ANEXO 4
LINEAMIENTOS PARA LA GESTIÓN DE RIESGOS DE SEGURIDAD DIGITAL EN ENTIDADES PÚBLICAS

REPÚBLICA DE COLOMBIA

MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES

VICEMINISTERIO DE ECONOMÍA DIGITAL

DIRECCIÓN DE GOBIERNO DIGITAL

MODELO DE GESTIÓN DE RIESGOS DE SEGURIDAD DIGITAL (MGRSD)

2018

Tabla de Contenido

1. GENERALIDADES 3
1.1 Derechos de autor 3
1.2 Objetivos 3
1.2.1 Objetivo general 3
1.2.2 Objetivos específicos 4
1.3 Alcance del documento 4
1.4 Glosario 4
2. SIGLAS Y ABREVIACIONES 5
3. INTERACCIÓN DEL MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN (MSPI) CON EL MODELO NACIONAL DE GESTIÓN DE RIESGOS DE SEGURIDAD DIGITAL (MGRSD) 6
4. GESTIÓN DE RIESGOS DE SEGURIDAD DIGITAL PARA ENTIDADES PÚBLICAS 8
4.1 Fase 1. Planificación de la GRSD 8
4.1.1 Contexto interno y externo de la entidad pública 8
4.1.2 Alcance para aplicar la gestión de riesgos de seguridad digital 10
4.1.3 Alineación o creación de la política de gestión de riesgo de seguridad digital. 10
4.1.4 Definición de roles y responsabilidades 10
4.1.5 Definición de recursos para la Gestión de riesgos de seguridad digital 11
4.1.6 Identificación de activos de seguridad digital 11
4.1.7 Identificar los riesgos inherentes de seguridad digital 19
4.1.8 Identificación y evaluación de los controles existentes 23
4.1.9 Tratamiento de los riesgos de seguridad digital 24
4.1.10 Planes de Tratamiento de Riesgos de Seguridad Digital e Indicadores para la Gestión del Riesgo 24
4.2 Fase 2. Ejecución 24
4.3 Fase 3. Monitoreo y revisión 25
4.3.1 Registro y reporte de incidentes de seguridad digital 25
4.3.2 Reporte de la gestión del riesgo de seguridad digital al interior de la entidad pública 26
4.3.3 Reporte de la gestión del riesgo de seguridad digital a autoridades o entidades especiales 26
4.3.4 Auditorías internas y externas 27
4.3.5 Medición del desempeño 28
4.4 Fase 4. Mejoramiento continuo de la gestión del riesgo de seguridad digital 28
5. CONTROLES DE REFERENCIA PARA LA MITIGACIÓN DE RIESGOS DE SEGURIDAD DIGITAL 29

1. GENERALIDADES

1.1 Derechos de autor

Todas las referencias a los documentos del Modelo de Gestión de Riesgos de Seguridad Digital -MGRSD- son derechos reservados por parte del Ministerio de Tecnologías de la Información y las Comunicaciones -MINTIC-.

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

En consecuencia, el MINTIC goza de los derechos de autor[1] establecidos en la ley 23 de 1982 y demás normas concordantes y complementarias, respecto de los documentos del MGRSD y su contenido.

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

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

1.2 Objetivos

1.2.1 Objetivo general

[1] **Ley 1520 de 2012.** Artículo 5. El artículo 12 de la Ley 23 de 1982 quedará así: "Artículo 12. El autor o, en su caso, sus derechohabientes, tienen sobre las obras literarias y artísticas el derecho exclusivo de autorizar, o prohibir: a) La reproducción de la obra bajo cualquier manera o forma, permanente o temporal, mediante cualquier procedimiento incluyendo el almacenamiento temporal en forma electrónica.
Ley 1450 de 2011. Artículo 28. Propiedad intelectual obras en cumplimiento de un contrato de prestación de servicios o de un contrato de trabajo. El artículo 20 de la ley 23 de 1982 quedará así: "Artículo 20. En las obras creadas para una persona natural o jurídica en cumplimento de un contrato de prestación de servicios o de un contrato de trabajo, el autor es el titular originario de los derechos patrimoniales y morales; pero se presume, salvo pacto en contrario, que los derechos patrimoniales sobre la obra han sido transferidos al en cargante o al empleador, según sea el caso, en la medida necesaria para el ejercicio de sus actividades habituales en la época de creación de la obra. Para que opere esta presunción se requiere que el contrato conste por escrito. El titular de las obras de acuerdo a este artículo podrá intentar directamente o por intermedia persona acciones preservativas contra actos violatorios de los derechos morales informando previamente al autor o autores para evitar duplicidad de acciones".
Ley 23 de 1982. Artículo 30. El autor tendrá sobre su obra un derecho perpetuo, inalienable, e irrenunciable para: a) Reivindicar en todo tiempo la paternidad de su obra y, en especial, para que se indique su nombre o seudónimo cuando se realice cualquiera de los actos mencionados en el artículo 12 de esta ley.

El objetivo principal de este anexo es orientar a todas las entidades del Gobierno nacional, territoriales y sector público en la implementación de la gestión de riesgos de seguridad digital basada en la definición metodológica del MGRSD para, entre otros aspectos, incrementar la confianza de las múltiples partes interesadas en el uso del entorno digital y del aseguramiento de los activos de información en cada entidad pública.

1.2.2 Objetivos específicos

a. Otorgar una herramienta de orientación para la ejecución de la GRSD en las entidades de Gobierno nacional, territoriales y del sector público en general.
b. Estandarizar el proceso de gestión de riesgos de seguridad digital en las entidades del Gobierno nacional, territoriales y del sector público en general.
c. Generar mecanismos para que las entidades del Gobierno nacional, territoriales y del sector público en general puedan establecer los elementos para identificar, analizar, valorar y tratar los riesgos, amenazas y vulnerabilidades del entorno digital.
d. Proponer estrategias para la ejecución de planes de acción para mitigar los riesgos generados en el entorno digital.

1.3 Alcance del documento

Este documento complementa y profundiza lo expuesto en la ***Guía para la Administración del Riesgo en la Gestión, Corrupción y Seguridad Digital. Diseño de Controles en Entidades Públicas,*** emitida conjuntamente entre el Departamento Administrativo de la Función Pública y la Secretaría de Transparencia de la Presidencia de la República, específicamente en las secciones de Análisis del contexto (con un enfoque hacia el entorno digital), identificación de activos, catálogos de amenazas y vulnerabilidades para el análisis de riesgos de seguridad digital, controles para la mitigación de los riesgos de seguridad digital, el reporte de riesgos de seguridad digital y otros aspectos adicionales para llevar a cabo una gestión del riesgo de seguridad digital adecuada.

1.4 Glosario

Ver Documento **Modelo de Gestión de Riesgos de Seguridad Digital (MGRSD).**

2. SIGLAS Y ABREVIACIONES

Abreviatura	Significado
CCOC	Comando Conjunto Cibernético del Comando General de las Fuerzas Militares de Colombia
CCP	Centro Cibernético Policial de la Policía Nacional de Colombia
ColCERT	Grupo de Respuesta a Emergencias Cibernéticas de Colombia
CONPES	Consejo Nacional de Política Económica y Social de Colombia
CSIRT	Equipos de Respuestas ante Incidentes de Seguridad
MGRSD	Modelo Nacional de Gestión de Riesgos de Seguridad Digital
MINTIC	Ministerio de Tecnologías de la Información y las Comunicaciones
MIPG	Modelo Integrado de Planeación y Gestión
MSPI	Modelo de Seguridad y Privacidad de la Información
GRSD	Gestión de Riesgos de Seguridad Digital
ICC	Infraestructuras Críticas Cibernéticas
TI	Tecnologías de Información
TIC	Tecnologías de la Información y las Comunicaciones
TO	Tecnologías de Operación

3. INTERACCIÓN DEL MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN (MSPI) CON EL MODELO NACIONAL DE GESTIÓN DE RIESGOS DE SEGURIDAD DIGITAL (MGRSD)

Conforme lo indica el ámbito de aplicación del Decreto 1078 de 2015 respecto a la estrategia de Gobierno Digital -GD-, las entidades públicas deben realizar la implementación del Modelo de Seguridad y Privacidad de la Información -MSPI- con el objetivo de conformar un Sistema de Gestión de Seguridad de la Información al interior de la entidad.

