# GESTIÓN DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN EN EL SECTOR PÚBLICO

Osorio Corredor, Luis Edwin
luisedwinosorio@gmail.com
Universidad Piloto de Colombia

***Resumen***— Este documento identifica los principales aspectos que deben tener en cuenta las organizaciones del sector púbico, en un proceso de gestión del riesgo de seguridad de la información, partiendo desde establecer el contexto, detallar un enfoque, realizar una identificación, un análisis y una evaluación, así como el tratamiento de los riesgos, para luego pasar a comunicar y realizar consultas, acompañadas de un constante monitoreo mediante auditorías, utilizando herramientas y guías aprobadas en Colombia.

***Índice de Términos***— Activo, amenaza, ataque, impacto, incidente, riesgo, vulnerabilidad, modelo PHVA, MECI.

***Abstract*** —This document identifies the main aspects that organizations of the public sector should take into account, in a process of risk management of the information security, starting from establishing the context, detailing an approach, carrying out an identification, an analysis and an evaluation, as well as the treatment of the risks, to then go on to communicate and make consultations, accompanied by constant monitoring through audits, using tools and guides approved in Colombia.

***Keywords***— Active, threat, attack, impact, incident, risk, vulnerability, model PHVA, MECI.

## I. INTRODUCCIÓN

El uso de las Tecnologías de la Información (TI) ha aumentado en las organizaciones del sector público durante los últimos años, independientemente de la actividad que estas desarrollen, ya que al igual que los ambientes naturales o construidos, estas se encuentran en constante evolución.

Sin embargo, la masificación de las TI paralelamente ha generado nuevos riesgos asociados a su desarrollo, convirtiendo a estas organizaciones, en objetivos potenciales de ataques que impacten negativamente al Gobierno Nacional y la ciudadanía en general.

Es por esto que desde el Ministerio de las Tecnologías de la Información y las Comunicaciones (MINTIC), se ha venido impulsando la Estrategia de Gobierno Digital, como una manera de proteger y conservar la integridad de la información de la población, que las organizaciones del sector público requieren salvaguardar.

Es importante tener en cuenta que la información está protegida, si dispone de sistemas que aseguran su confidencialidad, integridad y disponibilidad, los cuales han de estar vinculados estrechamente a detectar y controlar amenazas y vulnerabilidades, al igual que a la evaluación de los riesgos y amenazas. De aquí, que al desarrollo de estas actividades se denomina G*estión del riesgo*. Es decir, para garantizar la seguridad e integridad de la información, se debe identificar y gestionar de manera óptima los riesgos en la organización del sector público y su entorno.

Y para esto, el Departamento Administrativo de la Función Pública (DAFP) [1] estableció la *Guía para la administración del riesgo*, la cual sugiere que para realizar una gestión eficaz del riesgo se debe seguir tres etapas y a partir de ellas, ha de desarrollarse una serie de actividades ajustadas a la realidad de la organización, en aras de administrar los riesgos acordes a sus particularidades.

La primera etapa trata sobre el *compromiso de la alta y media dirección*, [1] donde se destaca la importancia de estas áreas, respaldando las acciones emprendidas en pro de estimular una cultura de la detección y prevención del riesgo.

En la segunda etapa, la conformación de un equipo MECI o de un grupo interdisciplinario es primordial [1], por cuanto que está integrado por delegados de diferentes áreas, quienes deben conocer la organización y su funcionamiento, esto con el objetivo de facilitar la adaptación de la metodología y el diseño de mapas de riesgos.

Y la tercera etapa, pero no menos importante, es la fase de capacitación en la metodología [1], que consiste, como su nombre lo indica, en capacitar en riesgos al equipo interdisciplinario, para que se transformen en multiplicadores de esta información al interior de cada uno de los procesos donde sea que participen.

