2020

Colombia Compra Eficiente

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

## AGENCIA NACIONAL DE CONTRATACIÓN PUBLICA COLOMBIA COMPRA EFICIENTE


**Director General**
José Andrés O'Meara Riveira

**Secretaria General**
Claudia Ximena Lopez Pareja

**Subdirector de Negocios**
Andrés Ricardo Mancipe Gonzalez

**Subdirector de Gestión Contractual**
Jorge Augusto Tirado Navarro

**Subdirectora de Estudios de Mercado y Abastecimiento Estratégico (EMAE)**
Catalina Pimienta Gómez

**Subdirector de Información y Desarrollo Tecnológico (IDT)**
Rigoberto Rodriguez Peralta

**Asesor Jurídico**
Juan David Marín Lopez

**Asesor Económico**
Steven Orozco Rodríguez

**Asesor Control Interno**
Judith Gomez Zambrano

**Asesor Planeación**
Karina Blanco Marín

## CONTENIDO

## INTRODUCCIÓN

El presente documento define las acciones que la Agencia Nacional de Contratación Publica Colombia Compra Eficiente ANCP-CCE ejecuta para tratar y gestionar los Riesgos de Seguridad y Privacidad de Información.

El plan de tratamiento de riesgos de seguridad y privacidad de la información le permite Agencia Nacional de Contratación Pública Colombia Compra Eficiente ANCP-CEE enfocar y priorizar los esfuerzos necesarios para proteger los Activos de Información en cualquiera de sus estados ante los riesgos que atenten contra la Confidencialidad, Integridad y Disponibilidad a través de la implementación de medidas y controles de seguridad que permitan mitigar los riesgos e impactos a los que están expuestos, aprovechando los recursos de mejor manera y aportando el mayor valor a la operación de la entidad.

El presente Plan de Tratamiento de riesgos se encuentra articulado con la metodología de riesgos vigente, establecida en la Política de Administración de Riesgos de la entidad, del proceso de Seguridad de la Información y con la última Guía aprobada por el DAFP y MINTIC.

## OBJETIVO

El objetivo de la Gestión de Riesgos de Seguridad y Privacidad de la Información es identificar, priorizar, y tratar los Riesgos de Seguridad y Privacidad de la Información, logrando preservar la Confidencialidad, Integridad y Disponibilidad de los Activos de Colombia Compra Eficiente.

## DEFINICIONES

| |
|---|
| **Activo de Información**: toda aquella información que reside en medio electrónico o físico, que tiene un significado y valor para Colombia Compra Eficiente y, por ende, necesita ser protegida. |
| **Amenaza:** Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización. |
| **Confidencialidad**: principio de la Seguridad de la Información que busca asegurar que la información de Colombia Compra Eficiente sea accedida únicamente por personal autorizado (tanto interno como externo a Colombia Compra Eficiente), para suplir una necesidad legítima para la realización de sus funciones, con el fin de prevenir el uso o divulgación de la misma en forma no autorizada. |
| **Contenedor de la Información**: cualquier plataforma tecnológica o lugar físico que almacena, procesa, transmite un Activo de Información por cualquier lapso de tiempo o propósito. |
| **Disponibilidad**: principio de la Seguridad de la Información que busca asegurar que la información esté disponible cuando sea requerido por los procesos, servicios, ciudadanos y en general partícipes de los procesos de contratación alojados en las plataformas bajo responsabilidad de Colombia Compra Eficiente. |
| **Integridad**: principio de Seguridad de la Información que busca asegurar que la información esté protegida contra modificaciones no autorizadas para garantizar su consistencia, exactitud y completitud. Se debe garantizar la trazabilidad de la información. |

