Específicos

[1] MinTIC en los medios, tomado de: https://www.mintic.gov.co/portal/inicio/Sala-de-prensa/MinTIC-en-los-medios/72963:Colombia-supera-los-30-millones-de-conexiones-a-internet-de-banda-ancha

[2] República de Colombia. Modelo Nacional de Gestión de riesgos de seguridad digital, tomado de: https://www.funcionpublica.gov.co/eva/admon/files/empresas/ZW1wcmVzYV83Ng==/imagenes/4495/articles-61854_documento.docx

✓ Proveer lineamientos y guía metodológica a todos los procesos de la Gobernación de Santander para la adecuada GRSD.
✓ Contribuir al fortalecimiento y apropiación de conocimiento sobre la gestión de riesgos, Seguridad y Privacidad de la información, Seguridad Digital y Continuidad de la Operación en la Entidad.
✓ Alinear la GRSD con la política de administración de riesgo de la Gobernación de Santander y con las buenas prácticas a nivel mundial (NTC ISO/IEC 27001 e ISO 27005 vigente).
✓ Cumplir con los requisitos legales y reglamentarios en gestión de riesgos de seguridad digital pertinentes a la legislación colombiana.

4. Alcance

La presente metodología es aplicable a todos los procesos y sus áreas que conforman el sistema integrado de gestión de la Gobernación de Santander y a todas las actividades realizadas por todo el personal que labora en la Entidad; funcionarios, contratistas, practicantes, proveedores y terceros que accedan a las instalaciones, información y sistemas informáticos, durante el ejercicio de sus funciones contemplando riesgos de seguridad digital y privacidad de la información.

5. Glosario

Activo: [Según ISO 27000]: En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de la misma (sistemas, soportes, edificios, personas...) que tenga valor para la organización.
Activo de información: Es la información que, por su importancia para las actividades de la Gobernación de Santander, es reconocida como un bien que tiene un valor significativo para la Entidad. En el contexto de la norma ISO/IEC 27001 son: "Conocimientos, datos o información que una organización o entidad valora y por lo tanto debe proteger", esta puede existir de forma física (archivos impresos, libros, Cd's, etc) o lógica (Bases de datos, archivos en Word, Excel Pdf, fotografías, videos, etc).
Amenaza: [Según ISO 27000]: Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización.
Base de datos: Aplicación utilizada para la almacenar gran cantidad de datos, relacionados y estructurados, que pueden ser consultados rápidamente de acuerdo con las características selectivas que se deseen.
Confidencialidad: Propiedad que determina que la información sólo esté disponible y sea revelada a individuos, entidades o procesos autorizados.
Control Automático: un control es automático cuando las actividades de ejecución del mismo se ejecutan por un sistema y/o aplicativo de manera automática, sin interacción humana.
Control Correctivo: Se caracterizan por la toma de acciones para revertir eventos no deseados, por ejemplo, la utilización de un antivirus.

Control Detectivo: Son acciones que buscan identificar eventos en el momento que se presentan, por ejemplo, una auditoria se considera un control detectivo.

Control Manual: un control es manual cuando para su ejecución se incluyen actividades para mitigar el riesgo que son realizadas por una persona, lo cual podría tener implícito el error humano

Control Preventivo: Son controles que buscan anticipar eventos no deseados antes de que sucedan, por ejemplo, el control de acceso a instalaciones físicas, la revisión de maletines.

Custodio del activo de información: Es la parte encargada de administrar y hacer efectivos los controles de seguridad que el dueño o propietario del activo de la información haya definido, por ejemplo, realizar las copias de respaldo o Backpus, la asignación privilegios de acceso, modificación y borrado, la identificación de posibles incidentes relacionados con el activo, etc.

Disponibilidad: Propiedad de que la información sea accesible y utilizable por solicitud de una Entidad autorizada, cuando ésta así lo requiera.

Dueño o propietario del activo de información: Es la persona o cargo responsable por el activo de información, es quien tiene la facultad de definir como se clasifica dicho activo, la criticidad del mismo para la Entidad y los derechos de acceso que pueden tener al activo de información los usuarios.

Integridad: Propiedad de salvaguardar la exactitud y estado completo de los activos

ISO 27001:2013: norma internacional que permite el aseguramiento, la confidencialidad e integridad de los datos y de la información, así como de los sistemas que la procesan.

ISO 27005: Estándar internacional que se ocupa de la gestión de los riesgos relativos a la seguridad de información.

Ley 1581 de 2012: Ley de tratamiento de datos personales efectuado en territorio colombiano

Ley 1712 de 2014: Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional

Modelo de Seguridad y Privacidad de la información (MSPI): Documento del MINTIC con los lineamientos de buenas prácticas en Seguridad y Privacidad para las entidades del Estado.

Política: para la gestión del riesgo [Según NTC ISO 31000:2011]: Declaración de la dirección y las intenciones generales de una organización con respecto a la gestión del riesgo. [Según ISO/IEC 27000:2016]: Intenciones y dirección de una organización como las expresa formalmente su alta dirección.

Riesgo: [Según ISO 27000]: Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias.

Usuarios: Se entiende por usuarios, a cualquier persona entidad, cargo, proceso, sistema automatizado o grupo de trabajo que acceda a los activos de información de la Gobernación de Santander, para generar, obtener, transformar, conservar o utilizar información de la Entidad en papel o en medio digital, esto incluye: funcionarios de carrera administrativa y de libre nombramiento, temporales, practicantes, contratistas, recurso humano de empresas proveedoras de servicio y aplicaciones que consuman servicios o información de la entidad.

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

6. Política de gestión de riesgos de Seguridad Digital

La Gobernación de Santander, entendiendo la importancia de una adecuada GRSD, se compromete en disminuir y gestionar adecuadamente el riesgo de seguridad digital sobre sus activos de información, protegiendo la confidencialidad, integridad y disponibilidad de cada uno de ellos.

Lo anterior está determinado a través de:

- ✓ La protección de los activos de información.
- ✓ La mitigación de los riesgos de seguridad digital en las funciones más importantes de la Gobernación de Santander.
- ✓ La protección de los principios de seguridad de la información (confidencialidad, integridad y disponibilidad).
- ✓ La confianza de los grupos de valor al interior y al exterior de la entidad.

7. Metodología para la gestión de riesgos de seguridad digital

El proceso de GRSD consta de la definición del enfoque organizacional para la valoración del riesgo y su posterior tratamiento, a continuación, se detalla cada uno de los componentes de la GRSD:

7.1. Definición del contexto de seguridad digital

El contexto en seguridad digital parte del análisis de los objetivos estratégicos y metas de la entidad, en este caso la Gobernación de Santander; busca lograr identificar los riesgos de seguridad digital presentes en cada una de las actividades de la Entidad y establecer controles que permitan la mitigación del impacto o la reducción de su probabilidad.

La GRSD se desarrolla dentro del contexto interno y externo determinado en la política de administración del riesgo de la Gobernación de Santander, el contexto de seguridad digital contempla como factores principales:

7.1.1. Contexto Interno

En el contexto interno se determina y recolectan las características o aspectos del ambiente, tales como son: su estructura organizacional, funciones y responsabilidades, políticas, objetivos, estrategias implementadas, recursos (económicos, personas, procesos, sistemas, tecnología e información), relaciones con las partes involucradas y cultura organizacional para determinar en ellos, circunstancias que puedan afectar la seguridad digital y que sean factores de riesgo inherente para la institución, como lo son:

- ✓ Direccionamiento estratégico y planeación institucional.
- ✓ Caracterización del proceso, objetivos, alcance y actividades.

- ✓ Disponibilidad de Capital, Liquidez, Mercados Financieros, Desempleo, Competencia.
- ✓ Competencias y disponibilidad del personal.
- ✓ Demografía, Responsabilidad Social y Orden Público.
- ✓ Avances en tecnología, acceso a sistemas de información externos y Gobierno Digital.
- ✓ Flujos de transferencia de información interna.
- ✓ Estructura organizacional.
- ✓ Vulnerabilidades y debilidades conocidas en los sistemas de información e infraestructura tecnológica.
- ✓ Roles y responsabilidades en la seguridad digital al interior de los procesos y en toda la Gobernación de Santander.
- ✓ Habilidades técnicas en el manejo, uso y protección de los activos de información al interior de la Gobernación de Santander.

7.1.2. Contexto externo

El contexto externo se determina a través de la identificación de factores que impactan la gestión de riesgos de seguridad digital:

- ✓ Cambios de gobierno, legislación, políticas públicas y regulación.
- ✓ Necesidades de la ciudadanía y los grupos de interés.
- ✓ Agentes de amenazas que buscan la explotación de vulnerabilidades.
- ✓ Normatividad vigente que rige el tratamiento de la información para las entidades públicas, en las que se incluyen, pero no se limitan:
- ✓ Ley 1437 de 2011, Capítulo IV.
- ✓ Ley 1581 de 2012.
- ✓ Ley 1712 de 2014.
- ✓ Decreto 2573 de 2014.
- ✓ Decreto 1413 de 2017.
- ✓ Aspectos externos que pueden verse afectados con los riesgos de seguridad digital, por ejemplo, el ambiente social, económico y de reputación de la Gobernación de Santander.

7.2. Definición del alcance de la gestión de riesgos de seguridad digital

La GRSD es responsabilidad de todos los servidores públicos y colaboradores de la Gobernación de Santander, así como, de todos los terceros que directa o indirectamente apoyan el cumplimiento de los objetivos de la Entidad.

La GRSD tiene alcance sobre todos los procesos estratégicos, misionales, de apoyo y de evaluación que conforman el Sistema Integrado de Gestión de la Gobernación de Santander y todas las actividades realizadas por los servidores públicos durante el ejercicio de sus funciones contemplando riesgos de seguridad digital y privacidad de la información.

7.3. Definición de roles y responsabilidades

Según los principios generales, la gestión de riesgo es una actividad transversal en toda la organización, cada una de las líneas de defensa en la Gobernación de Santander tiene responsabilidades y actividades a cargo alienadas a la adecuada gestión de riesgos; para consultar las responsabilidades remitirse al punto 9. RESPONSABILIDAD Y COMPROMISOS FRENTE A LA POLÍTICA DE ADMINISTRACIÓN DEL RIESGO[3] contenido en la política de administración de riesgo 2020.

7.4. Identificación de activos de información

Un activo de información en el contexto de la norma ISO/IEC 27001 son: "Conocimientos, datos o información que una organización o entidad valora y por lo tanto debe proteger".

Se considera un activo de información, todos los elementos tales como: aplicaciones informáticas, servicios web, redes, hardware, información física o digital, recurso humano (personas) que le permite a la Gobernación de Santander funcionar en un entorno digital.

Alineado a lo anterior, la Gobernación de Santander se compromete a proteger la confidencialidad, integridad y disponibilidad de todos sus activos de información; para esto, los responsables de los procesos (primera línea) deben identificar, documentar y valorar todos sus activos de información.