El MSPI integra en cada una de sus fases tareas asociadas a la gestión de riesgos de seguridad digital, ya que esta práctica constituye su base fundamental. La guía para la gestión del riesgo de función pública, junto con el presente Anexo, llevarán a cumplir dichas tareas de gestión de riesgo de seguridad digital requeridas en el **MSPI**.

En esencia, la interacción entre ambos modelos puede resumirse de la siguiente manera:

1. Las actividades de identificación de activos, identificación, análisis, evaluación y tratamiento de los riesgos se alinean con la fase de PLANIFICACIÓN del **MSPI**.
2. Las actividades de implementación de los planes de tratamiento de riesgos se alinean con la fase de IMPLEMENTACIÓN del **MSPI**.
3. Las actividades de monitoreo y revisión, revisión de los riesgos residuales, efectividad de los planes de tratamiento o los controles implementados y auditorías se alinean con la fase de MEDICIÓN DEL DESEMPEÑO del **MSPI**.
4. Las actividades de MEJORAMIENTO CONTINUO en ambos modelos son similares y trabajan simultáneamente, ya que dependerán de las fases de Medición del Desempeño para identificar aspectos a mejorar en la aplicación de ambos Modelos.

A continuación se ilustra en que acciones del MPSI se tendrá interacción directa con el Modelo de Gestión de Riesgos de Seguridad Digital (MGRSD):

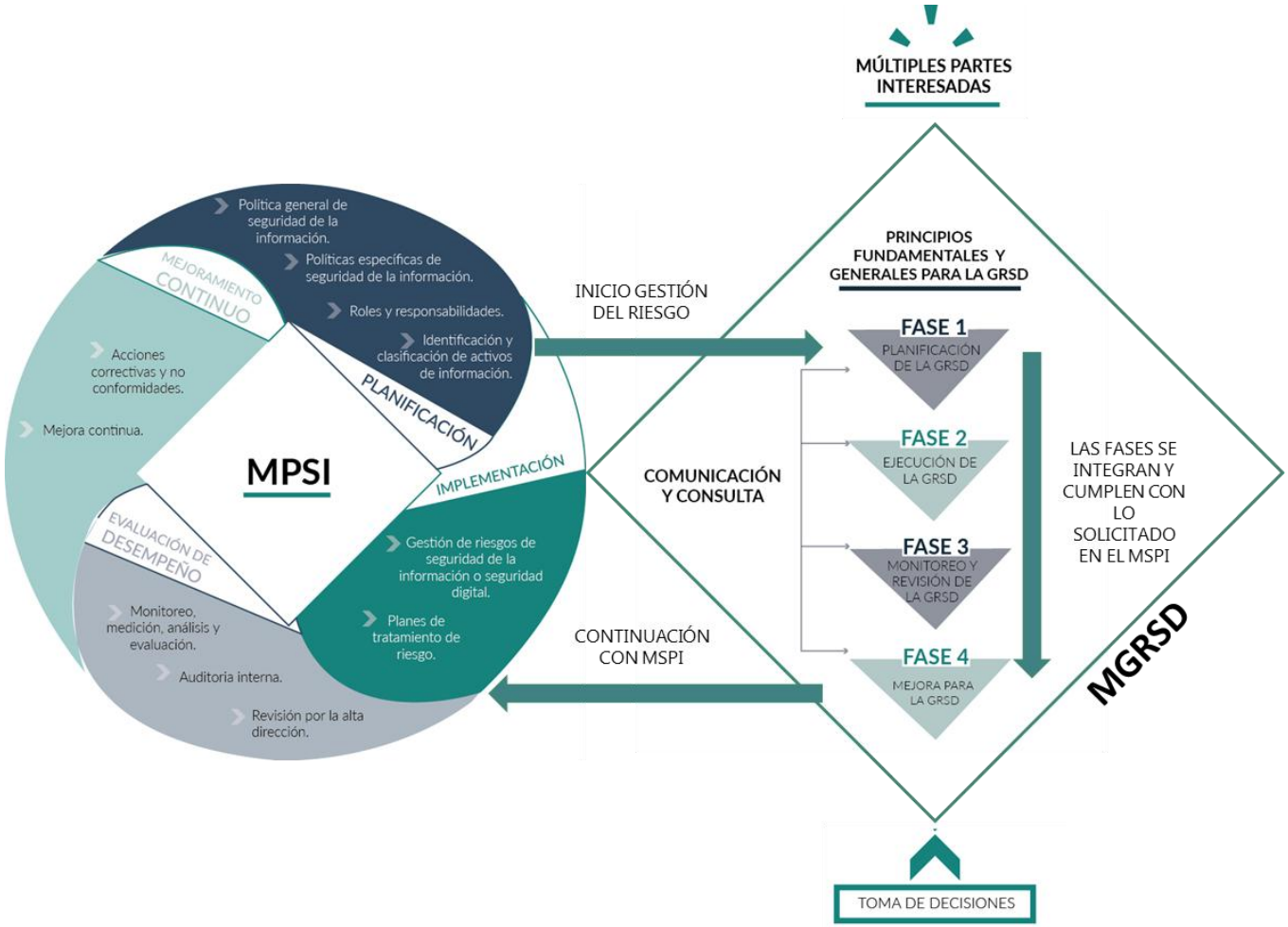

Imagen 1. Interacción entre el MSPI y el MGRSD.
Fuente: Ministerio de Tecnologías de la Información y las Comunicaciones

4. GESTIÓN DE RIESGOS DE SEGURIDAD DIGITAL PARA ENTIDADES PÚBLICAS

En los siguientes numerales se indican los aspectos complementarios a lo expuesto en el documento "*Guía para la Administración del Riesgo en la Gestión, Corrupción y Seguridad Digital. Diseño de Controles en Entidades Públicas"* [2], donde se incluyen los riesgos de seguridad digital.

4.1 Fase 1. Planificación de la GRSD

La fase de planificación comprende todo lo expuesto en los **Pasos 1, 2 y 3** de la *Guía para la Administración de los Riesgo de Gestión, Corrupción y Seguridad Digital y el Diseño de Controles en Entidades Públicas, emitida por la Función Pública*, es decir, comprende todo lo relacionado con las siguientes actividades:

- Definición del contexto interno, externo y de los procesos de la entidad pública.
- Definición de la política de administración de riesgo.
- Designación de roles y responsabilidades.
- Definición de criterios de probabilidad, impacto y zonas de riesgo aceptable.
- Identificación de activos.
- Identificación de riesgos.
- Valoración de riesgos.
- Definición del tratamiento de los riesgos.

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

4.1.1 Contexto interno y externo de la entidad pública

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

4.1.1.1 Establecimiento del contexto externo

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

[2] LINK FUNCIÓN PÚBLICA (PENDIENTE)

CONTEXTO EXTERNO
• Clientes, proveedores de servicios y empresas que sean competencia directa y/o se relacionen con la misión de la entidad pública analizada. • Normativas o aspectos jurídicos que apliquen directa o indirectamente a la entidad pública; ejemplo, la ley 1581 de 2012 o la ley 1712 de 2014, circulares o regulaciones emitidas por superintendencias o ministerios, como el decreto 1078 de 2015 o el decreto 1499 de 2017. • Dependencias económicas y financieras por parte de otras empresas. • Entorno cultural. • Cualquier otro factor externo de tipo internacional, nacional (gobierno), regional o local. • Cantidad de ciudadanos a los cuales la entidad pública brinda servicios a través del entorno digital como trámites a través de páginas web. • Aspectos externos que pueden verse afectados con los riesgos de seguridad digital, tales como el ambiente social, económico y ambiental que tengan alguna relación con las operaciones asociadas a la entidad pública.

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

4.1.1.2 Establecimiento del contexto interno

El contexto interno considera factores que impactan directamente a:

- La entidad pública, en general, su organización, sistemas de información o servicios, reglamentación interna, número de sedes, empleados, entre otros aspectos.
- Cada uno de los procesos sobre los cuales están soportadas sus operaciones.