| |
|---|
| **Proceso**: grupo de actividades relacionadas de manera lógica que, cuando se llevan a cabo, utilizan los recursos de Colombia Compra Eficiente para lograr resultados definitivos o transformar elementos de entrada, a través de una serie de actividades, en un producto o servicio. |
| **Propietario del Activo (o de la Información)**: funcionario encargado de identificar y establecer el alcance y valor o criticidad de un Activo de Información, los requerimientos de seguridad del mismo y la comunicación de éstos a los custodios del Activo de Información. |
| **Dueño del Proceso**: funcionario de Colombia Compra Eficiente responsable del adecuado cumplimento de las actividades que conforman un proceso, y que están encaminadas a satisfacer una demanda tanto interna como externa a Colombia Compra Eficiente. |
| **Riesgo Residual:** Riesgo restante después de aplicar el tratamiento al Riesgo. |
| **Riesgo**: 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.<br>**Riesgos de seguridad digital:** Posibilidad Combinación de amenazas y vulnerabilidades en el entorno digital. Puede debilitar el logro de objetivos económicos y sociales, afectar la soberanía nacional, la integridad territorial, el orden constitucional y los intereses nacionales. Incluye aspectos relacionados con el ambiente físico, digital y las personas |
| **Seguridad de la Información:** Preservación de la Confidencialidad, Integridad y Disponibilidad de la información, en adición también de otras propiedades como autenticación, autorización, registro de actividad, no repudio y confiabilidad pueden ser también consideradas. |
| **Vulnerabilidad:** debilidad asociada al Contenedor de un Activo de Información y que puede ser explotada para materializar un Riesgo, causando incidentes no deseados que pueden dar lugar a la pérdida de Confidencialidad, Integridad o Disponibilidad de los Activos de Información. |

**Gestión de Riesgos de Seguridad y Privacidad de la Información**

La gestión de Riesgos de Seguridad y Privacidad de la Información del presente plan obedece la estructura y etapas definidas en el estándar internacional ISO 27005 y la *"Guía para la Administración de los Riesgos de Gestión, Corrupción y Seguridad Digital y el Diseño de Controles en Entidades Públicas*" del Ministerio de Tecnologías de la Información y las Comunicaciones y el Departamento Administrativo de la Función Pública. A continuación, se aprecia la ilustración 1, que muestra cómo se realiza la gestión de Riesgos de Seguridad y Privacidad de la Información, en la entidad:

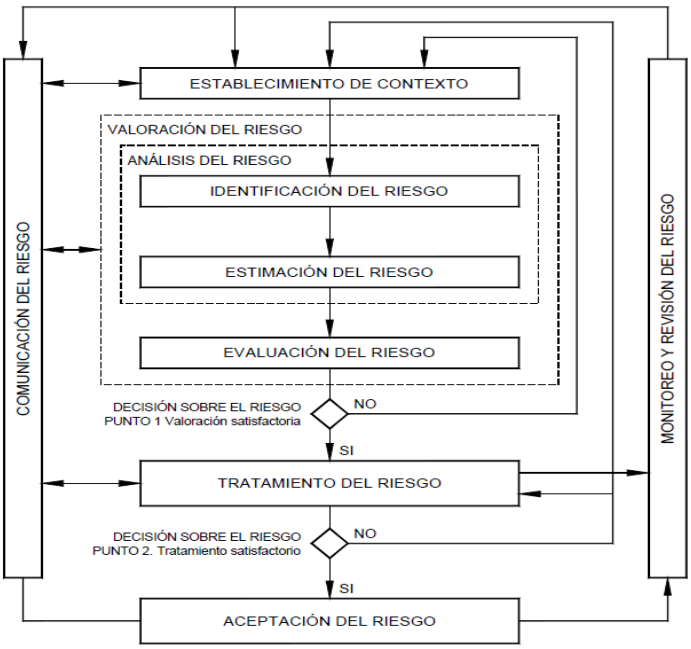



Ilustración 1 Gestión del Riesgo (Fuente ISO27005)

La gestión del riesgo dentro de la seguridad de la información se puede también enmarcar dentro del ciclo de planear, hacer, verificar y actuar (PHVA). El proceso de identificación y evaluación de los riesgos de seguridad de la información está compuesto por las siguientes fases:

## 1. Fase de Planificación

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:

### 1.1 Establecimiento de contexto

Esta primera etapa define el alcance que tendrá la gestión de los Riesgos de seguridad y privacidad de la Información, los responsables y los criterios de evaluación y aceptación de Riesgos que se identificaran y trataran.

Para Colombia Compra Eficiente, la gestión de Riesgos de Seguridad y privacidad de la Información se realizará sobre los procesos, que tengan Activos de Información clasificados como Altos.

Los líderes de Procesos, propietarios y responsables de Activos de Información son los encargados de realizar la gestión del Riesgo sobre dichos Activos de Información. El Líder de Seguridad de la Información debe promover y apoyar la ejecución de esta actividad.

El establecimiento del contexto dentro de la Agencia Nacional de contratación Pública -Colombia Compra eficiente ANCP -CCE se define de acuerdo con los parámetros internos y externos en consideración con los parámetros descritos en la Política de Administración de Riesgos de la entidad permitiéndole determinar los factores generadores de riesgos.

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.