A continuación, se presenta el paso a paso para generar el inventario y valoración de los activos de información:

7.4.1. Paso 1. Listar los activos de información

En cada proceso, se debe listar todos los activos a su cargo, indicando un consecutivo, el nombre del activo y una descripción del mismo.

ID: Número consecutivo utilizado como identificador único para el activo.

Proceso: Nombre del proceso al que pertenece el activo.

Secretaría: Nombre de la Secretaría a la que pertenece el activo.

Oficina: Detalle de la dependencia especifica que utiliza el activo de información.

Activo: Nombre del activo de información identificado.

Descripción: Detalles breves y claros que permitan la plena identificación del activo de información

A continuación, un ejemplo de la identificación de un activo de información:

[3] Política de administración del riesgo 2020 Gobernación de Santander, ver: http://historico.santander.gov.co/intra/index.php/sig/finish/582-4-manuales-instructivos-guias-planes-programas-politicas-reglamentos/11446-politica-de-administracion-del-riesgo

ID	Proceso	Secretaría	Oficina	Activo	Descripción
TIC-SI-001	Tecnologías de la información y las comunicaciones.	Secretaría TIC	Dirección de Sistemas de información	Aplicativo ARANDA	Software utilizado para la gestión de servicios de soporte tecnológico al interior de la Gobernación de Santander
TIC-DE-002	Tecnologías de la información y las comunicaciones.	Secretaría TIC	Despacho	Plan estratégico de tecnologías de la información	Documento estratégico de TI que busca asegurar la alineación de TI con las metas y objetivos de la Gobernación de Santander

Tabla 1. Ejemplo de Identificación de un activo de información

7.4.2. Paso 2. Identificación del dueño de los activos de información

Cada uno de los activos de información identificados debe tener un dueño o propietario designado, en la Gobernación de Santander, cada uno de los responsables de los procesos serán los dueños de los activos de información a cargo de sus áreas.

Los activos de información deben tener un custodio asignado, dicho custodio puede ser un cargo, dueño de proceso, o grupo de trabajo que será el encargado de administrar y hacer efectivos los controles de seguridad digital que el propietario de la información haya definido, por ejemplo, copias de seguridad, asignación de privilegios de acceso, modificación y borrado.

A continuación, se describen los campos para la identificación de los dueños de los activos:

ID: Número consecutivo utilizado como identificador único para el activo.

Proceso: Nombre del proceso al que pertenece el activo.

Nombre del Activo: Nombre del activo de información identificado.

Descripción: Detalles breves y claro que permita la plena identificación del activo de información

Oficina: Detalle de la dependencia especifica que utiliza el activo de información.

Propietario: El propietario del activo de información, el cargo responsable de su gestión y protección al interior de la entidad.

Custodio: En caso de ser asignado, se debe detallar el custodio del activo de información, es quien hace efectivos los controles definidos para la protección de los activos de información, si no se asigna un custodio para el activo, se asume que el propietario realizará los dos roles.

Medio de conservación: indicar el medio en el cual se conserva la información o el activo de información, entre los medios de almacenamiento se mantienen:

- ✓ Documentos de Archivo (físicos y electrónicos).
- ✓ Archivos institucionales (físicos y electrónicos).
- ✓ Sistemas de Información Corporativos.
- ✓ Sistemas de Trabajo Colaborativo.
- ✓ Sistemas de Administración de Documentos.
- ✓ Sistemas de Mensajería Electrónica.
- ✓ Portales, Intranet y Extranet.
- ✓ Sistemas de Bases de Datos.
- ✓ Disco duros, servidores, discos o medios portables, cintas o medios de video y audio (análogo o digital), etc.
- ✓ Cintas y medios de soporte (back up o contingencia).
- ✓ Uso de tecnologías en la nube.
- ✓ N/A

Ubicación física o digital del archivo: Diligenciar donde se encuentra alojado el documento o activo de información, puede ser en medios físicos o en medios digitales.

A continuación, un ejemplo de la identificación del dueño y custodio del activo:

ID	Proceso	Activo	Descripción	Oficina	Propietario	Custodio	Medio de conservación	Ubicación física o digital del archivo
TIC-SI-001	Tecnologías de la información y las ...	Aplicativo ARANDA	Software utilizado para la gestión de servicios de soporte tecnológico al interior de la Gobernación de Santander	Sistemas de Información	Secretario de TIC	Dir sistemas de información	Sistemas de Información Corporativos	Digital
TIC-DE-002	Tecnologías de la información y las ...	Documento PETI	Documento estratégico de TI que busca asegurar la alineación de TI con las metas y objetivos de la Gobernación de Santander	Despacho - secretaria TIC	Secretario de TIC	Profesional Universitario / Despacho secretaria.	Uso de tecnologías en la nube	Digital

Tabla 2. Ejemplo de identificación del dueño del activo

7.4.3. Paso 3. Clasificar los tipos de 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.

A continuación, se describe la tipología utilizada para la clasificación de activos y su detalle:

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 de la Entidad, la reputación, entre otros.
Componentes de red	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.
Personas	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	Espacio o área asignada para alojar y salvaguardar los datos considerados como activos críticos para la empresa. Por ejemplo, DataCenter, centros de redes, Racks, cuartos de energía.

Tabla 3. Tipos de activos

Según lo anterior, se presenta un ejemplo de clasificación de activos:

ID	Proceso	Activo	Descripción	Tipo de Activo
TIC-SI-001	Tecnologías de la información y las comunicaciones.	Aplicativo ARANDA	Software utilizado para la gestión de servicios de soporte tecnológico al interior de la Gobernación de Santander	Software
TIC-DE-002	Tecnologías de la información y las comunicaciones.	Documento PETI	Documento estratégico de TI que busca asegurar la alineación de TI con las metas y objetivos de la Gobernación de Santander	Información

Tabla 4. Ejemplo de clasificación de activos según el tipo

7.4.4. Paso 4. Clasificar la información

Se debe realizar la clasificación de la información conforme lo indicado en las leyes 1712 de 2014 y 1581 de 2012, el Modelo de Seguridad y Privacidad de la información (MSPI) en su guía de gestión de activos, el dominio 8 del Anexo A de la norma ISO27001:2013 y demás normatividades aplicables.

La Ley 1712 de 2014 establece los siguientes niveles de clasificación de la información:

Información pública: Es toda información que un sujeto obligado genere, obtenga, adquiera o controle en su calidad de tal, es decir, es toda información que puede ser entregada o publicada sin restricciones a cualquier persona dentro y fuera de la entidad, sin que esto implique daños a terceros ni a las actividades o procesos de la entidad.

Información pública clasificada: Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, pertenece al ámbito propio, particular y privado o semiprivado de una persona natural o jurídica por lo que su acceso podrá ser negado o exceptuado, siempre que se trate de las circunstancias legítimas y necesarias y los derechos particulares o privados, es información disponible para todos los procesos de la entidad y que en caso de ser conocida por terceros sin autorización puede conllevar un impacto negativo para los procesos de la misma.

Esta información es propia de la entidad o de terceros y puede ser utilizada por todos los funcionarios de la entidad para realizar labores propias de los procesos, pero no puede ser conocida por terceros sin autorización del propietario.

Información pública reservada. Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, es exceptuada de acceso a la ciudadanía por daño a intereses públicos y bajo cumplimiento de la totalidad de los requisitos consagrados en el artículo 19 de la ley 1712 de 2014.

La información pública reservada, es toda información disponible sólo para un proceso de la entidad y que en caso de ser conocida por terceros sin autorización puede conllevar un impacto negativo de índole legal, operativa, de pérdida de imagen o económica.

Adicional a lo anterior, La Ley 1581 de 2012 define los principios y disposiciones aplicables al tratamiento de datos personales, por lo cual, se debe indicar si la información relacionada contiene o no este tipo de datos.

Entendiendo como dato personal "*datos 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."[4]

ID: número consecutivo utilizado como identificador único para el activo.

Proceso: Nombre del proceso al que pertenece el activo.

Activo: Nombre del activo de información identificado.

Descripción: Detalles breves y claros que permitan la plena identificación del activo de información

Confidencialidad (de acuerdo a clasificación ley 1712): la clasificación puede ser Información pública reservada, Información pública clasificada e Información pública.

Datos personales (de acuerdo a clasificación Ley 1581): se debe detallar sí la información contiene o no datos personales según lo definido en la ley 1581 de 2012.

A continuación, un ejemplo de la clasificación de la información:

ID	Proceso	Activo	Descripción	Confidencialidad (de acuerdo a clasificación Ley 1712)	Datos personales (de acuerdo a clasificación Ley 1581)
TIC-SI-001	Tecnologías de la información y las comunicaciones.	Aplicativo ARANDA	Software utilizado para la gestión de servicios de soporte tecnológico al interior de la Gobernación de Santander	N/A	N/A
TIC-DE-002	Tecnologías de la información y las comunicaciones.	Documento PETI	Documento estratégico de TI que busca asegurar la alineación de TI con las metas y objetivos de la Gobernación de Santander	Información pública clasificada	No contiene datos personales

Tabla 5. Ejemplo de clasificación de los activos según ley 1712 de 2014 y 1581 de 2012

7.4.5. Paso 5. Determinar la criticidad del activo

Para cada uno de los activos de información previamente identificados, es necesario evaluar su criticidad de acuerdo a la probable perdida de confidencialidad, integridad y disponibilidad, esta evaluación, debe permitir determinar el grado de importancia que tiene para el proceso cada uno de ellos, para posteriormente, durante el análisis de riesgos, tener presente dicha valoración con el fin de realizar una evaluación adecuada de cada caso.

[4] Definición de datos sensibles según la 1581 de 2012, tomado el 13 de abril de 2021 de: http://www.secretariasenado.gov.co/senado/basedoc/ley_1581_2012.html

7.4.5.1. Criticidad respecto a su confidencialidad

Como se realizó en el Paso 4. Clasificar la información, la confidencialidad se refiere a que la información no esté disponible ni sea revelada a individuos, entidades o procesos no autorizados, en la Gobernación de Santander, se han definido 3 niveles con los tipos de información declarados según la ley 1712 del 2014[5]:

Criticidad	Detalle
Información pública reservada	Información disponible sólo para un proceso de la entidad y que en caso de ser conocida por terceros sin autorización puede conllevar un impacto negativo de índole legal, operativo, de pérdida de imagen o económica
Información pública clasificada	Información disponible para todos los procesos de la Gobernación de Santander y que en caso de ser conocida por terceros sin autorización puede conllevar un impacto negativo para todos sus procesos. Esta información es propia de la Gobernación de Santander y puede ser utilizada por todos los funcionarios para realizar labores propias de los procesos, pero no puede ser conocida por terceros sin autorización del dueño del activo de información.
Información pública	Información que puede ser entregada o publicada sin restricciones a cualquier persona dentro y fuera de la entidad, sin que esto implique daños a terceros ni a las actividades y procesos de la entidad.