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

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

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

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

4.1.2 Alcance para aplicar la gestión de riesgos de seguridad digital

El alcance de la administración del riesgo de seguridad digital debe ser extensible y aplicable a los **procesos** de la entidad pública que indiquen los criterios diferenciales del **Modelo de Seguridad y Privacidad de la Información**[3], habilitador de la Estrategia de Gobierno Digital expedida por el MINTIC.

4.1.3 Alineación o creación de la política de gestión de riesgo de seguridad digital.

Es necesario que la entidad pública establezca una política de gestión de riesgo integral, donde se incluya el compromiso en la gestión de los **riesgos de seguridad digital** en todos sus niveles. Esta debe crearse como lo indica la *Guía de administración del riesgo de gestión* del DAFP en el **Paso 1,** incluyendo la gestión de riesgos de seguridad digital. Esta actividad es responsabilidad de la **Línea estratégica** dispuesta por el MIPG.

4.1.4 Definición de roles y responsabilidades

Además de las líneas de defensa y las responsabilidades designadas en la "*Guía para la Administración del Riesgo en la Gestión, Corrupción y Seguridad Digital. Diseño de Controles en Entidades Públicas"* del DAFP, es necesario indicar o profundizar en las responsabilidades que deberá tener designadas el Responsable de Seguridad Digital:

Responsable de Seguridad Digital

Cada entidad pública **debe designar un responsable de Seguridad Digital** que también es el responsable de la Seguridad de la Información, el cual debe pertenecer a un área que haga parte de la Alta Dirección o Línea Estratégica y las responsabilidades que deberá cumplir respecto a la gestión del riesgo de seguridad digital serán las siguientes:

RESPONSABLE DE SEGURIDAD DIGITAL
Definir el procedimiento para la Identificación y Valoración de Activos.
Adoptar o adecuar el procedimiento formal para la gestión de riesgos de seguridad digital (Identificación, Análisis, Evaluación y Tratamiento).
Asesorar y acompañar a la primera línea de defensa en la realización de la gestión de riesgos de seguridad digital y en la recomendación de controles para mitigar los riesgos.
Apoyar en el seguimiento a los planes de tratamiento de riesgo definidos.
Informar a la línea estratégica sobre cualquier variación importante en los niveles o valoraciones de los riesgos de seguridad digital.

Fuente: Ministerio de Tecnologías de la Información y las Comunicaciones

[3] http://www.mintic.gov.co/gestionti/615/articles-5482_Modelo_de_Seguridad_Privacidad.pdf

Nota: Como complemento de esta actividad, la entidad pública debe tomar como referencia lo definido en la **Guía Roles y responsabilidades del MSPI**[4] de la Estrategia de Gobierno Digital del MINTIC, en complemento a lo anterior.

4.1.5 Definición de recursos para la Gestión de riesgos de seguridad digital

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

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

- Personal capacitado e idóneo para la gestión del riesgo de seguridad digital.
- Recursos económicos para la implementación de controles de mitigación de riesgos (con base al análisis de riesgo realizado).
- Recursos para los aspectos de mejora continua, monitoreo y auditorías.

4.1.6 Identificación de activos de seguridad digital

Un activo es cualquier elemento que tenga valor para la organización, sin embargo, en el contexto de seguridad digital son activos elementos tales como aplicaciones de la entidad pública, servicios Web, redes, información física o digital, Tecnologías de la Información -TI- o Tecnologías de la Operación -TO-) que utiliza la organización para su funcionamiento.

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

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

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

[4] http://www.mintic.gov.co/gestionti/615/w3-propertyvalue-7275.html Guía # 4 - Roles y Responsabilidades

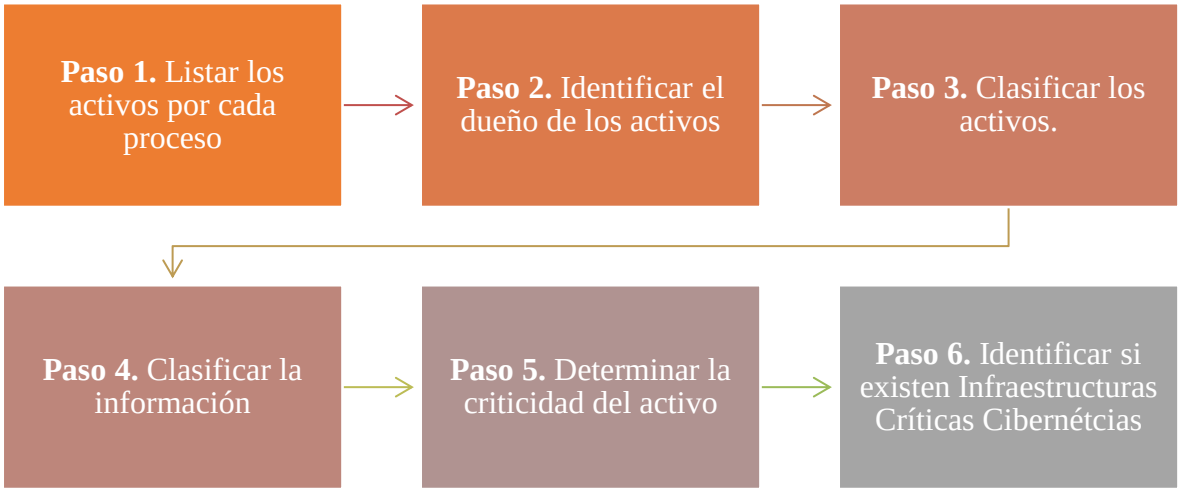

Imagen 2. Pasos para la identificación y valoración de activos.
Fuente: Ministerio de Tecnologías de la Información y las Comunicaciones

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

Paso 1. Listar los activos por cada proceso:

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

Ejemplo:

PROCESO	ACTIVO	DESCRIPCION
Gestión Financiera	Base de datos de nómina	Base de datos con información de nómina de la entidad
Gestión Financiera	Aplicativo de Nómina	Servidor web que contiene el front office de la entidad
Gestión Financiera	Cuentas de Cobro	Formatos de cobro diligenciados

Fuente: Ministerio de Tecnologías de la Información y las Comunicaciones

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

Paso 2. Identificar el dueño de los activos:

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

Ejemplo:

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

Fuente: Ministerio de Tecnologías de la Información y las Comunicaciones

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

Paso 3. Clasificar los activos:

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

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

Tabla 4. Tipología de Activos:

Tipo de activo	Descripción
Información	Información almacenada en formatos físicos (papel, carpetas, CD, DVD) o en formatos digitales o electrónicos (ficheros en bases de datos, correos electrónicos, archivos o servidores), teniendo en cuenta lo anterior, se puede distinguir como información: Contratos, acuerdos de confidencialidad, manuales de usuario, procedimientos operativos o de soporte, planes para la continuidad del negocio, registros contables, estados financieros, archivos ofimáticos, documentos y registros del sistema integrado de gestión, bases de datos con información personal o con información relevante para algún proceso (bases de datos de nóminas, estados financieros) entre otros.
Software	Activo informático lógico como programas, herramientas ofimáticas o sistemas lógicos para la ejecución de las actividades

Hardware	Equipos físicos de cómputo y de comunicaciones como, servidores, biométricos que por su criticidad son considerados activos de información
Servicios	Servicio brindado por parte de la entidad para el apoyo de las actividades de los procesos, tales como: Servicios WEB, intranet, CRM, ERP, Portales organizacionales, Aplicaciones entre otros (Pueden estar compuestos por hardware y software)
Intangibles	Se consideran intangibles aquellos activos inmateriales que otorgan a la entidad una ventaja competitiva relevante, uno de ellos es la imagen corporativa, reputación o el good will, entre otros
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

Fuente: Ministerio de Tecnologías de la Información y las Comunicaciones

Ejemplo:

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

Fuente: Ministerio de Tecnologías de la Información y las Comunicaciones

Paso 4. Clasificar la información:

Realizar la clasificación de la información conforme lo indican las l**eyes 1712 de 2014, 1581 de 2012, el Modelo de Seguridad y Privacidad en su Guía de Gestión de Activos, el dominio 8 del Anexo A de la norma ISO27001:2013 y demás normatividad aplicable.** Esto adicionalmente ayudará a dilucidar la importancia de los activos de información en el siguiente Paso 5.