### Establecimiento del contexto externo

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

**CONTEXTO EXTERNO**

- Clientes, proveedores de servicios y empresas que sean competencia directa y/o se relacionen con la misión de la entidad pública analizada.
- Normativas o aspectos jurídicos que apliquen directa o indirectamente a la entidad pública; ejemplo, la ley 1581 de 2012 o la ley 1712 de 2014, circulares o regulaciones emitidas por superintendencias o ministerios, como el decreto 1078 de 2015 o el decreto 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.

Ilustración 2 Contexto Externo

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

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

Ilustración 3. Contexto Interno

**Establecimiento del contexto del proceso**

Se determinan las características o aspectos esenciales del proceso y sus interrelaciones. Se pueden considerar factores como:

- Objetivo del proceso
- Alcance del proceso
- Interrelación con otros procesos
- Procedimientos asociados
- Responsables del proceso
- Activos de seguridad digital del proceso: información, aplicaciones, hardware entre otros, que se deben proteger para garantizar el funcionamiento interno de cada proceso, como de cara al ciudadano.

## 1.2 Política de administración de riesgo.

La Entidad tiene establecida una política de gestión de riesgo integral “POLÍTICA DEL SISTEMA DE ADMINISTRACIÓN DE RIESGOS AGENCIA NACIONAL DE CONTRATACIÓN PÚBLICA COLOMBIA COMPRA EFICIENTE”, donde se incluya el compromiso en la gestión de los riesgos de seguridad digital en todos sus niveles.

## 1.3 Roles y responsabilidades

La Entidad debe designar un responsable de Seguridad Digital que también es el responsable de la Seguridad de la Información, 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

Ilustración 4. Responsable de Seguridad Digital

En complemento a lo anterior debe tomar como referencia lo definido en la Guía Roles y responsabilidades del MSPI de la Estrategia de Gobierno Digital del MINTIC

La ANCP-CCE dispone de los recursos para el desarrollo de la gestión de riesgos de seguridad digital, 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 de la ANCP-CCE asigna 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.

## 1.4 Criterios de probabilidad, impacto y zonas de riesgo aceptable

Los criterios para la evaluación de impacto y probabilidad de los Riesgos de Seguridad de la Información son los mismos definidos en el Manual Metodológico del Sistema de Administración del Riesgo de la ANCP-CCE.

## 1.5 Identificación de activos

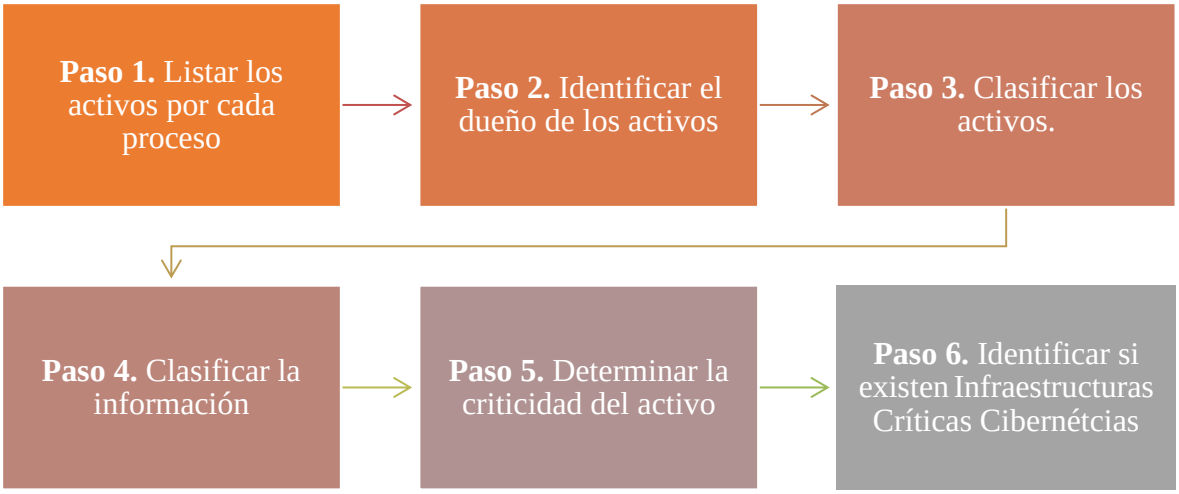
En esta etapa se deben identificar los contendores y Activos de Información que se podrían ver afectados por la materialización de los Riesgos, tomando en cuenta la matriz de identificación de Activos de la entidad,

producto de la ejecución de lo establecido en la Metodología de Activos de Información de Colombia Compra Eficiente.