Tabla 6. Criticidad del activo de acuerdo a su confidencialidad

7.4.5.2. Criticidad respecto a completitud o integridad

La integridad se refiere a la exactitud y completitud de la información (ISO 27001) esta propiedad es la que permite que la información sea precisa, coherente y completa desde su creación hasta su destrucción. En la Gobernación de Santander, se utilizan los siguientes niveles para valorar los activos de información de acuerdo a su integridad:

Criticidad	Detalle
Alta	Información cuya pérdida de exactitud y completitud puede conllevar a la Gobernación de Santander un alto impacto de índole legal o económica, retrasar sus funciones, o generar pérdidas de imagen severas a la Gobernación de Santander.
Media	Información cuya pérdida de exactitud y completitud puede conllevar un impacto negativo de índole legal o económica, retrasar sus funciones, o generar pérdida de imagen moderado a funcionarios de la Gobernación de Santander.
Baja	Información cuya pérdida de exactitud y completitud conlleva un impacto no significativo para la Gobernación de Santander o entes externos.

Tabla 7. Criticidad del activo de acuerdo a su integridad

7.4.5.3. Criticidad respecto a su disponibilidad

La disponibilidad es la propiedad de la información que se refiere a que ésta debe ser accesible y utilizable por solicitud de una persona entidad o proceso autorizada cuando así lo requiera esta, en el momento y en la forma que se requiere ahora y en el futuro, al igual que los recursos necesarios para su uso. En la Gobernación de Santander se utilizan los siguientes niveles:

Criticidad	Detalle
Alta	La no disponibilidad de la información, puede conllevar un impacto negativo de índole legal o económica, retrasar sus funciones, o generar pérdidas de imagen severas a entes externos.

[5] Conceptos de la ley 1712 de 2014, art 6, tomado el 13 de abril de 2021 de: http://www.secretariasenado.gov.co/senado/basedoc/ley_1712_2014.html#6

Criticidad	Detalle
Media	La no disponibilidad de la información, puede conllevar un impacto negativo de índole legal o económica, retrasar sus funciones, o generar pérdida de imagen moderada de la Gobernación de Santander.
Baja	La no disponibilidad de la información, puede afectar la operación normal de la entidad o entes externos, pero no conlleva implicaciones legales, económicas o de pérdida de imagen.

Tabla 8. Criticidad del activo de acuerdo a su disponibilidad

Activo: Nombre del activo de información identificado.

Tipo de Activo: ver Tabla 3. Tipos de activos

Criticidad respecto a su confidencialidad: Ver Tabla 6. Criticidad del activo de acuerdo a su confidencialidad

Criticidad respecto a completitud o integridad: Ver Tabla 7. Criticidad del activo de acuerdo a su integridad

Criticidad respecto a su disponibilidad: Ver Tabla 8. Criticidad del activo de acuerdo a su disponibilidad

Nivel de criticidad del activo: Es un cálculo realizado automáticamente, este depende de los valores de la confidencialidad, integridad y disponibilidad descritos anteriormente. El resultado del cálculo igual o mayor a 7 indica un nivel alto de criticidad. Por otra parte, un resultado menor igual que 6 y mayor igual que 4 se obtiene un nivel medio de criticidad y un resultado menor a 4 nos arroja un nivel bajo.

A continuación, un ejemplo de determinación de la criticidad del activo:

Activo	Tipo de Activo	Criticidad respecto a su confidencialidad	Criticidad respecto a completitud o integridad	Criticidad respecto a su disponibilidad	Nivel de Criticidad del activo
Aplicativo ARANDA	Software	N/A	Alta	Alta	Alta
Documento PETI	Secretario de las TIC	Información pública clasificada	Media	Baja	Baja

Tabla 9. Ejemplo de determinación de criticidad de un activo

7.4.6. Paso 6. Identificar infraestructuras críticas cibernéticas

Un activo de información puede hacer parte de una infraestructura crítica cibernética, este se considera de tal forma si presenta algún tipo de impacto o afectación que pueda superar alguno de los siguientes 3 criterios:

Impacto social	Cuando su afectación (disponibilidad, integridad o confidencialidad) impacte al 0,5% de la población nacional, 250.000 personas
Impacto económico	Cuando su afectación (disponibilidad, integridad o confidencialidad) afecte al PIB de un día o 0.123% del PIB anual

Impacto ambiental	Cuando su afectación (disponibilidad, integridad o confidencialidad) afecte el medio ambiente y se requiera 3 años para su recuperación

Tabla 10. Criterios para identificar infraestructuras criticas cibernéticas

En caso de identificarse infraestructura crítica cibernética, es necesario complementar esta información con cada uno de los elementos tecnológicos que la componen, por ejemplo, servidores, dispositivos de red, sistemas especializados de control, etc.

Activo: nombre del activo de información identificado.

Tipo de Activo: ver Tabla 3. Tipos de activos.

Criterio de impacto social: definir si existe o no un impacto social de acuerdo a lo definido en Tabla 10. Criterios para identificar infraestructuras criticas cibernéticas

Criterio de impacto ambiental: definir si existe o no un impacto ambiental de acuerdo a lo definido en Tabla 10. Criterios para identificar infraestructuras criticas cibernéticas

Criterio de impacto económico: definir si existe o no un impacto económico de acuerdo a lo definido en Tabla 10. Criterios para identificar infraestructuras criticas cibernéticas

Ejemplo de identificación de infraestructura critica cibernética:

Activo	Tipo de Activo	Criterio de Impacto social (Si/No)	Criterio de Impacto económico (Si/No)	Criterio de Impacto ambiental (Si/No)	Elementos tecnológicos que lo componen
Aplicativo ARANDA	Software	No	No	No	N/A
Documento PETI	Información	No	No	No	N/A

Tabla 11. Ejemplo de identificación de infraestructura critica cibernética

7.4.7. Paso 7. Protección de datos personales

La Ley de Protección de Datos Personales reconoce y protege el derecho que tienen todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bases de datos o archivos que sean susceptibles de tratamiento por entidades de naturaleza pública o privada.

Cuando hablamos de datos personales nos referimos a toda aquella información asociada a una persona y que permite su identificación. Por ejemplo, su documento de identidad, el lugar de nacimiento, estado civil, edad, lugar de residencia, trayectoria académica, laboral, o profesional. Existe también información más sensible como su estado de salud, sus características físicas, ideología política, vida sexual, entre otros aspectos (SIC, s.f.).

Todo lo anterior se fundamenta en lo descrito en la Ley 1581 de 2012[6]

[6] ley 1581 de 2012, tomado el 13 de abril de 2021 de: http://www.secretariasenado.gov.co/senado/basedoc/ley_1581_2012.html

Contiene datos personales: ¿El activo de información contiene datos personales? SI - NO

Tipo de dato personal: Las disposiciones sobre protección de datos, establecen tipologías de datos según el mayor o menor grado de aceptabilidad de la divulgación:

✓ Dato Público: Es el dato que la ley o la Constitución Política determina como tal, así como todos aquellos que no sean semiprivados o privados.

✓ Dato Semiprivado: Es el dato que no tiene naturaleza íntima, reservada, ni pública y cuyo conocimiento o divulgación puede interesar no sólo a su titular sino a cierto sector o grupo de personas.

✓ Dato Privado: Es el dato que por su naturaleza íntima o reservada sólo es relevante para el titular de la información.

✓ Dato Sensible: Es el dato que afecta la intimidad del titular o cuyo uso indebido puede generar su discriminación.

Finalidad de recolección de los datos personales: La recolección de los datos personales puede tener cualquiera de las siguientes finalidades:

a) Permitir el desarrollo del objeto de la Gobernación de Santander.
b) Desarrollar los estudios previos y procesos de selección para la contratación oficial de la Gobernación de Santander destinada a garantizar el funcionamiento de la entidad y la ejecución de proyectos y el desarrollo de esquemas de gerencia de proyectos.
c) Realizar la selección, contratación y/o vinculación de servidores públicos y contratistas de prestación de servicios de la Gobernación de Santander.
d) Formular, ejecutar y evaluar los programas de salud ocupacional y planes de atención a emergencias.
e) Mantener actualizada la historia laboral y registros de nómina de funcionarios de la Gobernación de Santander.
f) Atender y resolver peticiones, quejas, reclamos y sugerencias.
g) Conservar evidencia de los eventos de entrenamiento y sensibilización realizados, audiencias de adjudicación de contratos, reuniones internas y externas.
h) Atender requerimientos de información de entes de control tanto internos como externos.
i) Efectuar la convocatoria y generar evidencia de la realización de sesiones de rendición de cuentas y participación ciudadana.
j) Medir y realizar seguimiento a los niveles de satisfacción de los usuarios de los servicios de la Gobernación de Santander, a través de encuestas.
k) Registrar y/o autorizar el ingreso a las instalaciones de las instalaciones físicas de la Gobernación de Santander o cualquier edificación que sea utilizada para cumplir la misión de la Gobernación de Santander.
l) Realizar análisis de seguridad para garantizar la protección de las personas y los bienes materiales que se encuentren en las instalaciones referidas en el literal k de este numeral.
m) No Aplica

Cuenta con la autorización de tratamiento de datos personales y transferencia internacional de datos: De acuerdo a la Ley 1581, la entidad debe procurar por obtener la autorización para uso y tratamiento de datos personales proveniente del propietario de los datos.

Existe transferencia internacional de los datos personales: Seleccionar si hay o no transferencia internacional de datos personales

7.4.8. Paso 8. Datos Abiertos

Los datos abiertos son información pública dispuesta en formatos que permiten su uso y reutilización bajo licencia abierta y sin restricciones legales para su aprovechamiento. En Colombia, la Ley 1712 de 2014 sobre Transparencia y Acceso a la Información Pública Nacional, define los datos abiertos en el numeral sexto como "todos aquellos datos primarios o sin procesar, que se encuentran en formatos estándar e interoperables que facilitan su acceso y reutilización, los cuales están bajo la custodia de las entidades públicas o privadas que cumplen con funciones públicas y que son puestos a disposición de cualquier ciudadano, de forma libre y sin restricciones, con el fin de que terceros puedan reutilizarlos y crear servicios derivados de los mismos". De este modo, la Ley establece la obligatoriedad de las entidades públicas de "divulgar datos abiertos", teniendo en cuenta las excepciones de acceso a la información, asociadas a información clasificada y reservada establecidas en su título tercero, artículos 18 y 191.