Ejemplo:

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

ACTIVO	TIPO DE ACTIVO	Ley 1712 de 2014	Ley 1581 de 2012
			personales

Fuente: Ministerio de Tecnologías de la Información y las Comunicaciones

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

Paso 5. Determinar la criticidad del activo (Valoración del Activo):

Ahora la entidad pública debe evaluar la criticidad de los activos, a través de preguntas que le permitan determinar el grado de importancia de cada uno, para posteriormente, durante el análisis de riesgos tener presente esta criticidad para hacer una valoración adecuada de cada caso.

En este paso la entidad pública debe definir las escalas (que significa criticidad ALTA, MEDIA y BAJA) para valorar los activos respecto a la confidencialidad, integridad y disponibilidad e identificar su nivel de importancia o criticidad para el proceso. Para definir estas escalas puede tomar como referencia la *Guía de Gestión de Activos del Modelo de Seguridad y Privacidad de la Información* (MSPI)[5], estas escalas deberán ser definidas y documentadas en un procedimiento de gestión de activos que debe ser aprobado por parte de la línea estratégica de la entidad pública.

ACTIVO	TIPO DE ACTIVO	Criticidad respecto a su confidencialidad	Criticidad respecto a completitud o integridad	Criticidad respecto a su disponibilidad	Nivel de Criticidad
Base de datos de nómina	Información	ALTA	ALTA	ALTA	ALTA
Aplicativo de Nómina	Información	BAJA	MEDIA	BAJA	BAJA
Cuentas de Cobro	Información	BAJA	MEDIA	BAJA	BAJA

Fuente: Ministerio de Tecnologías de la Información y las Comunicaciones

[5] http://www.mintic.gov.co/gestionti/615/w3-propertyvalue-7275.html - Guía #5 Gestión Clasificación de Activos

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

Paso 6. Identificar si existen Infraestructuras Críticas Cibernéticas -ICC-

Se invita a que las entidades públicas identifiquen y reporten a las instnacias y autoridades respectivas en el Gobierno nacional si poseen ICC. Un activo es considerado infraestructura crítica si su impacto o afectación podría superar alguno de los siguientes 3 criterios:

IMPACTO SOCIAL (0,5%) de Población Nacional	IMPACTO ECONÓMICO PIB de un Día o 0,123% del PIB Anual	IMPACTO AMBIENTAL
250.000 personas	$464.619.736	3 años en recuperación

Fuente: Tomado de Comando Conjunto Cibernético (CCOC), Comando General Fuerzas Militares de Colombia. *Guía para la Identificación de Infraestructura Crítica Cibernética (ICC) de Colombia Primera Edición.*

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

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

Proceso	Activo	Descripción	Dueño del Activo	Tipo de Activo	Clasificación de información (Ley 1581 de 2012 / Ley 1712 de 2014)	Criticidad del Activo (Adicionar las preguntas para determinarla)
Ver Paso 1	Ver Paso 1	Ver Paso 1	Ver Paso 2	Ver Paso 3	Ver Paso 4	Ver Paso 5
Gestión Financiera	Base de datos de nómina	Base de datos con información de nómina de la entidad	Jefe oficina de nómina	Información	Ley 1712 Información reservada Ley 1581 No contiene datos personales Otras normas que apliquen	ALTA

Fuente: Ministerio de Tecnologías de la Información y las Comunicaciones

Recomendaciones adicionales para la identificación de activos:

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

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

Nota: adicional a lo anterior, la **Guía para la gestión y clasificación de activos del Modelo de Seguridad y Privacidad de la Información** de la Estrategia Gobierno Digital de MINTIC, capítulo 7, también brinda una orientación para clasificar los activos de información.

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

4.1.7 Identificar los riesgos inherentes de seguridad digital

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

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

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

Identificación de Amenazas:

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

- Deliberadas (D), fortuito (F) o ambientales (A).

Tabla 5. Tabla de amenazas comunes

Tipo	Amenaza	Origen
Daño físico	Fuego	F, D, A
	Agua	F, D, A
Eventos naturales	Fenómenos climáticos	E
	Fenómenos sísmicos	E
Pérdidas de los servicios esenciales	Fallas en el sistema de suministro de agua	E
	Fallas en el suministro de aire acondicionado	F, D, A
Perturbación debida a la radiación	Radiación electromagnética	F, D, A
	Radiación térmica	F, D, A
Compromiso de la información	Interceptación de servicios de señales de interferencia comprometida	D
	Espionaje remoto	D
Fallas técnicas	Fallas del equipo	D, F
	Mal funcionamiento del equipo	D, F
	Saturación del sistema de información	D, F
	Mal funcionamiento del software	D, F
	Incumplimiento en el mantenimiento del sistema de información	D, F
Acciones no autorizadas	Uso no autorizado del equipo	D, F
	Copia fraudulenta del software	D, F
Compromiso de las funciones	Error en el uso o abuso de derechos	D, F
	Falsificación de derechos	D

Fuente: ISO/IEC 27005:2009

- Amenazas dirigidas por el hombre: empleados con o sin intención, proveedores y piratas informáticos, entre otros.

Tabla 6. Tabla de amenazas dirigida por el hombre

Fuente de amenaza	Motivación	Acciones amenazantes
Pirata informático, intruso ilegal	Reto Ego	Piratería Ingeniería social
Criminal de la computación	Destrucción de la información Divulgación ilegal de la información	Crimen por computador Acto fraudulento
Terrorismo	Chantaje Destrucción	Ataques contra el sistema DDoS Penetración en el sistema
Espionaje industrial (inteligencia, empresas, gobiernos extranjeros, otros intereses)	Ventaja competitiva Espionaje económico	Ventaja de defensa Hurto de información
Intrusos (empleados con	Curiosidad	Asalto a un empleado

Fuente de amenaza	Motivación	Acciones amenazantes
entrenamiento deficiente, descontentos, malintencionados, negligentes, deshonestos o despedidos)	Ganancia monetaria	Chantaje

Fuente: ISO/IEC 27005:2009

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

Tabla 7. Tabla de Vulnerabilidades Comunes

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

Tipo	Vulnerabilidades
	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 (esto aplica para muchas actividades que la entidad no tenga documentadas y formalizadas como uso aceptable de activos, control de cambios, valoración de riesgos, escritorio y pantalla limpia entre otros)

Fuente: ISO/IEC 27005

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

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

Tabla 8. Tabla de Amenazas y Vulnerabilidades

Tipo de activo	Ejemplos de vulnerabilidades	Ejemplos de amenazas
Hardware	Almacenamiento de medios sin protección	Hurto de medios o documentos
Software	Ausencia de parches de seguridad	Abuso de los derechos
Red	Líneas de comunicación sin protección	Escucha encubierta
Información	Falta de controles de acceso físico	Hurto de información
Personal	Falta de capacitación en las herramientas	Error en el uso
Organización	Ausencia de políticas de seguridad	Abuso de los derechos

Fuente: Ministerio de Tecnologías de la Información y las Comunicaciones

Identificación del riesgo inherente de seguridad digital:

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

Adicionalmente, se debe identificar el **dueño del riesgo**, es decir, "*quien tiene que rendir cuentas sobre el riesgo o quien tiene la autoridad para gestionar el riesgo*"[6].

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

- **Lluvia de ideas:** mediante esta opción se busca animar a los participantes a que indiquen qué situaciones adversas asociadas al manejo de la información digital y los activos de información se pueden presentar o casos ocurridos que los participantes conozcan que se hayan dado en la entidad pública o en el sector. Deben existir un orden de la sesión, un líder y personas que ayuden con la captura de las memorias.
- **Juicio de expertos:** a través de este esquema se reúnen las personas con mayor conocimiento sobre la materia de análisis e indican cuáles aspectos negativos o riesgos de seguridad digital se pueden presentar. Para emplear esta técnica, se requiere disponer de una agenda con un orden de temas, establecer reglas claras y contar con la participación de un orientador o moderador, así como personas que tomen notas de los principales conceptos expuestos. Al finalizar, se retoman los principales riesgos identificados y se procede a hacer una valoración
- **Análisis de escenarios:** en este esquema también se busca que un grupo de personas asociadas al proceso determinen situaciones potenciales que pueden llegar a presentarse: explosión de un pozo, sobrecarga de un nodo, pérdida de control de una unidad operada remotamente; y con base en estas posibilidades, se determina qué puede llegar a suceder, desde la perspectiva digital, a los activos de información y las consecuencias de la afectación.
- **Otras técnicas que pueden ser empleadas son**: entrevistas estructuradas, encuestas o listas de chequeo.