## II. VISIÓN GENERAL DE LA GESTIÓN DEL RIESGO EN EL SECTOR PÚBLICO

En las organizaciones del sector público y particularmente en sus oficinas de tecnología, una correcta gestión del riesgo en la seguridad de la información, ha de centrarse en la evaluación de las vulnerabilidades y su respectivo riesgo, para luego focalizarse en su tratamiento.

Para esto, el Gobierno Nacional a través del DAFP y el MINTIC, ha desarrollado herramientas para que las entidades que hacen parte del sector, tomen como referencia para gestionar riesgos, con mayor énfasis en los relacionados con la privacidad y la seguridad de la información, en las que elabora el MINTIC.

Es así como podemos observar en la Fig. 1, el proceso que sugiere la herramienta propuesta por el DAFP, para realizar de manera secuencial una correcta identificación de riesgos, partiendo de conocer el *contexto estratégico organizacional*, para posteriormente y con base en dicha información, proceder a efectuar la identificación de riesgos asociados a la realidad organizacional, analizarlos y valorarlos.

Una vez identificados, analizados y valorados, se debe proceder a establecer controles efectivos, los cuales han de ser monitoreados periódicamente, de manera tal que sea posible

ajustarlos, de acuerdo con los cambios del entorno, que en el caso particular de las organizaciones del sector público, están asociados a temas políticos o de cambio en los gobiernos.


*Fig. 1 Visión general de la gestión del riesgo. Tomado de la Guía para la administración del riesgo del DAFP. [1]*

En la Fig. 2, se destaca el tema de la valoración y el análisis de riesgos, como proceso iterativo dentro de una organización.

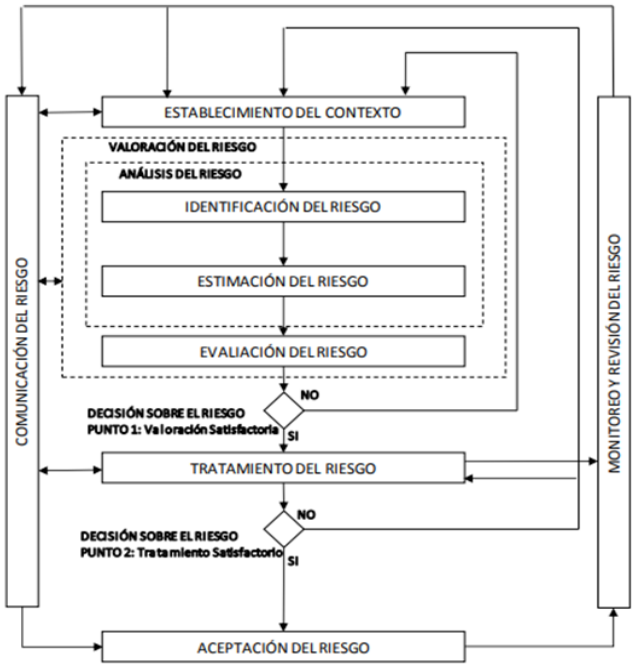


*Fig. 2 Valoración del riesgo tomado de la NTC/IEC 27005 [1]*

*a. ¿Por qué se debe Gestionar el Riesgo?*

Ya que los riesgos de pérdida de información, son un tema que representa mayor vulnerabilidad en las organizaciones del sector público nacional, las entidades se concentran cada vez más en identificarlos y gestionarlos.

La capacidad de minimizar la ocurrencia de hechos que vulneren la seguridad y reaccionar oportunamente ante intromisiones indeseables, ayudará a las organizaciones a desarrollar las funciones para las cuales fueron creadas, generando mayor confianza entre sus funcionarios y en la ciudadanía en general.

*b. ¿Qué es la Gestión del Riesgo?*

La gestión del riesgo no es más que pronosticar e identificar las circunstancias que pueden afectar las actividades de las entidades, y cuando se habla de actividades, no solo se habla desde el punto de vista de la logística, sino que además se incluyen los aspectos estratégicos, financieros, reputacionales, sociales y legales.