A continuación, se señalan algunos ejemplos de datos abiertos de entidades públicas disponibles en el Portal de Datos del Estado Colombiano:

✓ Los resultados de las elecciones dispuestos por la Registraduría Nacional del Estado Civil, con información detallada de las últimas jornadas electorales, tanto presidenciales, como territoriales y legislativas.
✓ Las contrataciones públicas dispuestas por la Agencia de Contratación – Colombia Compra Eficiente, donde se disponen todos los gastos en contratación que realiza el estado, permitiendo saber a quién le compra el Estado, cuanto gastó y en qué gasto.
✓ Los resultados sobre calidad educativa tales como las pruebas Saber dispuestas por el Instituto Colombiano para la Educación Superior – ICFES.
✓ Información de los códigos únicos de medicamentos para los registros sanitarios vigentes dispuestos por el Ministerio de Salud.

Los datos abiertos tienen como principal característica que están publicados en sitios web de manera gratuita, accesibles al público, dispuestos en formatos que permiten su uso, reutilización y aprovechamiento sin restricciones legales y bajo licencia abierta[7]

¿El activo de información es Estratégico? El área o dependencia considera que es un conjunto de datos que le interesa a la comunidad, o es consultado periódicamente para ser puesto en el portal de datos abiertos.

[7] Tomado el día 13 de abril de 2021 de: https://herramientas.datos.gov.co/sites/default/files/Guia%20de%20Datos%20Abiertos%20de%20Colombia.pdf

¿Es un Dato Abierto? Se encuentra publicado en el portal de datos abiertos o es susceptible de ser publicado en datos abiertos. Si la respuesta es no, se debe marcar con un N/A (no aplica) los demás campos sobre datos abiertos.

Sectorial fuente del dato abierto. Este atributo sólo es utilizado si la respuesta en el atributo de Datos Abiertos es SI. Corresponde al tipo de clasificación temática, tales como: Agrícola y pesquera, Ambiental, Científica, Cultural, Económica y Comercial, Geográfica, Política, Sistema Legal, Social, Transporte y Tráfico y demás que sean identificados.

Categoría: se detalla la sectorial de donde se genera los datos, salud, minas, educación, entes de control, deporte, desarrollo, agricultura, infraestructura.

Frecuencia de actualización: este campo está definido por la frecuencia en que se actualiza el dato, semanal, mensual, bimestral, trimestral, semestral y anual.

URL de Publicación en Datos.gov.co Este atributo sólo es utilizado si la respuesta en el atributo de Datos Abiertos es SI. Dirección electrónica del lugar donde se encuentra disponibles los datos abiertos y dispuestos para su descarga.

Cobertura geográfica. Solo aplica cuando el activo de información es dato abierto

Tipo de información. Puede ser:

Información estructurada
Esta información se suele encontrar en la mayoría de bases de datos. Son archivos de tipo texto que se suelen mostrar en filas y columnas con títulos. Son datos que pueden ser ordenados y procesados fácilmente por todas las herramientas de minería de datos.

Un ejemplo común de información estructurada es la información que se encuentra almacenada en una base de datos, como MS Access, SQL, ORACLE.

Información semiestructurada
Los datos semiestructurados son de un nivel medio de estructuración y rigidez organizativa. Se encuentran a medio camino entre los estructurados y los no estructurados. Un ejemplo válido sería un servidor local que almacenara todos los datos de correo electrónico y archivos adjuntos dentro de la base de datos.

Información no estructurada

La información no estructurada son datos que no están en una base de datos o están contenidos en algún otro tipo de estructura de datos. Los datos no estructurados pueden ser textuales o no textuales. Por ejemplo, son los datos que se generan en mensajes de correo electrónico, presentaciones PowerPoint, documentos de Word, software de colaboración y mensajes instantáneos.

7.5. Identificación de los riesgos inherentes de seguridad digital

Para efectos de esta metodología se definen como riesgos inherentes de seguridad digital:

- ✓ Pérdida de la confidencialidad
- ✓ Pérdida de la integridad
- ✓ Pérdida de la disponibilidad

Cada uno de los activos de información tendrá asociado uno o más riesgos relacionados, a los cuales se analizará 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:

7.5.1. Factores de riesgo

Se entiende como factores de riesgo a las fuentes generadoras de riesgo, a continuación, se detalla un listado de factores de riesgo a tener a la Entidad:

Factor	Definición	Descripción
Procesos	Eventos relacionados con errores en las actividades que deben realizar los servidores públicos en la Entidad	Falta de procedimientos
		Errores de grabación, autorización
		Errores de cálculo para pagos internos
		Falta de capacitación, temas relacionadas con el personal
Talento Humano	Incluye seguridad y salud en el trabajo. Se analiza posible dolo e intención frente a la corrupción.	Hurto de activos
		Posibles comportamientos no éticos de los empleados
		Fraude interno (corrupción, soborno)
Tecnología	Eventos relacionados con la infraestructura tecnológica de la entidad	Daño de equipos
		Caída de aplicaciones
		Caída de redes
		Errores en programas
Infraestructura	Eventos relacionados con la infraestructura física de la entidad	Derrumbes
		Incendios
		Inundaciones
		Daños a activos físicos

Tabla 12. Factores de riesgo

7.5.2. Identificación de amenazas

Las amenazas de seguridad son situaciones o fuentes que pueden hacer daño a los activos de información y materializar los riesgos, las amenazas pueden ser deliberadas, accidentales o ambientales (naturales) y pueden dar como resultado, por ejemplo, daño o pérdida de los servicios esenciales.

Para cada uno de los tipos de amenazas, la siguiente lista indica los casos en que D (deliberadas), F (fortuitas) y A (ambientales) son pertinentes. La letra D se utiliza para todas las acciones deliberadas que tienen como objetivo los activos de la información, F se utiliza para las acciones

humanas que pueden dañar accidentalmente los activos de información y A se utiliza para todos los incidentes que no se basa en las acciones humanas:

Tipo	Amenaza	Origen
Daño físico	Fuego Agua Contaminación Destrucción de los equipos o medios Polvo Corrosión Congelamiento.	F, D, A
Eventos naturales	Fenómenos climáticos Fenómenos sísmicos Fenómenos volcánicos Fenómenos meteorológicos Inundación.	A
Pérdida de los servicios esenciales	Falla en el sistema de suministro de agua o de aire acondicionado Pérdida de suministro de energía Falla en el equipo de telecomunicaciones	A, F F, D, A A, F
Perturbación debida a la radiación	Radiación electromagnética, Radiación térmica, Impulsos electromagnéticos	F, D, A
Compromiso de la información	Interceptación de señales de interferencia comprometida Espionaje remoto Escucha encubierta Hurto de medios o documentos Hurto de equipo Recuperación de medios reciclados o desechados Divulgación Datos provenientes de fuentes no confiables Manipulación con hardware Manipulación con software Detección de la posición	D D D D D D F, D F, D D F, D D
Fallas técnicas	Falla del equipo Mal funcionamiento del equipo Saturación del sistema de información Mal funcionamiento del Software Incumplimiento en el mantenimiento del sistema de información	F F F, D F F, D
Acciones no autorizadas	Uso no autorizado del equipo Copia fraudulenta del software Uso de software falso o copiado Corrupción de los datos Procesamiento ilegal de los datos	D D F, D D D
Compromiso de las funciones	Error en el uso Abuso de derechos Falsificación de derechos Negación de acciones Incumplimiento de la disponibilidad de personal	F F, D D D F, D, A

Tabla 13. Ejemplo de amenazas

También existen amenazas dirigidas por el hombre, como los son:

Fuente de amenaza	Motivación	Acciones amenazantes
Pirata informático, intruso ilegal	Reto, Ego, Rebelión, Estatus Y Dinero	✓ Piratería ✓ Ingeniería social

Fuente de amenaza	Motivación	Acciones amenazantes
		✓ Intrusión ✓ accesos forzados al sistema ✓ Acceso no autorizado al sistema.
Criminal de la computación	Destrucción de información, Divulgación ilegal de información, Ganancia monetaria, Alteración no autorizada de los datos	✓ Crimen por computador (por ejemplo, espionaje cibernético) ✓ Acto fraudulento (por ejemplo, repetición, personificación, interceptación) ✓ Soborno de la información ✓ Suplantación de identidad ✓ Intrusión en el sistema.
Terrorismo	Chantaje, Destrucción, Explotación, Venganza, Ganancia política, Cubrimiento de los medios de comunicación	✓ Bomba/terrorismo ✓ Guerra de la información (warfare) ✓ Ataques contra el sistema (por ejemplo, negación distribuida del servicio) ✓ Penetración en el sistema ✓ Manipulación del sistema
Espionaje industrial (Inteligencia, empresas, gobiernos extranjeros, otros intereses gubernamentales)	Ventaja competitiva Espionaje económico.	✓ Ventaja de defensa ✓ Ventaja Política ✓ Explotación económica ✓ Hurto de información ✓ Intrusión en la privacidad personal ✓ Ingeniería social ✓ Penetración en el sistema ✓ Acceso no autorizado al sistema (acceso a información clasificada, de propiedad y/o relacionada con la tecnología)
Intrusos (empleados con entrenamiento deficiente, descontento, malintencionado, negligente, deshonesto o despedido)	Curiosidad, Ego, Inteligencia, Ganancia monetaria, Venganza, Errores y omisiones no intencionales) por ejemplo, error en el ingreso de los 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 (por ejemplo, virus, bomba lógica, troyano) ✓ Venta de información personal ✓ Errores en el sistema (bugs) ✓ Intrusión al sistema ✓ Sabotaje del sistema ✓ Acceso no autorizado al sistema

Tabla 14. Fuente de amenazas y acciones amenazantes

7.5.3. Identificación de vulnerabilidades

Las vulnerabilidades de seguridad son debilidades conocidas en un activo de información, a continuación, se presenta un listado de las vulnerabilidades más comunes que pueden ser utilizadas para la identificación de riesgos inherentes de seguridad digital:

Tipo	Vulnerabilidades
Hardware	✓ Mantenimiento insuficiente ✓ Ausencia de esquemas de reemplazo periódico ✓ Sensibilidad a la radiación electromagnética

Tipo	Vulnerabilidades
	✓ Susceptibilidad a las variaciones de temperatura (o al polvo y suciedad) ✓ Almacenamiento sin protección ✓ Falta de cuidado en la disposición final ✓ Copia no controlada
Software	✓ Ausencia o insuficiencia de pruebas de software ✓ Ausencia de terminación de sesión ✓ Ausencia de registros de auditoría ✓ Asignación errada de los derechos de acceso ✓ Interfaz de usuario compleja ✓ Ausencia de documentación ✓ Fechas incorrectas ✓ Ausencia de mecanismos de identificación y autenticación de usuarios ✓ Contraseñas sin protección ✓ Software nuevo o inmaduro
Red	✓ Ausencia de pruebas de envío o recepción de mensajes ✓ Líneas de comunicación sin protección ✓ Conexión deficiente de cableado ✓ Tráfico sensible sin protección ✓ Punto único de falla
Personal	✓ Ausencia del personal ✓ Entrenamiento insuficiente ✓ Falta de conciencia en seguridad ✓ Ausencia de políticas de uso aceptable ✓ Trabajo no supervisado de personal externo o de limpieza
Lugar	✓ Uso inadecuado de los controles de acceso al edificio ✓ Áreas susceptibles a inundación ✓ Red eléctrica inestable ✓ Ausencia de protección en puertas o ventanas
Organización	✓ Ausencia de procedimiento de registro/retiro de usuarios ✓ Ausencia de proceso para supervisión de derechos de acceso ✓ Ausencia de control de los activos que se encuentran fuera de las instalaciones ✓ Ausencia de acuerdos de nivel de servicio (ANS o SLA) ✓ Ausencia de mecanismos de monitoreo para brechas en la seguridad ✓ Ausencia de procedimientos y/o de políticas en general