Posterior a la identificación de los riesgos de seguridad digital con sus respectivas amenazas y vulnerabilidades enunciadas en este documento, se deberá continuar con el **Paso 3. Valoración del Riesgo, de la "***Guía para la Administración del Riesgo en la Gestión, Corrupción y Seguridad Digital. Diseño de Controles en Entidades Públicas***"** del DAFP.

4.1.8 Identificación y evaluación de los controles existentes

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

[6] GTC 137 Gestión del Riesgo. Vocabulario

Nota: Para determinar si existen uno o varios controles asociados a los riesgos inherentes identificados se puede consultar la sección **4. OBJETIVOS DE CONTROL Y CONTROLES DE REFERENCIA** (*Tomados del Anexo A de la Norma ISO/IEC 27001:2013*) como un insumo base y determinar si ya posee alguno de los controles orientados a seguridad digital que están enunciados en dicho anexo.

4.1.9 Tratamiento de los riesgos de seguridad digital

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

El tratamiento de los riesgos es un proceso cíclico, el cual involucra una selección de opciones para modificarlos, por lo tanto, la entidad pública puede tener en cuenta las opciones planteadas en la *"Guía para la Administración del Riesgo en la Gestión, Corrupción y Seguridad Digital. Diseño de Controles en Entidades Públicas"* del DAFP**: Evitar, aceptar, compartir o mitigar el riesgo.**

Importante:
Si la entidad pública decide **mitigar o tratar el riesgo** mediante la selección de controles que permitan disminuir la probabilidad o el impacto del riesgo, deberá tener en cuenta la **Sección 4. OBJETIVOS DE CONTROL Y CONTROLES DE REFERENCIA**, basados en la norma ISO/IEC 27001:2013 en su Anexo A, como un insumo base para mitigar los riesgos de seguridad digital, sin embargo, la entidad pública puede implementar nuevos controles de seguridad que no estén incluidos dentro del Anexo, siempre y cuando sean efectivos y eficaces para disminuir la probabilidad o el impacto del riesgo.

4.1.10 Planes de Tratamiento de Riesgos de Seguridad Digital e Indicadores para la Gestión del Riesgo

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

4.2 Fase 2. Ejecución

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

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

El responsable de seguridad digital deberá supervisar y acompañar el proceso de implementación de los planes de tratamiento, verificando que los responsables de los planes

(**Primer Línea de Defensa** y la **Oficina de Tecnologías de la Información -TI-** generalmente) ejecuten las tareas en los tiempos pactados y que los recursos se estén ejecutando de acuerdo con lo planeado.

4.3 Fase 3. Monitoreo y revisión

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

- Realizar seguimiento y monitoreo al plan de acción en la etapa de implementación y finalización de los planes de acción.
- Revisar periódicamente las actividades de control para determinar su relevancia y actualizarlas de ser necesario.
- Realizar monitoreo de los riesgos y controles tecnológicos.
- Efectuar la evaluación del plan de acción y realizar nuevamente la valoración de los riesgos de seguridad digital para verificar su efectividad.
- Verificar que los controles están diseñados e implementados de manera efectiva y operen como se pretende para controlar los riesgos.
- Suministrar recomendaciones para mejorar la eficiencia y eficacia de los controles.

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

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

4.3.1 Registro y reporte de incidentes de seguridad digital

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

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

Nota: El reporte de incidentes de seguridad de la información a terceros (entes de control, reguladores, superintendencias, instancias o autoridades en la materia, entre otros), **no es la misionalidad del presente documento**, sin embargo, se recomienda realizar dichos reportes conforme lo estipulan los entes o las buenas prácticas en seguridad digital.

4.3.2 Reporte de la gestión del riesgo de seguridad digital al interior de la entidad pública

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

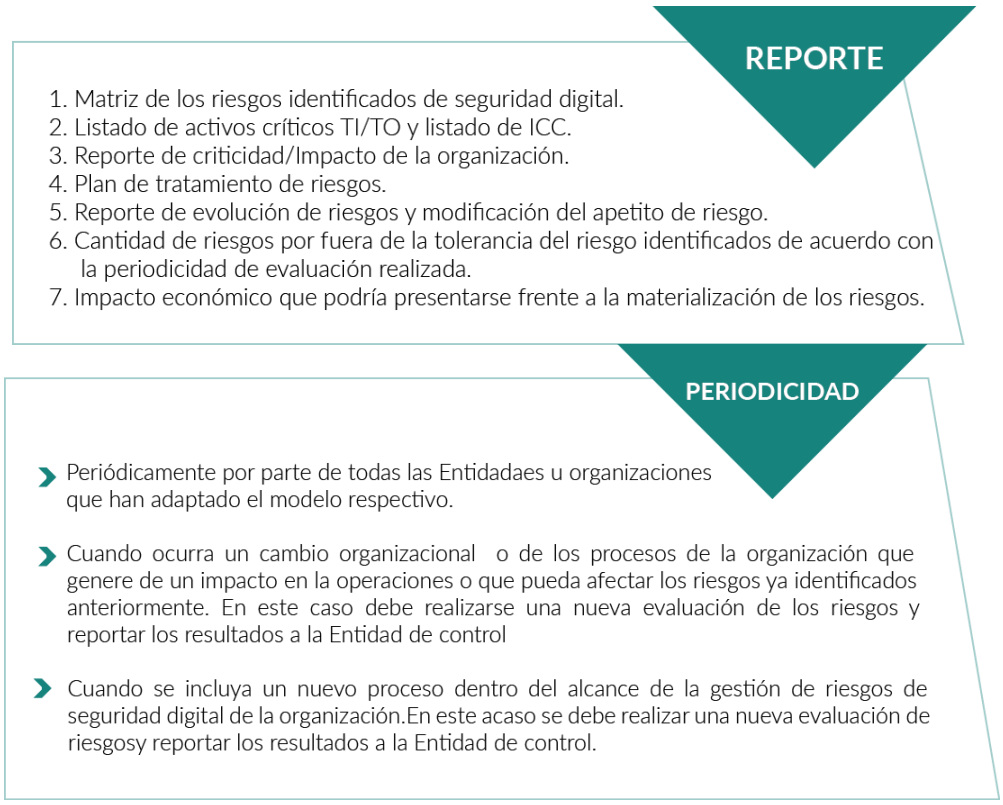

Imagen 3. Reportes de información por parte de la entidad.
Fuente: Ministerio de Tecnologías de la Información y las Comunicaciones

4.3.3 Reporte de la gestión del riesgo de seguridad digital a autoridades o entidades especiales

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

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

Información por consolidar para generar el reporte de información:

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

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

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

Reportes relacionados con Infraestructuras Críticas Cibernéticas, cuando aplique:

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

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

4.3.4 Auditorías internas y externas

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

4.3.5 Medición del desempeño

La entidad pública debe utilizar medidas de desempeño (indicadores[7]) para la gestión de los riesgos de seguridad digital, las cuales deben reflejar el cumplimiento de los objetivos propuestos. Estas deben ser evaluadas periódicamente alineadas con la revisión por la línea estratégica.

4.4 Fase 4. Mejoramiento continuo de la gestión del riesgo de seguridad digital

La entidad pública debe garantizar la mejora continua de la gestión de riesgos de seguridad digital, por lo tanto, debe establecer que cuando existan hallazgos, falencias o incidentes de seguridad digital se debe mitigar el impacto de su existencia y tomar acciones para controlarlos y prevenirlos. Adicionalmente, se debe establecer y hacer frente a las consecuencias propias de la no conformidad que llegó a materializarse.