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, 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.

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.

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




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

Ilustración 5. Pasos para la identificación y valoración de activos.

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.
Paso 2. Identificar el dueño o propietario 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.
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 la tipología de activos con el fin de hacer la clasificación mencionada.

| Tipo de activo | Descripción |
|---|---|
| **Información** | Información almacenada en formatos físicos (papel, carpetas, CD, DVD) o en formatos digitales o electrónicos (ficheros en bases de datos, correos electrónicos, archivos o servidores), teniendo en cuenta lo anterior, se puede distinguir como información: Contratos, acuerdos de confidencialidad, manuales de usuario, procedimientos operativos o de soporte, planes para la continuidad del negocio, registros contables, estados financieros, archivos ofimáticos, documentos y registros del sistema integrado de gestión, bases de datos con información personal o con información relevante para algún proceso (bases de datos de nóminas, estados financieros) entre otros. |
| **Software** | Activo informático lógico como programas, herramientas ofimáticas o sistemas lógicos para la ejecución de las actividades |
| **Hardware** | Equipos físicos de cómputo y de comunicaciones como, servidores, biométricos que por su criticidad son considerados activos de información |
| **Servicios** | Servicio brindado por parte de la entidad para el apoyo de las actividades de los procesos, tales como: Servicios WEB, intranet, CRM, ERP, Portales organizacionales, Aplicaciones entre otros (Pueden estar compuestos por hardware y software) |
| **Intangibles** | Se consideran intangibles aquellos activos inmateriales que otorgan a la entidad una ventaja competitiva relevante, uno de ellos es la imagen corporativa, reputación o el good will, entre otros |
| **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 |
| **Recurso Humano (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 |
| **Otros** | Activos de información que no corresponden a ninguno de los tipos descritos anteriormente, pero deben ser valorados para conocer su criticidad al interior del proceso |

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

Ilustración 6. Tipología de Activos

Paso 4. Clasificar la información:

Realizar la clasificación de la información conforme lo indican las leyes 1712 de 2014, 1581 de 2012, el Modelo de Seguridad y Privacidad en su Guía de Gestión de Activos, y demás normatividad aplicable.
Paso 5. Determinar la criticidad del activo (Valoración del Activo):
Evaluar la criticidad de los activos, a través de preguntas que le permitan determinar el grado de importancia de cada uno. Conforme lo establecido en la Metodología de Activos de Información de Colombia Compra Eficiente se valoraron los activos respecto a la confidencialidad, integridad y disponibilidad mediante las escalas (ALTA, MEDIA y BAJA) que identifican su nivel de importancia o criticidad para el proceso. La Entidad define gestionar los riesgos solo en aquellos que tengan un nivel de criticidad Alto, tomando como referencia la Guía de Gestión del Riesgo del MinTIC.
Paso 6. Identificar si existen Infraestructuras Críticas Cibernéticas -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*.

Ilustración 7. Criterios Infraestructuras Críticas Cibernéticas -ICC-

Con base a los seis (6) pasos vistos previamente, se generó el formato con CÓDIGO: CCE-GTI-FM-14 para realizar tanto la identificación e inventario de activos como para hacer su levantamiento.

### 1.6 Identificación de riesgos

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).

| 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

Ilustración 8 Tabla de amenazas comunes

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

| Fuente de amenaza | Motivación | Acciones amenazantes |
|---|---|---|
| Pirata informático, intruso ilegal | Reto<br>Ego | Piratería<br>Ingeniería social |
| Criminal de la computación | Destrucción de la información<br>Divulgación ilegal de la información | Crimen por omputador<br>Acto fraudulento |
| Terrorismo | Chantaje<br>Destrucción | Ataques contra el sistema DDoS<br>Penetración en el sistema |
| Espionaje industrial (inteligencia, empresas, gobiernos extranjeros, otros intereses) | Ventaja competitiva<br>Espionaje económico | Ventaja de defensa<br>Hurto de información |
| Intrusos (empleados con entrenamiento deficiente, descontentos, malintencionados, negligentes, deshonestos o despedidos) | Curiosidad<br>Ganancia monetaria | Asalto a un empleado<br>Chantaje |

**Fuente**: ISO/IEC 27005:2009

Ilustración 9**.** Tabla de amenazas dirigida por el hombre

**Identificación de vulnerabilidades:**

Se plantean los siguientes listados de vulnerabilidades que pueden ser aprovechadas por alguna amenaza.

| 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 |
| | Ausencia de control de los activos 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 |

**Fuente**: ISO/IEC 27005

Ilustración 10**.** Tabla de Vulnerabilidades Comunes

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

| Tipo de activo | Ejemplos de vulnerabilidades | Ejemplos de amenazas |
|---|---|---|
| Hardware | 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

Ilustración 11**.** Tabla de Amenazas y Vulnerabilidades

**Identificación de las consecuencias**

Se identifican los daños o las consecuencias para la organización que podrían ser causadas por un escenario de incidente. Un escenario de incidente es la descripción de una Amenaza que explota una vulnerabilidad determinada o un conjunto de vulnerabilidades en un incidente de Seguridad de la Información.