Tabla 15. Ejemplo de vulnerabilidades

A continuación, se presentan algunos ejemplos de relación entre vulnerabilidades de acuerdo con el tipo de activo de información y las amenazas:

Tipos de activo de información	Ejemplos de vulnerabilidades	Ejemplos de amenazas
Hardware	Mantenimiento insuficiente/instalación fallida de los medios de almacenamiento.	Incumplimiento en el mantenimiento sistema de información
	Ausencia de esquemas de reemplazo periódico.	Destrucción de equipos o de medios
	Susceptibilidad a la humedad, el polvo y la suciedad.	Polvo, corrosión, congelamiento
	Sensibilidad a la radiación electromagnética	Radiación electromagnética
	Ausencia de un eficiente control de cambios en la configuración	Error en el uso
	Susceptibilidad a las variaciones de voltaje	Pérdida del suministro de energía
	Susceptibilidad a las variaciones de temperatura	Fenómenos meteorológicos
	Almacenamiento sin protección	Hurto de medios o documentos
	Falta de cuidado en la disposición final	Hurto de medios o documentos

Tipos de activo de información	Ejemplos de vulnerabilidades	Ejemplos de amenazas
	Copia no controlada	Hurto de medios o documentos
Software	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 la 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
	Ausencia 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
	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
	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 usos no controlados 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
	Falla en la producción de informes de gestión	Uso no autorizado del equipo
Red	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.	Conexión deficiente de los cables.
	Punto único de falla	Falla 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
Personal	Ausencia del personal	Incumplimiento en la disponibilidad del personal
	Procedimientos inadecuados de contratación	Destrucción de equipos o medios
	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

Tipos de activo de información	Ejemplos de vulnerabilidades	Ejemplos de amenazas
	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
Lugar	Uso inadecuado o descuidado del control de acceso físico a las edificaciones y los recintos	Destrucción de equipo o medios
	Ubicación en un área susceptible de inundación	Inundación
	Red energética inestable	Pérdida del suministro de energía
	Ausencia de protección física de la edificación, puertas y ventanas	Hurto de equipo
Organización	Ausencia de procedimiento formal para el	Abuso de los derechos
	registro y retiro de usuarios	Abuso de los derechos
	Ausencia de proceso formal para la revisión (supervisión) de los derechos de acceso	Abuso de los derechos
	Ausencia o insuficiencia de disposiciones (con respecto a la seguridad) en los contratos con los clientes y/o terceras partes	Abuso de los derechos
	Ausencia de procedimiento de monitoreo de los recursos de procesamiento de información	Abuso de los derechos
	Ausencia	Abuso de los derechos
	Ausencia de procedimientos de identificación y valoración de riesgos	Abuso de los derechos
	Ausencia de reportes de fallas en los registros de administradores y operadores	Incumplimiento en el sistema de información
	Respuesta inadecuada de mantenimiento del servicio	Incumplimiento en el sistema de información
	Ausencia de acuerdos de nivel de servicio, o insuficiencia en los mismos.	Incumplimiento en el sistema de información
	Ausencia de procedimiento de control de cambios	Corrupción de datos
	Ausencia de procedimiento formal para el control de la documentación del SGSI	Corrupción de datos
	Ausencia de procedimiento formal para la supervisión del registro del SGSI	Datos provenientes de fuentes no confiables
	Ausencia de procedimiento formal para la autorización de la información disponible al público	Negación de acciones
	Ausencia de asignación adecuada de responsabilidades en la seguridad de la información	Falla del equipo
	Ausencia de planes de continuidad	Error en el uso
	Ausencia de políticas sobre el uso del correo electrónico	Error en el uso
	Ausencia de procedimientos para la introducción del software en los sistemas operativos	Error en el uso
	Ausencia de registros en las bitácoras (logs) de administrador y operario.	Error en el uso
	Ausencia de procedimientos para el manejo de información clasificada	Error en el uso
	Ausencia de responsabilidades en la seguridad de la información en la descripción de los cargos	Procesamiento ilegal de datos

Tipos de activo de información	Ejemplos de vulnerabilidades	Ejemplos de amenazas
	Ausencia o insuficiencia en las disposiciones (con respecto a la seguridad de la información) en los contratos con los empleados	Hurto de equipo
Organización	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 o insuficiencia de política sobre limpieza de escritorio y de pantalla	Hurto de medios o documentos
	Ausencia de autorización de los recursos de procesamiento de la información	Hurto de medios o documentos
	Ausencia de mecanismos de monitore establecidos para las brechas en la seguridad	Hurto de medios o documentos
	Ausencia de revisiones regulares por parte de la gerencia	Uso no autorizado del equipo
	Ausencia de procedimientos para la presentación de informes sobre las debilidades en la seguridad	Uso no autorizado del equipo
	Ausencia de procedimientos del cumplimiento de las disposiciones con los derechos intelectuales	Uso de software falso o copiado

Tabla 16. Ejemplo de vulnerabilidad vs amenazas, clasificada por tipos

7.6. Análisis del riesgo inherente de seguridad digital

Para cada uno de los activos de información que ya han sido identificados y valorados con anterioridad, puede existir uno o varios riesgos de seguridad digital, como primera línea de defensa, esta responsabilidad recae sobre el proceso propietario del activo de información; el análisis del riesgo incluye, identificar los riesgos, analizar y valorar los riesgos para posteriormente tratarlos.

Cada uno de los riesgos deberá tener un propietario del riesgo (quien tiene que rendir cuentas sobre el riesgo o quien tiene la autoridad para gestionar el riesgo), este propietario, será el líder o responsable del proceso, en caso de requerirse, este último podrá delegar la gestión del riesgo, pero lo anterior, no lo exime de la responsabilidad inherente sobre el mismo. A continuación, se describe cada uno de los elementos a tener en cuenta para el análisis del riesgo inherente de seguridad digital:

Activo: Nombre del activo de información identificado.

Propiedad del riesgo: La propiedad del riesgo está enmarcada en la pérdida de cualquiera de los pilares de la seguridad digital, esta propiedad puede ser, pérdida de confidencialidad, de integridad o de disponibilidad que afecte a la información o al activo de información

Amenazas - causa inmediata: Se define la amenaza que pueda generar alguna afectación a la información o al activo de información, también puede entenderse como la causa inmediata.

Vulnerabilidades - causa raíz: Se define la vulnerabilidad identificada en el activo de información, una vulnerabilidad es una debilidad conocida o no que puede ser explotada por una amenaza, también puede entenderse como la causa raíz.

Descripción del Riesgo: Se realiza una descripción del riesgo, esta descripción se obtiene a partir de la propiedad del riesgo + amenazas + vulnerabilidades

Responsable: Es el cargo responsable de la gestión del riesgo, es el mismo dueño del activo o quien delegue.

Clasificación del riesgo: Como lo indica la guía del DAFP en su capítulo 2.6 Guía para la administración del riesgo y el diseño de controles en entidades públicas, la clasificación del riesgo se define así:

Clasificación de riesgo	Descripción
Ejecución y administración de procesos	Pérdidas derivadas de errores en la ejecución y administración de procesos.
Fraude externo	Pérdida derivada de actos de fraude por personas ajenas a la organización (no participa personal de la entidad).
Fraude interno	Pérdida debido a actos de fraude, actuaciones irregulares, comisión de hechos delictivos abuso de confianza, apropiación indebida, incumplimiento de regulaciones legales o internas de la entidad en las cuales está involucrado por lo menos 1 participante interno de la organización, son realizadas de forma intencional y/o con ánimo de lucro para sí mismo o para terceros
Fallas tecnológicas	Errores en hardware, software, telecomunicaciones, interrupción de servicios básicos
Relaciones laborales	Pérdidas que surgen de acciones contrarias a las leyes o acuerdos de empleo, salud o seguridad, del pago de demandas por daños personales o de discriminación.
Usuarios, productos y prácticas	Fallas negligentes o involuntarias de las obligaciones frente a los usuarios y que impiden satisfacer una obligación profesional frente a éstos
Daños a activos fijos/ eventos externos	Pérdida por daños o extravíos de los activos fijos por desastres naturales u otros riesgos/eventos externos como atentados, vandalismo, orden público

Tabla 17. Clasificación de riesgos guía DAFP

Probabilidad: para determinar la probabilidad, debe analizarse que tan posible es que ocurra o se materialice el riesgo, se expresa en términos de frecuencia, esto implica analizar un número de eventos en un periodo determinado, la probabilidad se identifica con base en los siguientes criterios:

Probabilidad de ocurrencia				
Nivel	**Calificación**	**Descripción**	**Frecuencia**	**Porcentaje**
1	Muy Baja	El evento puede ocurrir solo en circunstancias excepcionales (poco comunes o anormales).	No se ha presentado en los últimos 5 años	20%
2	Baja	El evento puede ocurrir en algún momento	Al menos 1 vez en los últimos 5 años	40%
3	Moderada	El evento podrá ocurrir en algún momento.	Al menos 1 vez en los últimos 2 años	60%
4	Alta	Es viable que el evento ocurra en la mayoría de las circunstancias.	Al menos una vez en el último año	80%
5	Muy Alta	Se espera que el evento ocurra en la mayoría de las circunstancias.	Más de 1 vez al año	100%

Tabla 18. Criterios para la calificación de la probabilidad

Impacto: Por impacto se entiende como las consecuencias que puede ocasionar a la entidad la materialización de algún riesgo, para determinar el impacto se utilizan los siguientes criterios:

Impacto generado				
Nivel	**Calificación**	**Afectación**	**Consecuencias**	**Porcentaje**
1	Insignificante	Afectación <=5% de la población. Afectación <=5% del presupuesto anual de la entidad.	Sin afectación a la integridad y disponibilidad del activo de información.	20%
2	Menor	Afectación hasta 20% de la población. Afectación hasta 20% del presupuesto anual de la entidad.	Afectación leve a la integridad y disponibilidad del activo de información, afectación leve a la confidencialidad.	40%
3	Moderado	Afectación hasta 40% de la población. Afectación hasta 40% del presupuesto anual de la entidad.	Afectación a la integridad y disponibilidad del activo de información, con continuidad de la operación normal. Afectación moderada a la información con alto nivel de confidencialidad	60%
4	Mayor	Afectación hasta 60% de la población. Afectación hasta 60% del presupuesto anual de la entidad.	Afectación a la integridad y disponibilidad del activo de información, con continuidad intermitente de la operación normal. Afectación significativa a la confidencialidad	80%
5	Catastrófico	Afectación hasta 80% de la población. Afectación hasta 80% del presupuesto anual de la entidad.	Afectación a la integridad y disponibilidad del activo de información, sin continuidad de la operación normal. Información con altísimo nivel de sensibilidad comprometida	100%