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

- Revisar y evaluar los hallazgos encontrados en las auditorías internas, otras auditorías e informes de los entes de control realizadas.
- Establecer las posibles causas y consecuencias del hallazgo.
- Determinar si existen otros hallazgos similares para establecer acciones correctivas y evitar así que se lleguen a materializar.
- Emprender acciones de revisión continua, que permitan gestionar el riesgo a tiempo, disminuir el impacto y la probabilidad de ocurrencia del riesgo detectado, así como la aparición de nuevos riesgos que puedan afectar el desempeño de la entidad pública o de los servicios que presta al ciudadano.

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

[7] Consultar en la ***Guía de Administración del Riesgo de Gestión, Corrupción y Seguridad Digital*** del DAFP – Sección **Indicadores - Gestión del Riesgo de Seguridad Digital**, para definir indicadores de seguimiento para la gestión del riesgo de seguridad digital.

5. CONTROLES DE REFERENCIA PARA LA MITIGACIÓN DE RIESGOS DE SEGURIDAD DIGITAL

Las entidades públicas podrán mitigar/tratar los riesgos de seguridad digital empleando los siguientes controles, tomados del *Anexo A del estándar ISO/IEC 27001:2013 y los dominios a los que pertenecen*, siempre y cuando se ajusten al análisis de riesgos.

El contenido de la tabla se puede interpretar de la siguiente manera:

A.X – Dominio
A.X.X – Objetivo de Control
A.X.X.X - Controles

A.5 Políticas de seguridad de la información		
A.5.1	**Directrices establecidas por la dirección para la seguridad de la información**	**Objetivo: Brindar orientación y apoyo por parte de la dirección, para la seguridad de la información de acuerdo con los requisitos del negocio y con las leyes y reglamentos pertinentes.**
A.5.1.1	Políticas para la seguridad de la información	Control: 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	Control: 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 continuas.
A.6 Organización de la seguridad de la información		
A.6.1	**Organización interna**	**Objetivo: Establecer un marco de referencia de gestión para iniciar y controlar la implementación y la operación de la seguridad de la información dentro de la organización.**
A.6.1.1	Roles y responsabilidades para la seguridad de información	Control: Se deberían definir y asignar todas las responsabilidades de la seguridad de la información.
A.6.1.2	Separación de deberes	Control: Los deberes y áreas de responsabilidad en conflicto se deberían 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	Control: Se deberían mantener los contactos apropiados con las autoridades pertinentes.
A.6.1.4	Contacto con grupos de interés especial	Control: Es conveniente 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	Control: La seguridad de la información se debería tratar en la gestión de proyectos, independientemente del tipo de proyecto.
A.6.2	**Dispositivos móviles y teletrabajo**	**Objetivo: Garantizar la seguridad del teletrabajo y el uso de dispositivos móviles.**
A.6.2.1	Política para dispositivos móviles	Control: Se deberían 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	Control: Se deberían 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 Seguridad de los recursos humanos	
A.7.1	**Antes de asumir el empleo**	**Objetivo: Asegurar que los empleados y contratistas comprenden sus responsabilidades y son idóneos en los roles para los que se consideran.**
A.7.1.1	Selección	Control: Las verificaciones de los antecedentes de todos los candidatos a un empleo se deberían llevar a cabo de acuerdo con las leyes, reglamentos y ética pertinentes, y deberían 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	Control: Los acuerdos contractuales con empleados y contratistas, deberían establecer sus responsabilidades y las de la organización en cuanto a la seguridad de la información.
A.7.2	**Durante la ejecución del empleo**	**Objetivo: Asegurarse de que los empleados y contratistas tomen conciencia de sus responsabilidades de seguridad de la información y las cumplan.**
A.7.2.1	Responsabilidades de la dirección	Control: La dirección debería 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	Control: Todos los empleados de la organización, y en donde sea pertinente, los contratistas, deberían recibir la educación y la formación en toma de conciencia apropiada, y actualizaciones regulares sobre las políticas y procedimientos pertinentes para su cargo.
A.7.2.3	Proceso disciplinario	Control: Se debería contar con un proceso disciplinario formal el cual debería ser comunicado, para emprender acciones contra empleados que hayan cometido una violación a la seguridad de la información.
A.7.3	**Terminación o cambio de empleo**	**Objetivo: Proteger los intereses de la organización como parte del proceso de cambio o terminación del contrato.**
A.7.3.1	Terminación o cambio de responsabilidades de empleo	Control: Las responsabilidades y los deberes de seguridad de la información que permanecen validos después de la terminación o cambio de contrato se deberían definir, comunicar al empleado o contratista y se deberían hacer cumplir.
	A.8 Gestión de activos	
A.8.1	**Responsabilidad por los activos**	**Objetivo: Identificar los activos organizacionales y definir las responsabilidades de protección apropiadas.**
A.8.1.1	Inventario de activos	Control: Se deberían identificar los activos asociados con la información y las instalaciones de procesamiento de información, y se debería elaborar y mantener un inventario de estos activos.
A.8.1.2	Propiedad de los activos	Control: Los activos mantenidos en el inventario deberían tener un propietario.
A.8.1.3	Uso aceptable de los activos	Control: Se deberían 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	Control: Todos los empleados y usuarios de partes externas deberían devolver todos los activos de la organización que se encuentren a su cargo, al terminar su empleo, contrato o acuerdo.
A.8.2	**Clasificación de la información**	**Objetivo: Asegurar que la información recibe un nivel apropiado de protección, de acuerdo con su importancia para la organización.**
A.8.2.1	Clasificación de la información	Control: La información se debería 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	Control: Se debería 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	Control: Se deberían 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	**Manejo de Medios**	**Objetivo: Evitar la divulgación, la modificación, el retiro o la destrucción no autorizados de información almacenada en los medios.**
A.8.3.1	Gestión de medios removibles	Control: Se deberían 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	Control: Se debería disponer en forma segura de los medios cuando ya no se requieran, utilizando procedimientos formales.
A.8.3.3	Transferencia de medios físicos	Control: Los medios que contienen información se deberían proteger contra acceso no autorizado, uso indebido o corrupción durante el transporte.
	A.9 Control de acceso	
A.9.1	**Requisitos del negocio para control de acceso**	**Objetivo: Limitar el acceso a información y a instalaciones de procesamiento de información.**
A.9.1.1	Política de control de acceso	Control: Se debería 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	Política sobre el uso de los servicios de red	Control: Solo se debería permitir acceso de los usuarios a la red y a los servicios de red para los que hayan sido autorizados específicamente.
A.9.2	**Gestión de acceso de usuarios**	**Objetivo: Asegurar el acceso de los usuarios autorizados y evitar el acceso no autorizado a sistemas y servicios.**
A.9.2.1	Registro y cancelación del registro de usuarios	Control: Se debería 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	Control: Se debería implementar un proceso de suministro de acceso formal de usuarios para asignar o revocar los derechos de acceso a todo tipo de usuarios para todos los sistemas y servicios.
A.9.2.3	Gestión de derechos de acceso privilegiado	Control: Se debería restringir y controlar la asignación y uso de derechos de acceso privilegiado.
A.9.2.4	Gestión de información de autenticación secreta de usuarios	Control: La asignación de la información secreta se debería controlar por medio de un proceso de gestión formal.
A.9.2.5	Revisión de los derechos de acceso de usuarios	Control: Los propietarios de los activos deberían revisar los derechos de acceso de los usuarios, a intervalos regulares.
A.9.2.6	Retiro o ajuste de los derechos de acceso	Control: Los derechos de acceso de todos los empleados y de usuarios externos a la información y a las instalaciones de procesamiento de información se deberían retirar al terminar su empleo, contrato o acuerdo, o se deberían ajustar cuando se hagan cambios.
A.9.3	**Responsabilidades de los usuarios**	**Objetivo: Hacer que los usuarios rindan cuentas por la salvaguarda de su información de autenticación.**
A.9.3.1	Uso de la información de autenticación secreta	Control: Se debería exigir a los usuarios que cumplan las prácticas de la organización para el uso de información de autenticación secreta.