*c. ¿Qué Aspectos Importantes se Deben Tener en la Gestión del Riesgo para Poder Cumplir los Objetivos?*

En respuesta a esta pregunta y a su vez el más difícil de cumplir, es generar conciencia, desaprender y volver a aprender. Cuando se habla de la gestión del riesgo, un presidente de una junta directiva, un gerente de una unidad de negocio, el equipo corporativo, los líderes de los procesos, han de entender que existen riesgos tanto internos como externos, es decir, situaciones de manejo propio y otras que, por contextos políticos, sociales, económicos o naturales, escapan de su control, pero han de ser identificados a tiempo.

¿Qué se quiere decir con todo esto?, que el riesgo está siempre conviviendo con las organizaciones y lo importante es aprender a entender, conocer e identificar, aspectos como: ¿Cuáles son las vulnerabilidades de la organización, que la ponen en situación de riesgo?, ¿Qué se va a asumir?, ¿Qué se va a transferir?, ¿Cuál es la mejor forma de desarrollar procesos y metodologías de forma transversal?

Ciertamente, una organización ha de velar por que su operación se desarrolle de la mejor forma, pero identificando los riesgos propios y externos, por cuanto el entorno en qué se encuentra afecta su desarrollo, ya que no es igual a nivel de riesgo que esté ubicada por ejemplo cercana al mar que si estuviese situada en el interior del país.

Asimismo, es importante indicar que en el desarrollo de una correcta gestión del riesgo es fundamental apoyarse en alguno de los estándares reconocidos mundialmente para el tratamiento de estos como: ISO 27005, ISO 31010, AS/NZS 4360, entre otros.

No obstante, como en todos los sistemas basados en procesos, es recomendable utilizar el ciclo PHVA, como base para establecer un sistema de gestión de riesgos que se encuentre enfocado en la mejora continua.

*d. ¿Qué es el Ciclo PHVA?*

También conocido como el ciclo de la mejora continua, es una metodología que describe los cuatro pasos esenciales que se deben llevar a cabo de forma sistemática, para lograr la mejora continua, tal y como se observa en la Fig. 3, entendiendo al mejoramiento continuado como la disminución de fallos, el aumento de la eficacia y eficiencia, la solución de problemas, la previsión y eliminación de riesgos potenciales.

Los pasos propuestos en este ciclo PHVA para la gestión de riesgos son las siguientes:

*Planificar:* Es el punto de partida del ciclo, que se debe construir a partir de una línea de base, sobre la cual se van a establecer objetivos de mejora claros, junto con los parámetros de medición que se van a utilizar para gestionar los riesgos.

*Hacer:* Posterior a la planificación se procede con la ejecución de las acciones necesarias para lograr los objetivos propuestos.

*Verificar:* Todo lo que se hace, es susceptible de ser mejorado. Sin embargo, para lograrlo se debe contar con cifras que nos permitan medir y valorar la efectividad de los cambios implementados.

*Actuar:* En este punto se deben tomar las decisiones y desarrollar las acciones necesarias para corregir las desviaciones encontradas en la verificación, esto con el propósito de mejorar continuamente y minimizar los riesgos.

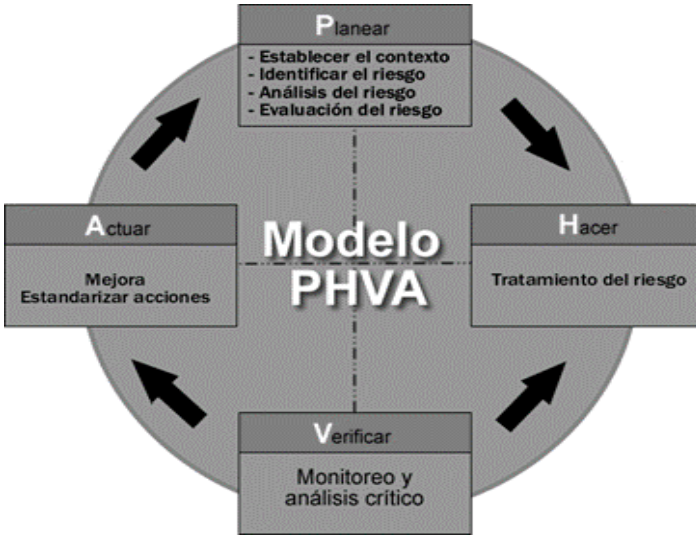


*Fig. 3. Ciclo PHVA tomado de la Guía para la administración del riesgo del DAFP [1]*