Tabla 19. Criterios para la calificación del impacto

Zona de riesgo: a partir del análisis de la probabilidad de ocurrencia del riesgo y su impacto, se determina la zona de riesgo inherente

Zona de riesgo= Impacto x probabilidad

A continuación, un ejemplo de identificación de riesgos:

Activo	**Propiedad del riesgo**	**Amenazas - causa inmediata**	**Vulnerabilidades - causa raíz**	**Descripción del Riesgo**	**Responsable**	**Clasificación del riesgo**	**Probabilidad**	**Impacto**	**Zona de riesgo**

Aplicativo ARANDA	Pérdida de Disponibilida	Pérdida del suministro de energía	Susceptibilidad a las variaciones de voltaje	Pérdida de disponibilidad del aplicativo por fallas en el suministro de energía debido a la ausencia de dispositivos de control de voltaje.	Secretario TIC	Fallas tecnológicas	Baja	Menor	Moderado
Documento PETI	Pérdida de Confidencialid	Abuso de derechos	Uso inadecuado o descuidado del control de acceso físico a las edificaciones y los recintos	Pérdida de confidencialidad de la información del documento PETI por abuso de los derechos de acceso físico debido a la ausencia de control físico de acceso.	Secretario TIC	Fraude Externo	Alta	Moderado	Moderado

Tabla 20. Ejemplo de identificación de nivel de riesgos

7.7. Identificación de los controles existentes

Una vez establecidos y valorados los riesgos inherentes se debe proceder con la identificación y evaluación de los controles existentes y sus efectos en el riesgo identificado.

La identificación de los controles existentes ayuda a evitar trabajo o costos innecesarios para el correcto tratamiento de riesgo, por ejemplo, cuando existe duplicidad de los controles.

Mientras se realiza la identificación de los controles existentes es necesario revisar si dichos controles funcionan correctamente, ya que si el control no funciona como se espera, puede causar nuevas vulnerabilidades y es posible que se requieran controles complementarios para tratar de manera eficaz el riesgo identificado.

A continuación, se detalla cada uno de los campos a tener en cuenta para la identificación de los controles existentes:

Control existente: detalle del control existente para mitigar el riesgo

¿El control afecta la probabilidad o afecta el impacto?: si el control busca prevenir o detectar las causas que dan origen al riesgo entonces se dice que afecta la probabilidad, en caso de que el control busque corregir dichas causas, se dice que afectará el impacto.

¿Las actividades que desarrolla el control, buscan prevenir, detectar o corregir las causas que dan origen al riesgo?: Al igual que el anterior, se debe detallar si las actividades del control buscan prevenir, detectar o corregir las causas que dan origen al riesgo.

¿El control se ejecuta de manera automática o manual?: Las actividades de ejecución de un control pueden ser automáticas o manuales, se dice que son automáticas cuando las actividades se ejecutan por un sistema y/o aplicativo de manera automática, sin la intervención de personas para su ejecución; la ejecución manual incluye actividades para mitigar el riesgo que son realizadas por una persona, esto lógicamente tiene implícito el error humano.

¿Existen manuales, instructivos o procedimientos para el manejo del control?: Definir si las actividades de ejecución y manejo de un control están soportadas a través de manuales, instructivos o procedimientos documentados aprobados.

¿Cómo es la frecuencia de ejecución del control?: la ejecución de control puede ser continua o aleatoria; se dice que es continua cuando son ejecutadas cada vez que se realiza la actividad originadora del riesgo, por ejemplo, utilización de contraseña de acceso a una aplicación; y se dice que es aleatoria, cuando los controles no siempre se ejecutan cuando se realiza la actividad originadora de riesgo, por ejemplo, revisión periódica de los logs de auditoria de una aplicación.

¿Se cuenta con evidencias de la ejecución y seguimiento del control? Acá se debe validar si hay evidencias tangibles de la ejecución del control y su efectividad.

¿Las desviaciones o diferencias ejecutadas del control establecido son investigadas y resueltas de manera oportuna? Se debe validar si han existido desviaciones o diferencias en la correcta ejecución del control vs lo esperado con respecto a la mitigación del riesgo, si han existido, validar si han sido o no investigadas y resueltas de manera oportuna; lo anterior, debe estar soportado documentalmente.

A continuación, un ejemplo de la identificación de controles existentes:

Descripción del Riesgo	Control existente	¿El control afecta la probabilidad o afecta el impacto?	¿Las actividades que desarrolla el control, buscan prevenir, detectar o corregir las causas que dan origen al riesgo?	¿El control se ejecuta de manera automática o Manual?	¿Existen manuales, instructivos o procedimientos para el manejo del control?	¿Cómo es la frecuencia de ejecución del control?	¿Se cuenta con evidencias de la ejecución y seguimiento del control?	¿Las desviaciones o diferencias ejecutadas del control establecido son investigadas y resueltas de manera oportuna?
Pérdida de disponibilidad del aplicativo por fallas en el suministro de energía debido a la ausencia de dispositivos de control de voltaje.	UPS para el servidor	Probabilidad	Prevenir	Automática	No	Continua	Si	Si
	Cambio periódico de elementos eléctricos y voltaje	Probabilidad	Prevenir	Manual	Si	Aleatoria	Si	Si
	Copias de respaldo periódicas de la información en el aplicativo	Impacto	Corregir	Automático	Sí	Continua	No	Sí

Tabla 21. Ejemplo de evaluación de controles existentes

Nota: Para determinar si existen uno o varios controles asociados a los riesgos inherentes identificados se pueden consultar el Anexo 1 del presente documento OBJETIVOS DE CONTROL Y CONTROLES DE REFERENCIA (Tomados del Anexo A de la Norma ISO/IEC 27001:2013) como un insumo base y determinar si ya posee alguno de los controles orientados a seguridad digital que están enunciados en dicho anexo.

7.8. Planes de tratamiento de riesgos de seguridad digital e indicadores

Una vez identificados los riesgos, es necesario definir la forma como se realizará el tratamiento que se le dará a cada uno de ellos, lo anterior, será el Plan de Tratamiento de Riesgos, dicho plan estará alineado a los criterios y al apetito de riesgos definido en la Política de Administración de Riesgos de la Gobernación de Santander.[8]

En este paso se debe identificar con claridad el orden en que serán implementadas las acciones, y la forma en que se integrarán con los procesos de la Entidad.

El plan de tratamiento de riesgos debe incluir:

- ✓ El detalle de las opciones de tratamiento de riesgo (Eliminar, Mitigar o Aceptar)
- ✓ Responsables de aprobar e implementar el plan
- ✓ Las acciones para el tratamiento del riesgo inherente
- ✓ Tiempos de implementación de las actividades y las acciones de tratamiento
- ✓ Mediciones del rendimiento del plan
- ✓ Acciones para el monitoreo del plan

7.9. Indicadores para la medición de la GRSD

Los indicadores de riesgos son las métricas utilizadas para la medición de la adecuada gestión de riesgos en la Gobernación de Santander, provee señales tempranas de exposiciones al riesgo y probables desviaciones que puedan tener impacto en el logro de los objetivos de la Entidad, a continuación, los indicadores utilizados para la GRSD:

Identificación de activos de información	
DEFINICIÓN	
El indicador permite determinar y hacer seguimiento a la protección de los activos de información con alto nivel de criticidad	
DESCRIPCIÓN DE VARIABLES	**FÓRMULA**
V1: Número de activos de información críticos	(V1/V2)*100
V2: Número total de activos de información	

Tabla 22. Indicador sobre avance de identificación de activos de información

Funcionarios que han recibido capacitación en gestión de riesgos de seguridad digital

[8] Política de administración del riesgo 2020 Gobernación de Santander, ver: http://historico.santander.gov.co/intra/index.php/sig/finish/582-4-manuales-instructivos-guias-planes-programas-politicas-reglamentos/11446-politica-de-administracion-del-riesgo

DEFINICIÓN	
El indicador permite determinar y hacer seguimiento a la sensibilización de los funcionarios con respecto a la protección de activos de información.	
DESCRIPCIÓN DE VARIABLES	**FÓRMULA**
V1: Número de personas capacitadas	(V1/V2)*100
V2: Número total de funcionarios en la entidad	

Tabla 23. Indicador sobre capacitación en GRSD

Eventos de riesgos materializados	
DEFINICIÓN	
El indicador permite determinar y hacer seguimiento a la gestión de riesgos desde el punto de vista de materialización de riesgos.	
DESCRIPCIÓN DE VARIABLES	**FÓRMULA**
V1: Número de eventos de riesgos materializados	(V1/V2)*100
V2: Número total de riesgos identificados	

Tabla 24. Indicador sobre eventos de riesgos materializados

Anexo 1 OBJETIVOS DE CONTROL Y CONTROLES DE REFERENCIA

Núm.	Control	Descripción
A.5.1.1	Políticas para la seguridad de la información	Se debería definir un conjunto de políticas para la seguridad de la información, aprobada por la dirección, publicada y comunicada a los empleados y partes externas pertinentes.
A.5.1.2	Revisión de las políticas para seguridad de la información	Las políticas para seguridad de la información se deberían revisar a intervalos planificados o si ocurren cambios significativos, para asegurar su conveniencia, adecuación y eficacia continúas.
A.6.1.1	Roles y responsabilidades para la seguridad de información	Se deberían definir y asignar todas las responsabilidades de la seguridad de la información
A.6.1.1	Roles y responsabilidades para la seguridad de la información	Se deben definir y asignar todas las responsabilidades de la seguridad de la información.
A.6.1.2	Separación de deberes	Los deberes y áreas de responsabilidad en conflicto se deben separar para reducir las posibilidades de modificación no autorizada o no intencional, o el uso indebido de los activos de la organización.
A.6.1.3	Contacto con las autoridades	Se deben mantener contactos apropiados con las autoridades pertinentes.
A.6.1.4	Contacto con grupos de interés especial	Se deben mantener contactos apropiados con grupos de interés especial u otros foros y asociaciones profesionales especializadas en seguridad.
A.6.1.5	Seguridad de la información en la gestión de proyectos	La seguridad de la información se debe tratar en la gestión de proyectos, independientemente del tipo de proyecto.
A.6.2.1	Política para dispositivos móviles	Se deben adoptar una política y unas medidas de seguridad de soporte, para gestionar los riesgos introducidos por el uso de dispositivos móviles.
A.6.2.2	Teletrabajo	Se deben implementar una política y unas medidas de seguridad de soporte, para proteger la información a la que se tiene acceso, que es procesada o almacenada en los lugares en los que se realiza teletrabajo.
A.7.1.1	Selección	Las verificaciones de los antecedentes de todos los candidatos a un empleo se deben llevar a cabo de acuerdo con las leyes, reglamentaciones y ética pertinentes, y deben ser proporcionales a los requisitos de negocio, a la clasificación de la información a que se va a tener acceso, y a los riesgos percibidos.
A.7.1.2	Términos y condiciones del empleo	Los acuerdos contractuales con empleados y contratistas deben establecer sus responsabilidades y las de la organización en cuanto a la seguridad de la información.
A.7.2.1	Responsabilidades de la dirección	La dirección debe exigir a todos los empleados y contratistas la aplicación de la seguridad de la información de acuerdo con las políticas y procedimientos establecidos por la organización.
A.7.2.2	Toma de conciencia, educación y formación en la seguridad de la información	Todos los empleados de la organización, y en donde sea pertinente, los contratistas, deben recibir la educación y la formación en toma de conciencia apropiada, y actualizaciones regulares sobre las políticas y procedimientos de la organización pertinentes para su cargo.