Se debe analizar e identificar las consecuencias de los escenarios de incidentes en términos de:

- Tiempo de investigación y reparación
- Pérdida de tiempo operacional
- Pérdida de oportunidad
- Salud y seguridad
- Costo financiero
- Imagen, reputación y buen nombre.

De acuerdo con el resultado de la aplicación de la metodología de activos, se deben asociar en la matriz de riesgos de seguridad digital y de la Información, los grupos de activos de información y los riesgos identificados.

## 1.7 Valoración de riesgos

**Identificación del riesgo inherente de seguridad digital:**

El propósito de la identificación del Riesgo es determinar que eventos podrían suceder que afecten la Disponibilidad, la Integridad o la Confidencialidad de la información de Colombia Compra Eficiente, y llegar a reconocer las causas que los provocan, los Activos de información asociados y las consecuencias que podría tener su materialización.

De ser posible, para este análisis se deben tener en cuenta datos históricos, incidentes de Seguridad de la Información, conocimiento sobre la entidad y los procesos de las personas involucradas, y opiniones de expertos.

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.

Por medio de la estimación del riesgo, la Agencia Nacional de Contratación Pública – Colombia Compra Eficiente ANCP-CCE busca establecer la probabilidad de ocurrencia del riesgo y el nivel y/o impacto de consecuencia, con el fin de estimar la zona de riesgo inicial, generalmente llamada riesgo inherente, realizar su priorización y establecer la estrategia de tratamiento.

Mientras que en la evaluación del riesgo: Se busca confrontar los resultados del análisis de riesgo inicial frente a los controles establecidos, con el fin de determinar la zona de riesgo final (RIESGO RESIDUAL). Con el fin de estimar la zona de riesgo inicial; para lo cual será necesario entender como:

**Análisis de la probabilidad**

Se analiza qué tan posible es que ocurra el riesgo, se expresa en términos de frecuencia o factibilidad, donde frecuencia implica analizar el número de eventos en un periodo determinado, se trata de hechos que se han materializado o se cuenta con un historial de situaciones o eventos asociados al riesgo; factibilidad implica analizar la presencia de factores internos y externos que pueden propiciar el riesgo, se trata en este caso de un hecho que no se ha presentado pero es posible que suceda.

| NIVEL | DESCRIPTOR | DESCRIPCIÓN | FRECUENCIA |
|---|---|---|---|
| 5 | **Casi seguro** | Se espera que el evento ocurra en la mayoría de las circunstancias. | Más de 1 vez al año. |
| 4 | **Probable** | Es viable que el evento ocurra en la mayoría de las circunstancias. | Al menos 1 vez en el último año. |
| 3 | **Posible** | El evento podrá ocurrir en algún momento. | Al menos 1 vez en los últimos 2 años. |
| 2 | **Improbable** | El evento puede ocurrir en algún momento. | Al menos 1 vez en los últimos 5 años. |
| 1 | **Rara vez** | El evento puede ocurrir solo en circunstancias excepcionales (poco comunes o anormales). | No se ha presentado en los últimos 5 años. |

Ilustración 12**.** Tabla Criterios para calificar probabilidad

**Análisis de Impacto**

El impacto se debe analizar y calificar a partir de las consecuencias identificadas en la fase de descripción del riesgo.