A.9.4	**Control de acceso a sistemas y aplicaciones**	**Objetivo: Evitar el acceso no autorizado a sistemas y aplicaciones.**
A.9.4.1	Restricción de acceso Información	Control: El acceso a la información y a las funciones de los sistemas de las aplicaciones se debería restringir de acuerdo con la política de control de acceso.
A.9.4.2	Procedimiento de ingreso seguro	Control: Cuando lo requiere la política de control de acceso, el acceso a sistemas y aplicaciones se debería controlar mediante un proceso de ingreso seguro.
A.9.4.3	Sistema de gestión de contraseñas	Control: Los sistemas de gestión de contraseñas deberían ser interactivos y deberían asegurar la calidad de las contraseñas.
A.9.4.4	Uso de programas utilitarios privilegiados	Control: Se debería restringir y controlar estrictamente el uso de programas utilitarios que pudieran tener capacidad de anular el sistema y los controles de las aplicaciones.
A.9.4.5	Control de acceso a códigos fuente de programas	Control: Se debería restringir el acceso a los códigos fuente de los programas.
A.10	**Criptografía**	
A.10.1	**Controles criptográficos**	**Objetivo: Asegurar el uso apropiado y eficaz de la criptografía para proteger la confidencialidad, la autenticidad y/o la integridad de la información.**
A.10.1.1	Política sobre el uso de controles criptográficos	Control: Se debería desarrollar e implementar una política sobre el uso de controles criptográficos para la protección de la información.
A.10.1.2	Gestión de llaves	Control: Se debería 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 Seguridad física y del entorno	
A.11.1	**Áreas seguras**	**Objetivo: Prevenir el acceso físico no autorizado, el daño y la interferencia a la información y a las instalaciones de procesamiento de información de la organización.**
A.11.1.1	Perímetro de seguridad física	Control: Se deberían definir y usar perímetros de seguridad, y usarlos para proteger áreas que contengan información sensible o critica, e instalaciones de manejo de información.
A.11.1.2	Controles físicos de entrada	Control: Las áreas seguras se deberían proteger mediante controles de entrada apropiados para asegurar que solamente se permite el acceso a personal autorizado.
A.11.1.3	Seguridad de oficinas, recintos e instalaciones	Control: Se debería diseñar y aplicar seguridad física a oficinas, recintos e instalaciones.
A.11.1.4	Protección contra amenazas externas y ambientales	Control: Se debería diseñar y aplicar protección física contra desastres naturales, ataques maliciosos o accidentes.
A.11.1.5	Trabajo en áreas seguras	Control: Se deberían diseñar y aplicar procedimientos para trabajo en áreas seguras.
A.11.1.6	Áreas de despacho y carga	Control: Se deberían 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.
A.11.2	**Equipos**	**Objetivo: Prevenir la perdida, daño, robo o compromiso de activos, y la interrupción de las operaciones de la organización.**
A.11.2.1	Ubicación y protección	Control: Los equipos deberían estar ubicados y protegidos para reducir los

	de los equipos	riesgos de amenazas y peligros del entorno, y las oportunidades para acceso no autorizado.
A.11.2.2	Servicios de suministro	Control: Los equipos se deberían proteger contra fallas de energía y otras interrupciones causadas por fallas en los servicios de suministro.
A.11.2.3	Seguridad del cableado	Control: El cableado de potencia y de telecomunicaciones que porta datos o soporta servicios de información debería estar protegido contra interceptación, interferencia o daño.
A.11.2.4	Mantenimiento de equipos	Control: Los equipos se deberían mantener correctamente para asegurar su disponibilidad e integridad continuas.
A.11.2.5	Retiro de activos	Control: Los equipos, información o software no se deberían retirar de su sitio sin autorización previa.
A.11.2.6	Seguridad de equipos y activos fuera de las instalaciones	Control: Se deberían 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	Control: Se deberían verificar todos los elementos de equipos que contengan medios de almacenamiento, para asegurar que cualquier dato sensible o software con licencia haya sido retirado o sobrescrito en forma segura antes de su disposición o reutilización.
A.11.2.8	Equipos de usuario desatendidos	Control: Los usuarios deberían asegurarse de que a los equipos desatendidos se les dé protección apropiada.
A.11.2.9	Política de escritorio limpio y pantalla limpia	Control: Se debería 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 Seguridad de las operaciones	
A.12.1	**Procedimientos operacionales y responsabilidades**	**Objetivo: Asegurar las operaciones correctas y seguras de las instalaciones de procesamiento de información.**
A.12.1.1	Procedimientos de operación documentados	Control: Los procedimientos de operación se deberían documentar y poner a disposición de todos los usuarios que los necesiten.
A.12.1.2	Gestión de cambios	Control: Se deberían 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	Control: Para asegurar el desempeño requerido del sistema se debería hacer seguimiento al uso de los recursos, hacer los ajustes, y hacer proyecciones de los requisitos sobre la capacidad futura.
A.12.1.4	Separación de los ambientes de desarrollo, pruebas y operación	Control: Se deberían 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	**Protección contra códigos maliciosos**	**Objetivo: Asegurarse de que la información y las instalaciones de procesamiento de información estén protegidas contra códigos maliciosos.**
A.12.2.1	Controles contra códigos maliciosos	Control: Se deberían 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	**Copias de respaldo**	**Objetivo: Proteger contra la perdida de datos.**
A.12.3.1	Respaldo de información	Control: Se deberían hacer copias de respaldo de la información, del software e imágenes de los sistemas, y ponerlas a prueba regularmente de acuerdo con una política de copias de respaldo aceptada.
A.12.4	**Registro y seguimiento**	**Objetivo: Registrar eventos y generar evidencia.**
A.12.4.1	Registro de eventos	Control: Se deberían 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	Control: Las instalaciones y la información de registro se deberían proteger contra alteración y acceso no autorizado.
A.12.4.3	Registros del administrador y del operador	Control: Las actividades del administrador y del operador del sistema se deberían registrar, y los registros se deberían proteger y revisar con regularidad.
A.12.4.4	sincronización de relojes	Control: Los relojes de todos los sistemas de procesamiento de información pertinentes dentro de una organización o ámbito de seguridad se deberían sincronizar con una única fuente de referencia de tiempo.
A.12.5	**Control de software operacional**	**Objetivo: Asegurar la integridad de los sistemas operacionales.**
A.12.5.1	Instalación de software en sistemas operativos	Control: Se deberían implementar procedimientos para controlar la instalación de software en sistemas operativos.
A.12.6	**Gestión de la vulnerabilidad técnica**	**Objetivo: Prevenir el aprovechamiento de las vulnerabilidades técnicas.**
A.12.6.1	Gestión de las vulnerabilidades técnicas	Control: Se debería 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	Control: Se deberían establecer e implementar las reglas para la instalación de software por parte de los usuarios.
A.12.7	**Consideraciones sobre auditorias de sistemas de información**	**Objetivo: Minimizar el impacto de las actividades de auditoría sobre los sistemas operacionales.**
A.12.7.1	Información controles de auditoría de sistemas	Control: Los requisitos y actividades de auditoría que involucran la verificación de los sistemas operativos se deberían planificar y acordar cuidadosamente para minimizar las interrupciones en los procesos del negocio.
	A.13 Seguridad de las comunicaciones	
A.13.1	**Gestión de la seguridad de las redes**	**Objetivo: Asegurar la protección de la información en las redes, y sus instalaciones de procesamiento de información de soporte.**
A.13.1.1	Controles de redes	Control: Las redes se deberían gestionar y controlar para proteger la información en sistemas y aplicaciones.
A.13.1.2	Seguridad de los servicios de red	Control: Se deberían 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 servicios de red, ya sea que los servicios se presten internamente o se contraten externamente.
A.13.1.3	Separación en las redes	Control: Los grupos de servicios de información, usuarios y sistemas de información se deberían separar en las redes.
A.13.2	**Transferencia de información**	**Objetivo: Mantener la seguridad de la información transferida dentro de una organización y con cualquier entidad externa.**
A.13.2.1	Políticas y procedimientos de transferencia de información	Control: Se debería contar con políticas, procedimientos y controles de transferencia formales para proteger la transferencia de información mediante el uso de todo tipo de instalaciones de comunicación.
A.13.2.2	Acuerdos sobre transferencia de información	Control: Los acuerdos deberían tener en cuenta la transferencia segura de información del negocio entre la organización y las partes externas.
A.13.2.3	Mensajería electrónica	Control: Se debería proteger adecuadamente la información incluida en la mensajería electrónica.