Núm.	Control	Descripción
A.7.2.3	Proceso disciplinario	Se debe contar con un proceso formal, el cual debe ser comunicado, para emprender acciones contra empleados que hayan cometido una violación a la seguridad de la información.
A.7.3.1	Terminación o cambio de responsabilidades de empleo	Las responsabilidades y los deberes de seguridad de la información que permanecen válidos después de la terminación o cambio de empleo se deben definir, comunicar al empleado o contratista y se deben hacer cumplir.
A.8.1.1	Inventario de activos	Se deben identificar los activos asociados con información e instalaciones de procesamiento de información, y se debe elaborar y mantener un inventario de estos activos.
A.8.1.2	Propiedad de los activos	Los activos mantenidos en el inventario deben tener un propietario.
A.8.1.3	Uso aceptable de los activos	Se deben identificar, documentar e implementar reglas para el uso aceptable de información y de activos asociados con información e instalaciones de procesamiento de información.
A.8.1.4	Devolución de activos	Todos los empleados y usuarios de partes externas deben devolver todos los activos de la organización que se encuentren a su cargo, al terminar su empleo, contrato o acuerdo.
A.8.2.1	Clasificación de la información	La información se debe clasificar en función de los requisitos legales, valor, criticidad y susceptibilidad a divulgación o a modificación no autorizada.
A.8.2.2	Etiquetado de la información	Se debe desarrollar e implementar un conjunto adecuado de procedimientos para el etiquetado de la información, de acuerdo con el esquema de clasificación de información adoptado por la organización.
A.8.2.3	Manejo de activos	Se deben desarrollar e implementar procedimientos para el manejo de activos, de acuerdo con el esquema de clasificación de información adoptado por la organización.
A.8.3.1	Gestión de medios removibles	Se deben implementar procedimientos para la gestión de medios removibles, de acuerdo con el esquema de clasificación adoptado por la organización.
A.8.3.2	Disposición de los medios	Se debe disponer en forma segura de los medios cuando ya no se requieran, utilizando procedimientos formales.
A.8.3.3	Transferencia de medios físicos	Los medios que contienen información se deben proteger contra acceso no autorizado, uso indebido o corrupción durante el transporte.
A.9.1.1	Política de control de acceso	Se debe establecer, documentar y revisar una política de control de acceso con base en los requisitos del negocio y de seguridad de la información.
A.9.1.2	Acceso a redes y a servicios en red	Solo se debe permitir acceso de los usuarios a la red y a los servicios de red para los que hayan sido autorizados específicamente.
A.9.2.1	Registro y cancelación del registro de usuarios	Se debe implementar un proceso formal de registro y de cancelación de registro de usuarios, para posibilitar la asignación de los derechos de acceso.
A.9.2.2	Suministro de acceso de usuarios	Se debe implementar un proceso de suministro de acceso formal de usuarios para asignar o revocar los derechos de acceso para todo tipo de usuarios para todos los sistemas y servicios.
A.9.2.3	Gestión de derechos de acceso privilegiado	Se debe restringir y controlar la asignación y uso de derechos de acceso privilegiado.

Núm.	Control	Descripción
A.9.2.4	Gestión de información de autenticación secreta de usuarios	La asignación de información de autenticación secreta se debe controlar por medio de un proceso de gestión formal.
A.9.2.5	Revisión de los derechos de acceso de usuarios	Los propietarios de los activos deben revisar los derechos de acceso de los usuarios, a intervalos regulares.
A.9.2.6	Retiro o ajuste de los derechos de acceso	Los derechos de acceso de todos los empleados y de usuarios externos a la información y a las instalaciones de procesamiento de información se deben retirar al terminar su empleo, contrato o acuerdo, o se deben ajustar cuando se hagan cambios.
A.9.3.1	Uso de información de autenticación secreta	Se debe exigir a los usuarios que cumplan las prácticas de la organización para el uso de información de autenticación secreta.
A.9.4.1	Restricción de acceso ala información	El acceso a la información y a las funciones de los sistemas de las aplicaciones se debe restringir de acuerdo con la política de control de acceso.
A.9.4.2	Procedimiento de ingreso seguro	Cuando lo requiere la política de control de acceso, el acceso a sistemas y aplicaciones se debe controlar mediante un proceso de ingreso seguro.
A.9.4.3	Sistema de gestión de contraseñas	Los sistemas de gestión de contraseñas deben ser interactivos y deben asegurar la calidad de las contraseñas.
A.9.4.4	Uso de programas utilitarios privilegiados	Se debe restringir y controlar estrictamente el uso de programas utilitarios que podrían tener capacidad de anular el sistema y los controles de las aplicaciones.
A.9.4.5	Control de acceso a códigos fuente de programas	Se debe restringir el acceso a los códigos fuente de los programas.
A.10.1.1	Política sobre el uso de controles criptográficos	Se debe desarrollar e implementar una política sobre el uso de controles criptográficos para la protección de la información.
A.10.1.2	Gestión de llaves	Se debe desarrollar e implementar una política sobre el uso, protección y tiempo de vida de las llaves criptográficas, durante todo su ciclo de vida.
A.11.1.1	Perímetro de seguridad física	Se deben definir y usar perímetros de seguridad, y usarlos para proteger áreas que contengan información confidencial o crítica, e instalaciones de manejo de información.
A.11.1.2	Controles de acceso físicos	Las áreas seguras se deben proteger mediante controles de acceso apropiados para asegurar que solo se permite el acceso a personal autorizado.
A.11.1.3	Seguridad de oficinas, recintos e instalaciones	Se debe diseñar y aplicar seguridad física a oficinas, recintos e instalaciones.
A.11.1.4	Protección contra amenazas externas y ambientales	Se debe diseñar y aplicar protección física contra desastres naturales, ataques maliciosos o accidentes.
A.11.1.5	Trabajo en áreas seguras	Se deben diseñar y aplicar procedimientos para trabajo en áreas seguras.
A.11.1.6	Áreas de despacho y carga	Se deben controlar los puntos de acceso tales como áreas de despacho y de carga y otros puntos en donde pueden entrar personas no autorizadas, y si es posible, aislarlos de las instalaciones de procesamiento de información para evitar el acceso no autorizado.

Núm.	Control	Descripción
A.11.2.1	Ubicación y protección de los equipos	Los equipos deben estar ubicados y protegidos para reducir los riesgos de amenazas y peligros del entorno, y las posibilidades de acceso no autorizado.
A.11.2.2	Servicios de suministro	Los equipos se deben proteger contra fallas de energía y otras interrupciones causadas por fallas en los servicios de suministro.
A.11.2.3	Seguridad del cableado	El cableado de energía eléctrica y de telecomunicaciones que porta datos o brinda soporte a los servicios de información se debe proteger contra interceptación, interferencia o daño
A.11.2.4	Mantenimiento de equipos	Los equipos se deben mantener correctamente para asegurar su disponibilidad e integridad continuas.
A.11.2.5	Retiro de activos	Los equipos, información o software no se deben retirar de su sitio sin autorización previa.
A.11.2.6	Seguridad de equipos y activos fuera de las instalaciones	Se deben aplicar medidas de seguridad a los activos que se encuentran fuera de las instalaciones de la organización, teniendo en cuenta los diferentes riesgos de trabajar fuera de dichas instalaciones.
A.11.2.7	Disposición segura o reutilización de equipos	Se deben verificar todos los elementos de equipos que contengan medios de almacenamiento para asegurar que cualquier dato confidencial o software licenciado haya sido retirado o sobreescrito en forma segura antes de su disposición o reuso.
A.11.2.8	Equipos de usuario desatendido	Los usuarios deben asegurarse de que a los equipos desatendidos se les da protección apropiada.
A.11.2.9	Política de escritorio limpio y pantalla limpia	Se debe adoptar una política de escritorio limpio para los papeles y medios de almacenamiento removibles, y una política de pantalla limpia en las instalaciones de procesamiento de información.
A.12.1.1	Procedimientos de operación documentados	Los procedimientos de operación se deben documentar y poner a disposición de todos los usuarios que los necesitan.
A.12.1.2	Gestión de cambios	Se deben controlar los cambios en la organización, en los procesos de negocio, en las instalaciones y en los sistemas de procesamiento de información que afectan la seguridad de la información.
A.12.1.3	Gestión de capacidad	Se debe hacer seguimiento al uso de recursos, hacer los ajustes, y hacer proyecciones de los requisitos de capacidad futura, para asegurar el desempeño requerido del sistema.
A.12.1.4	Separación de los ambientes de desarrollo, pruebas, y operación	Se deben separar los ambientes de desarrollo, prueba y operación, para reducir los riesgos de acceso o cambios no autorizados al ambiente de operación.
A.12.2.1	Controles contra códigos maliciosos	Se deben implementar controles de detección, de prevención y de recuperación, combinados con la toma de conciencia apropiada de los usuarios, para proteger contra códigos maliciosos.
A.12.3.1	Respaldo de la información	Se deben hacer copias de respaldo de la información, software e imágenes de los sistemas, y ponerlas a prueba regularmente de acuerdo con una política de copias de respaldo acordadas.
A.12.4.1	Registro de eventos	Se deben elaborar, conservar y revisar regularmente los registros acerca de actividades del usuario, excepciones, fallas y eventos de seguridad de la información.
A.12.4.2	Protección de la información de registro	Las instalaciones y la información de registro se deben proteger contra alteración y acceso no autorizado.
A.12.4.3	Registros del administrador	Las actividades del administrador y del operador del sistema se