| NIVEL | VALOR DEL IMPACTO | CRITERIOS DE IMPACTO PARA RIESGOS DE SEGURIDAD DIGITAL | |
|---|---|---|---|
| | | Impacto (consecuencias) Cuantitativo | Impacto (consecuencias) Cualitativo |
| INSIGNIFICANTE | 1 | Afectación ≥X% de la **población**<br>Afectación ≥X% del **presupuesto** anual de la entidad<br>No hay **Afectación medioambiental** | Sin afectación de la integridad<br>Sin afectación de la disponibilidad<br>Sin afectación de la confidencialidad |
| MENOR | 2 | Afectación ≥X% de la población<br>Afectación ≥X% del presupuesto anual de la entidad<br>Afectación leve del Medio Ambiente requiere de ≥X días de recuperación | Afectación leve de la integridad<br>Afectación leve de la disponibilidad<br>Afectación leve de la confidencialidad |
| MODERADO | 3 | Afectación ≥X% de la población<br>Afectación ≥X% del presupuesto anual de la entidad<br>Afectación leve del Medio Ambiente requiere de ≥X semanas de recuperación | Afectación moderada de la integridad de la información debido al interés particular de los empleados y terceros<br>Afectación moderada de la disponibilidad de la información debido al interés particular de los empleados y terceros<br>Afectación moderada de la confidencialidad de la información debido al interés particular de los empleados y terceros |
| MAYOR | 4 | Afectación ≥X% de la población<br>Afectación ≥X% del presupuesto anual de la entidad<br>Afectación importante del Medio Ambiente que requiere de ≥X meses de recuperación | Afectación grave de la integridad de la información debido al interés particular de los empleados y terceros<br>Afectación grave de la disponibilidad de la información debido al interés particular de los empleados y terceros<br>Afectación grave de la confidencialidad de la información debido al interés particular de los empleados y terceros |
| CATASTRÓFICO | 5 | Afectación ≥X% de la población<br>Afectación ≥X% del presupuesto anual de la entidad<br>Afectación muy grave del Medio Ambiente que requiere de ≥X años de recuperación | Afectación muy grave de la integridad de la información debido al interés particular de los empleados y terceros<br>Afectación muy grave de la disponibilidad de la información debido al interés particular de los empleados y terceros<br>Afectación muy grave confidencialidad de la información debido al interés particular de los empleados y terceros |

Fuente Guía para la Administración de los Riesgos del DAFP.

Ilustración 13. Tabla Criterios para calificar el impacto

La variable población se define teniendo en cuenta el establecimiento del contexto externo de la entidad, es decir, que la consideración de población va a estar asociada a las personas a las cuales se les prestan servicios o trámites en el entorno digital y que de una u otra forma pueden verse afectadas por la materialización de algún riesgo en los activos identificados. Los porcentajes en las escalas pueden variar, según la entidad y su contexto.

La variable presupuesto es la consideración de presupuesto afectado por la entidad debido a la materialización del riesgo, contempla sanciones económicas o impactos directos en la ejecución presupuestal.

La variable ambiental estará también alineada con la afectación del medio ambiente por la materialización de un riesgo de seguridad digital. Esta variable puede no ser utilizada en la mayoría de los casos, pero debe tenerse en cuenta, ya que en alguna eventualidad puede existir afectación ambiental.

Ahora bien, de acuerdo con la metodología adoptada por la ANCP-CCE; para estimar el nivel de riesgo inicial, los valores determinados para la probabilidad y el impacto o consecuencias se combinan en la matriz de riesgo, con el fin de determinar la zona de riesgo en la cual se ubica el riesgo identificado. Este primer análisis del riesgo se denomina Riesgo Inherente y se define como aquél al que se enfrenta la entidad en ausencia de los controles y que solo con su definición permiten modificar su probabilidad o impacto como efecto de la mitigación

**Identificación y evaluación de los controles existentes**

Como lo indica la Guía de DAFP, 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.

Para determinar si existen uno o varios controles asociados a los riesgos inherentes identificados se puede consultar la Ilustración 14 (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.

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 | Areas 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. |

Fuente ISO/IEC 27001:2013 Anexo A

Ilustración 14. Controles de referencia para la mitigación de riesgos de seguridad digital

## 1.8 Definición del tratamiento de los riesgos

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.

Para la Agencia Nacional de Contratación Publica Colombia Compra Eficiente ANCP-CCE, el criterio para aceptar el Riesgo y no ejecutar ninguna medida de respuesta sobre las vulnerabilidades, solo aplica para Riesgos con nivel Bajo. Riesgos de nivel **Moderado**, **Alto y Extremo** deberán tener una medida de respuesta distinta a la aceptación del riesgo o justificar adecuadamente su aceptación y comunicarlo con la Alta Dirección.

Para 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 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.

Para el caso en el que se haya decidió tomar una medida de respuesta distinta a aceptar el Riesgo, se deben definir unas acciones de tratamiento (actividades de control) y evaluar los Riesgos Residuales, estas actividades le corresponden a la primera línea de defensa de la entidad y deben ser documentadas.