A.13.2.4	Acuerdos de confidencialidad o de no divulgación	Control: Se deberían 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 Adquisición, desarrollo y mantenimientos de sistemas		
A.14.1	**Requisitos de seguridad de los sistemas de información**	**Objetivo: Asegurar que la seguridad de la información sea una parte integral de los sistemas de información durante todo el ciclo de vida. Esto incluye también los requisitos para sistemas de información que prestan servicios en redes públicas.**
A.14.1.1	Análisis y especificación de requisitos de seguridad de la información	Control: Los requisitos relacionados con seguridad de la información se deberían 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 publicas	Control: La información involucrada en los servicios de aplicaciones que pasan sobre redes públicas se debería proteger de actividades fraudulentas, disputas contractuales y divulgación y modificación no autorizadas.
A.14.1.3	Protección de transacciones de los servicios de las aplicaciones	Control: La información involucrada en las transacciones de los servicios de las aplicaciones se debería proteger para evitar la transmisión incompleta, el enrutamiento errado, la alteración no autorizada de mensajes, la divulgación no autorizada, y la duplicación o reproducción de mensajes no autorizada.
A.14.2	**Seguridad en los procesos de desarrollo y soporte**	**Objetivo: Asegurar de que la seguridad de la información esté diseñada e implementada dentro del ciclo de vida de desarrollo de los sistemas de información.**
A.14.2.1	Política de desarrollo seguro	Control: Se deberían establecer y aplicar reglas para el desarrollo de software y de sistemas, a los desarrollos que se dan dentro de la organización.
A.14.2.2	Procedimientos de control de cambios en sistemas	Control: Los cambios a los sistemas dentro del ciclo de vida de desarrollo se deberían 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	Control: Cuando se cambian las plataformas de operación, se deberían revisar las aplicaciones críticas del negocio, y ponerlas 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	Control: Se deberían desalentar las modificaciones a los paquetes de software, que se deben limitar a los cambios necesarios, y todos los cambios se deberían controlar estrictamente.
A.14.2.5	Principios de construcción de sistemas seguros	Control: Se deberían 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	Control: Las organizaciones deberían establecer y proteger adecuadamente los ambientes de desarrollo seguros para las tareas de desarrollo e integración de sistemas que comprendan todo el ciclo de vida de desarrollo de sistemas.
A.14.2.7	Desarrollo contratado externamente	Control: La organización debería supervisar y hacer seguimiento de la actividad de desarrollo de sistemas contratados externamente.
A.14.2.8	Pruebas de seguridad de sistemas	Control: Durante el desarrollo se deberían llevar a cabo pruebas de funcionalidad de la seguridad.
A.14.2.9	Prueba de aceptación de sistemas	Control: Para los sistemas de información nuevos, actualizaciones y nuevas versiones, se deberían establecer programas de prueba para aceptación y criterios de aceptación relacionados.
A.14.3	**Datos de prueba**	**Objetivo: Asegurar la protección de los datos usados para pruebas.**
A.14.3.1	Protección de datos de prueba	Control: Los datos de ensayo se deberían seleccionar, proteger y controlar cuidadosamente.

A.15 Relación con los proveedores		
A.15.1	**Seguridad de la información en las relaciones con los proveedores**	**Objetivo: Asegurar la protección de los activos de la organización que sean accesibles a los proveedores.**
A.15.1.1	Política de seguridad de la información para las relaciones con proveedores	Control: Los requisitos de seguridad de la información para mitigar los riesgos asociados con el acceso de proveedores a los activos de la organización se deberían acordar con estos y se deberían documentar.
A.15.1.2	Tratamiento de la seguridad dentro de los acuerdos con proveedores	Control: Se deberían 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	Control: Los acuerdos con proveedores deberían 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	**Gestión de la prestación de servicios con los proveedores**	**Objetivo: Mantener el nivel acordado de seguridad de la información y de prestación del servicio en línea con los acuerdos con los proveedores.**
A.15.2.1	Seguimiento y revisión de los servicios de los proveedores	Las organizaciones deberían 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 proveedores	Control: Se deberían 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 información existentes , teniendo en cuenta la criticidad de la información, sistemas y procesos del negocio involucrados, y la revaloración de los riesgos.
A.16 Gestión de incidentes de seguridad de la información		
A.16.1	**Gestión de incidentes y mejoras en la seguridad de la información**	**Objetivo: Asegurar un enfoque coherente y eficaz para la gestión de incidentes de seguridad de la información, incluida la comunicación sobre eventos de seguridad y debilidades.**
A.16.1.1	Responsabilidad y procedimientos	Control: Se deberían 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	Control: Los eventos de seguridad de la información se deberían 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	Control: Se debería exigir a todos los empleados y contratistas que usan los servicios y sistemas de información de la organización, que observen e informen 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	Control: Los eventos de seguridad de la información se deberían evaluar y se debería 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	Control: Se debería 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	Control: El conocimiento adquirido al analizar y resolver incidentes de seguridad de la información se debería usar para reducir la posibilidad o el impacto de incidentes futuros.
A.16.1.7	Recolección de evidencia	Control: La organización debería definir y aplicar procedimientos para la identificación, recolección, adquisición y preservación de información que

		pueda servir como evidencia.
	A. 17 Aspectos de seguridad de la información de la gestión de continuidad de negocio	
A.17.1	**Continuidad de seguridad de la información**	**Objetivo: La continuidad de seguridad de la información se debería incluir en los sistemas de gestión de la continuidad de negocio de la organización.**
A.17.1.1	Planificación de la continuidad de la seguridad de la información	Control: La organización debería 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	Control: La organización debería 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	Control: La organización debería verificar a intervalos regulares los controles de continuidad de la seguridad de la información establecidos e implementados, con el fin de asegurar que son validos y eficaces durante situaciones adversas.
A.17.2	**Redundancias**	**Objetivo: Asegurar la disponibilidad de instalaciones de procesamiento de información.**
A.17.2.1	Disponibilidad de instalaciones de procesamiento de información.	Control: Las instalaciones de procesamiento de información se deberían implementar con redundancia suficiente para cumplir los requisitos de disponibilidad.
	A. 18 Cumplimiento	
A.18.1	**Cumplimiento de requisitos legales y contractuales**	**Objetivo: Evitar el incumplimiento de las obligaciones legales, estatutarias, de reglamentación o contractuales relacionadas con seguridad de la información, y de cualquier requisito de seguridad.**
A.18.1.1	Identificación de la legislación aplicable y de los requisitos contractuales	Control: Todos los requisitos estatutarios, reglamentarios y contractuales pertinentes, y el enfoque de la organización para cumplirlos, se deberían identificar y documentar explícitamente y mantenerlos actualizados para cada sistema de información y para la organización.
A.18.1.2	Derechos de propiedad intelectual	Control: Se deberían implementar procedimientos apropiados para asegurar el 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	Control: Los registros se deberían proteger contra perdida, 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 datos personales	Control: Cuando sea aplicable, se deberían asegurar la privacidad y la protección de la información de datos personales, como se exige en la legislación y la reglamentación pertinentes.
A.18.1.5	Reglamentación de controles criptográficos	Control: Se deberían usar controles criptográficos, en cumplimiento de todos los acuerdos, legislación y reglamentación pertinentes.
A.18.2	**Revisiones de seguridad de la información**	**Objetivo: Asegurar que la seguridad de la información se implemente y opere de acuerdo con las políticas y procedimientos organizacionales.**
A.18.2.1	Revisión independiente de la seguridad de la información	Control: 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 deberían revisar independientemente a intervalos planificados o cuando ocurran cambios significativos.

A.18.2.2	Cumplimiento con las políticas y normas de seguridad	Control: Los directores deberían 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	Control: Los sistemas de información se deberían revisar periódicamente para determinar el cumplimiento con las políticas y normas de seguridad de la información.

Tomado de ISO/IEC 27001:2013 Anexo A