Núm.	Control	Descripción
	y del operador	deben registrar, y los registros se deben proteger y revisar con regularidad.
A.12.4.4	Sincronización de relojes	Los relojes de todos los sistemas de procesamiento de información pertinentes dentro de una organización o ámbito de seguridad se deben sincronizar con una única fuente de referencia de tiempo.
A.12.5.1	Instalación de software en sistemas operativos	Se deben implementar procedimientos para controlar la instalación de software en sistemas operativos.
A.12.6.1	Gestión de las vulnerabilidades técnicas	Se debe obtener oportunamente información acerca de las vulnerabilidades técnicas de los sistemas de información que se usen; evaluar la exposición de la organización a estas vulnerabilidades, y tomar las medidas apropiadas para tratar el riesgo asociado.
A.12.6.2	Restricciones sobre la instalación de software	Se debe establecer e implementar las reglas para la instalación de software por parte de los usuarios.
A.12.7	Controles de auditorías de sistemas de información	Los requisitos y actividades de auditoría que involucran la verificación de los sistemas operativos se deben planificar y acordar cuidadosamente para minimizar las interrupciones en los procesos del negocio.
A.13.1.1	Controles de redes	Las redes se deben gestionar y controlar para proteger la información en sistemas y aplicaciones.
A.13.1.2	Seguridad de los servicios de red	Se deben identificar los mecanismos de seguridad, los niveles de servicio y los requisitos de gestión de todos los servicios de red, e incluirlos en los acuerdos de servicio de red, ya sea que los servicios se presten internamente o se contraten externamente.
A.13.1.3	Separación en las redes	Los grupos de servicios de información, usuarios y sistemas de información se deben separar en las redes.
A.13.2.1	Políticas y procedimientos de transferencia de información	Se debe contar con políticas, procedimientos y controles de transferencia formales para proteger la transferencia de información mediante el uso de todo tipo de instalaciones de comunicaciones.
A.13.2.2	Acuerdos sobre transferencia de información	Los acuerdos deben tratar la transferencia segura de información del negocio entre la organización y las partes externas.
A.13.2.3	Mensajería electrónica	Se debe proteger adecuadamente la información incluida en la mensajería electrónica.
A.13.2.4	Acuerdos de confidencialidad o de no divulgación	Se deben identificar, revisar regularmente y documentar los requisitos para los acuerdos de confidencialidad o no divulgación que reflejen las necesidades de la organización para la protección de la información.
A.14.1.1	Análisis y especificación de requisitos de seguridad de la información	Los requisitos relacionados con seguridad de la información se deben incluir en los requisitos para nuevos sistemas de información o para mejoras a los sistemas de información existentes.
A.14.1.2	Seguridad de servicios de las aplicaciones en redes públicas	La información involucrada en los servicios de las aplicaciones que pasan sobre redes públicas se debe proteger de actividades fraudulentas, disputas contractuales y divulgación y modificación no autorizadas.
A.14.1.3	Protección de transacciones de los servicios de las	La información involucrada en las transacciones de los servicios de las aplicaciones se debe proteger para evitar la transmisión incompleta, el enrutamiento errado, la alteración no autorizada de

Núm.	Control	Descripción
	aplicaciones	mensajes, la divulgación no autorizada, y la duplicación o reproducción de mensajes no autorizada.
A.14.2.1	Política de desarrollo seguro	Se deben establecer y aplicar reglas para el desarrollo de software y de sistemas, a los desarrollos dentro de la organización.
A.14.2.2	Procedimientos de control de cambios en sistemas	Los cambios a los sistemas dentro del ciclo de vida de desarrollo se deben controlar mediante el uso de procedimientos formales de control de cambios.
A.14.2.3	Revisión técnica de las aplicaciones después de cambios en la plataforma de operación	Cuando se cambian las plataformas de operación, se deben revisar las aplicaciones críticas del negocio, y someter a prueba para asegurar que no haya impacto adverso en las operaciones o seguridad de la organización.
A.14.2.4	Restricciones en los cambios a los paquetes de software	Se deben desalentar las modificaciones a los paquetes de software, los cuales se deben limitar a los cambios necesarios, y todos los cambios se deben controlar estrictamente.
A.14.2.5	Principios de construcción de los sistemas seguros	Se deben establecer, documentar y mantener principios para la construcción de sistemas seguros, y aplicarlos a cualquier actividad de implementación de sistemas de información.
A.14.2.6	Ambiente de desarrollo seguro	Las organizaciones deben establecer y proteger adecuadamente los ambientes de desarrollo seguros para las actividades de desarrollo e integración de sistemas que comprendan todo el ciclo de vida de desarrollo de sistemas.
A.14.2.7	Desarrollo contratado externamente	La organización debe supervisar y hacer seguimiento de la actividad de desarrollo de sistemas contratados externamente.
A.14.2.8	Pruebas de seguridad de sistemas	Durante el desarrollo se deben llevar a cabo pruebas de funcionalidad de la seguridad.
A.14.2.9	Prueba de aceptación de sistemas	Para los sistemas de información nuevos, actualizaciones y nuevas versiones, se deben establecer programas de prueba para aceptación y criterios de aceptación relacionados.
A.14.3.1	Protección de datos de prueba	Los datos de prueba se deben seleccionar, proteger y controlar cuidadosamente.
A.15.1.1	Política de seguridad de la información para las relaciones con proveedores	Los requisitos de seguridad de la información para mitigar los riesgos asociados con el acceso de proveedores a los activos de la organización se deben acordar con éstos y se deben documentar.
A.15.1.2	Tratamiento de la seguridad dentro de los acuerdos con proveedores	Se deben establecer y acordar todos los requisitos de seguridad de la información pertinentes con cada proveedor que pueda tener acceso, procesar, almacenar, comunicar o suministrar componentes de infraestructura de TI para la información de la organización.
A.15.1.3	Cadena de suministro de tecnología de información y comunicación	Los acuerdos con proveedores deben incluir requisitos para tratar los riesgos de seguridad de la información asociados con la cadena de suministro de productos y servicios de tecnología de información y comunicación.
A.15.2.1	Seguimiento y revisión de los servicios de los proveedores	Las organizaciones deben hacer seguimiento, revisar y auditar con regularidad la prestación de servicios de los proveedores.
A.15.2.2	Gestión de cambios en los servicios de los proveedores	Se deben gestionar los cambios en el suministro de servicios por parte de los proveedores, incluido el mantenimiento y la mejora de las políticas, procedimientos y controles de seguridad de la

Núm.	Control	Descripción
		información existentes , teniendo en cuenta la criticidad de la información, sistemas y procesos del negocio involucrados, y la reevaluación de los riesgos.
A.16.1.1	Responsabilidades y procedimientos	Se deben establecer las responsabilidades y procedimientos de gestión para asegurar una respuesta rápida, eficaz y ordenada a los incidentes de seguridad de la información.
A.16.1.2	Reporte de eventos de seguridad de la información	Los eventos de seguridad de la información se deben informar a través de los canales de gestión apropiados, tan pronto como sea posible.
A.16.1.3	Reporte de debilidades de seguridad de la información	Se debe exigir a todos los empleados y contratistas que usan los servicios y sistemas de información de la organización, que observen y reporten cualquier debilidad de seguridad de la información observada o sospechada en los sistemas o servicios.
A.16.1.4	Evaluación de eventos de seguridad de la información y decisiones sobre ellos.	Los eventos de seguridad de la información se deben evaluar y se debe decidir si se van a clasificar como incidentes de seguridad de la información.
A.16.1.5	Respuesta a incidentes de seguridad de la información	Se debe dar respuesta a los incidentes de seguridad de la información de acuerdo con procedimientos documentados.
A.16.1.6	Aprendizaje obtenido de los incidentes de seguridad de la información	El conocimiento adquirido al analizar y resolver incidentes de seguridad de la información se debe usar para reducir la posibilidad o el impacto de incidentes futuros.
A.16.1.7	Recolección de evidencia	La organización debe definir y aplicar procedimientos para la identificación, recolección, adquisición y preservación de información que pueda servir como evidencia.
A.17.1.1	Planificación de la continuidad de la seguridad de la información	La organización debe determinar sus requisitos para la seguridad de la información y la continuidad de la gestión de la seguridad de la información en situaciones adversas, por ejemplo, durante una crisis o desastre.
A.17.1.2	Implementación de la continuidad de la seguridad de la información	La organización debe establecer, documentar, implementar y mantener procesos, procedimientos y controles para asegurar el nivel de continuidad requerido para la seguridad de la información durante una situación adversa.
A.17.1.3	Verificación, revisión y evaluación de la continuidad de la seguridad de la información	La organización debe verificar a intervalos regulares los controles de continuidad de la seguridad de la información establecidos e implementados, con el fin de asegurar que son válidos y eficaces durante situaciones adversas.
A.17.2.1	Disponibilidad de instalaciones de procesamiento de información.	Las instalaciones de procesamiento de información se deben implementar con redundancia suficiente para cumplir los requisitos de disponibilidad.
A.18.1.1	Identificación de la legislación aplicable y de los requisitos contractuales	Todos los requisitos estatutarios, reglamentarios y contractuales pertinentes y el enfoque de la organización para cumplirlos, se deben identificar y documentar explícitamente, y mantenerlos actualizados para cada sistema de información y para la organización
A.18.1.2	Derechos de propiedad intelectual	Se deben implementar procedimientos apropiados para asegurar el

Núm.	Control	Descripción
		cumplimiento de los requisitos legislativos, de reglamentación y contractuales relacionados con los derechos de propiedad intelectual y el uso de productos de software patentados.
A.18.1.3	Protección de registros	Los registros se deben proteger contra pérdida, destrucción, falsificación, acceso no autorizado y liberación no autorizada, de acuerdo con los requisitos legislativos, de reglamentación, contractuales y de negocio.
A.18.1.4	Privacidad y protección de información de datos personales	Se deben asegurar la privacidad y la protección de la información de datos personales, como se exige en la legislación y la reglamentación pertinentes, cuando sea aplicable.
A.18.1.5	Reglamentación de controles criptográficos	Se deben usar controles criptográficos, en cumplimiento de todos los acuerdos, legislación y reglamentación pertinentes.
A.18.2.1	Revisión independiente de la seguridad de la información	El enfoque de la organización para la gestión de la seguridad de la información y su implementación (es decir, los objetivos de control, los controles, las políticas, los procesos y los procedimientos para seguridad de la información) se deben revisar independientemente a intervalos planificados o cuando ocurran cambios significativos.
A.18.2.2	Cumplimiento con las políticas y normas de seguridad	Los directores deben revisar con regularidad el cumplimiento del procesamiento y procedimientos de información dentro de su área de responsabilidad, con las políticas y normas de seguridad apropiadas, y cualquier otro requisito de seguridad.
A.18.2.3	Revisión del cumplimiento técnico	Los sistemas de información se deben revisar periódicamente para determinar el cumplimiento con las políticas y normas de seguridad de la información.

Tabla 25. Anexo A. ISO 27001 - Objetivos de control y controles de referencia