Como resultado de la etapa de evaluación del riesgo, se podrá identificar la matriz de riesgos de la Entidad lo que permitirá elegir la(s) estrategia(s) de tratamiento del riesgo en virtud de su valoración y de los criterios establecidos en el contexto de gestión de riesgos de la entidad.

**Definir actividades de control / acciones de tratamiento**

Se deben definir acciones que permitan reducir, evitar o transferir el Riesgo, según sea el caso. Adicionalmente, en esta etapa se debe especificar:

- El alcance de la acción
- Periodicidad con que se ejecutan
- Asignar el responsable de la ejecución de las acciones.
- Propósito del control
- Establecer como se realiza la acción
- Indicar qué acciones se toman cuanto existen observaciones o desviaciones resultantes de ejecutar el control
- La documentación que soporta la ejecución del control

Las actividades de control se identifican teniendo en cuenta que pueden ser preventivas o detectivas, aclarando que las preventivas se diseñan para evitar la materialización de un evento no deseado, previniendo la ocurrencia de riesgos que afecten la integridad, disponibilidad y confidencialidad de la Información; mientras que los controles detectivos, se centran en eventos que ya se materializaron con el fin de corregir la situación. Así mismo, es importante que los controles apunten a tratar las causas/vulnerabilidades que generan los riesgos, estos controles pueden tratar varias causas/vulnerabilidades o solo una, lo importante es que cada causa/Vulnerabilidad sea tratada y de forma efectiva.

**Definir Riesgos Residuales**

Luego de definir y ejecutar las acciones de tratamiento, se debe estimar el Riesgo Residual después de haber ejecutado las acciones, para esta actividad es necesario tener en cuenta la tabla de resultado de los posibles desplazamientos de probabilidad e impacto de la Guía para la Administración de los Riesgos de Gestión, Corrupción y Seguridad Digital y el Diseño de Controles en Entidades Públicas (Dafp y Mintic).

Teniendo en cuenta que, si la evaluación del conjunto de controles es débil, no disminuirá ningún cuadrante de impacto o probabilidad asociado al riesgo.

## 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.

## 3. Fase 3. Monitoreo y revisión

El responsable de seguridad digital deberá supervisar el proceso de implementación de los planes de tratamiento, verificando que los responsables de los planes ejecuten las tareas en los tiempos pactados y que los recursos se estén ejecutando de acuerdo con lo planeado.

La Entidad a través de las Líneas de defensa 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.

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.

La entidad pública debe utilizar medidas de desempeño 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.

Los Riesgos y sus factores son dinámicos (es decir, el valor de los Activos, los impactos, las Amenazas, las vulnerabilidades y la probabilidad de ocurrencia) por lo tanto se deberían monitorear y revisar con el fin de identificar todo cambio en el contexto de la organización en una etapa temprana que exija la valoración iterativa de los riesgos de seguridad de la información y para mantener una visión general de la perspectiva completa del Riesgo.

Para ello, se deben documentar las revisiones realizadas por el área de seguridad de la información, la fecha para la implementación de los tratamientos, la frecuencia y auto seguimientos que los responsables del tratamiento del riesgo deben realizar sobre la implementación de los controles.

El Líder de Seguridad de la Información, Liderará los auto seguimientos con los responsables y realizará reuniones con el fin de verificar la efectividad y la correcta aplicación de los controles. La periodicidad para cada reunión depende de las fechas establecidas en la ejecución de los controles.

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

La Entidad 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.

5. Actividades proyectadas en el plan de tratamiento de Riesgos

Las actividades planteadas a continuación fortalecen la gestión de los riesgos de privacidad y seguridad de la Información en Colombia Compra Eficiente, y complementan lo indicado en la Matriz de riesgos gestión, corrupción y seguridad de la Información, como también la Política y metodología de riesgos de seguridad de la Información y la metodología de activos de información; en las cuales se plantean los riegos ya identificados, con sus respectivos controles para el tratamiento respectivo, realizando el establecimiento y entendimiento del contexto, estimación, evaluación y tratamiento.

Para la vigencia 2021 se planean adelantar las siguientes actividades por parte de la Subdirección de Información y Desarrollo Tecnológico y el equipo de seguridad de la Información:

| ACTIVIDAD | DESCRIPCIÓN | RESPONSABLE | FECHA FINAL |
|---|---|---|---|
| Seguimiento de riesgos IDT (Seguridad de la Información) y activos de Información. | Se realizan seguimientos periódicos, de acuerdo a la periodicidad de los controles establecidos para cada riesgo. | Equipo de Seguridad de la Información | 30 de diciembre 2021 |
| Seguimiento Fase de tratamiento | Se realiza seguimiento al estado de los planes de tratamiento de riesgos identificados y verificación de evidencias. | Equipo de Seguridad de la Información | 30 de diciembre 2021 |
| Evaluación de Riesgos residuales | Evaluación de Riesgos residuales | Equipo de Seguridad de la Información | 30 de diciembre 2021 |

## 6. FICHA TÉCNICA DE CONTROL DE CAMBIOS.

| I. IDENTIFICACIÓN Y UBICACIÓN DEL DOCUMENTO | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| **Título:** | Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información | | | | | | | |
| **Fecha de elaboración:** | 24 | Nov | 2020 | **Fecha de aprobación:** | 22 | Dic | 2020 | |
| **Resumen de contenido:** | El plan es para identificar, priorizar, y tratar los Riesgos de Seguridad y Privacidad de la Información, logrando preservar la Confidencialidad, Integridad y Disponibilidad de los Activos de Colombia Compra Eficiente. | | | | | | | |
| **Área / Dependencia:** | Subdirección de Información y Desarrollo Tecnológico | | | | | | | |
| **Código:** | CCE-SGI-PL-02 | | | **Estado:** | Aprobada | | | |
| **Categoría - Tipo de documento** | IDI | | | | | | | |
| **Autor / Autores:** | Milena Patricia Cabrales | | | | | | | |
| **Aprobación por:** **Cargo:** | Rigoberto Rodríguez Peralta | | | | | | | |
| **Nombre:** | Subdirector de Información y Desarrollo Tecnológico | | | | | | | |
| **Información adicional:** | | | | | | | | |
| **Tipo de documento:** (Marque X) | Físico | ( ) | Electrónico | (X) | | | | |
| **Ubicación:** (especifique donde se aloja o reposa el documento) | Documentos del MIPG/ Subdirección IDT | | | | | | | |

| I. AUTORIZACIONES RESPONSABLES | | | | | | |
|---|---|---|---|---|---|---|
| **Acción** | **Nombre** | **Cargo / Perfil** | **Fecha** | | | **Firma** |
| **Elaboró** | Milena Patricia Cabrales | Contratista Líder de Seguridad | 24 | Nov | 2020 | Milena Cabrales |
| **Revisó** | Rigoberto Rodríguez Peralta | Subdirector de Información y Desarrollo Tecnológico | 30 | Nov | 2020 | Rigoberto Rodriguez |
| **Aprobó** | Comité Institucional de Gestión y Desempeño | ComitéInstitucional de Gestión y Desempeño | 22 | Dic | 2020 | Acta 22 de diciembre del 2020 |
| **¿Aprobación mediante comité interno?** A continuación, Marque **X** en **SI** o **NO** | | | | | | **SI** X **NO** |
| **Nombre de comité interno:** | Comité Institucional de Gestión y Desempeño | | | | | |
| **Acto administrativo de conformación comité interno:** | | | | | | |
| **Fecha de conformación de comité interno:** | | | | | | |
| **Medio de Aprobación de este documento:** | Reunión virtual | | | | | |

_____

**Nota1:** Si ha marcado (**NO**) **en la sección de: "¿Aprobación mediante comité interno?**" marque N/A (No aplica) en los siguientes 4 espacios de preguntas correspondientes a la sección de autorizaciones responsables.

**Nota2:** Diligenciar las fechas de la siguiente manera Dia: diligenciar dos dígitos en números; Mes: diligenciar el mes con las tres primeras letras del mes, ejemplo: Ene = Enero, Ago = Ago. Año: Diligenciar el año con los cuatro dígitos.

| I. CONTROL DE CAMBIOS DE DOCUMENTO | | | Versión vigente del documento: | | 02 |
|---|---|---|---|---|---|
| **VERSIÓN** | **FECHA** | **DESCRIPCIÓN DE AJUSTES** | **ELABORÓ** | **REVISÓ** | **APROBÓ** |
| 1 | 05/04/2019 | Creación del documento | Luis Alejandro Ruiz | Dana Pineda Marín | CIGD |
| 2 | 22/12/2020 | Actualización del Documento | Milena Patricia Cabrales Contratista Líder de Seguridad | Rigoberto Rodríguez Peralta Subdirector de IDT | CIGD |

_____

**Nota:** El control de cambios en el documento, se refiere a cualquier ajuste que se efectúe sobre el documento que describe ficha técnica del presente documento.