## III. ESTABLECIMIENTO DEL CONTEXTO

La definición del contexto no es otra cosa que comprender los datos esenciales de la organización y con ello poder planificar la gestión del riesgo, lo que es más importante, es en esta etapa se jerarquiza los objetivos de la organización, se fija el alcance y se determinan cuáles son los criterios en los cuales se va a medir la gestión del riesgo, para así facilitar las siguientes etapas de evaluación de estos.

Por lo tanto, para poder establecer el contexto, se deben considerar aspectos como el tener claridad sobre los objetivos de la organización, documentación relevante, identificación de las partes interesadas y con base en esta información, establecer un contexto externo y un contexto interno, junto con el alcance del proceso. Teniendo estos aspectos claros se puede apreciar obtener una visión global del contexto organizacional y de los riesgos y su gestión.

### *a. Identificar los Objetivos de la Organización*

Para el desarrollo de este punto ha de tenerse en cuenta que el riesgo es la eventualidad de que ocurra algo que tendrá impacto sobre los objetivos de la organización, por eso, lo primero que se tiene que hacer es tener claridad de cuáles son los aspectos que se planearon al estructurar los objetivos de la organización, ya sean por procesos generales, planes o proyectos. Comprendiendo lo anterior la organización ha de tener en claro sus objetivos y la capacidad para lograr identificarlos, así como el establecer su contexto y los factores que se van a desarrollar en esta etapa.

Ciertamente, los objetivos de la organización permiten determinar las actividades que se van a desarrollar y facilitan establecer los criterios de éxito. Es por ello por lo que se debe cumplir con el indicador del objetivo, en el momento de hacer las mediciones y así es viable determinar los impactos de los riesgos que se encuentran comprometidos al interior de los objetivos de la organización.

### *b. Documentos de Consulta para Establecer el Contexto*

Los documentos que se deben consultar y tareas a desarrollar para poder establecer el contexto y que facilitan el diseño de una guía, entre otros, son los planes estratégicos, la DOFA, legislación vigente, contratos, proyectos, presupuestos, con el fin de llegar a la fase de lluvia de ideas con un contexto claro.

### *c. Identificación de las Partes Involucradas Relevantes*

Las partes involucradas son todas aquellas que se ven directamente afectadas con las decisiones tomadas por la entidad, dentro de las que se encuentran otras entidades del estado, la alta dirección, los funcionarios y contratistas, las familias de estos, sindicatos, los clientes, organismos de control, el medio ambiente, la comunidad, proveedores, empresas financieras, entre otros.

Ahora bien, las anteriores actividades se pueden desarrollar con la realización de entrevistas o cuestionarios, a la alta gerencia, jefes, coordinadores, técnicos y usuarios.

### *d. Establecimiento del Contexto Externo*

Es la etapa en la cual la organización revisa la relación que tiene con el ambiente externo; y también considera la percepción de las partes involucradas y sus valores. Es en esta etapa donde la organización ha de tener en cuenta el alcance de la gestión del riesgo, requisitos legales y reglamentarios, percepciones y relaciones de partes involucradas, así como las claves externas, ambiente social, cultural, político, financiero, tecnológico, económico, natural y competitivo, exigencias y presiones del cliente y partes involucradas, proveedores, y otros aspectos que se consideren factores claves o críticos que afecten la organización.

### *e. Establecimiento del Contexto Interno*

Para el desarrollo de esta etapa se observa la situación interna, con la cual la organización busca alcanzar sus metas. Asimismo se examina la misión, visión y objetivos, como también las políticas implementadas, la cultura organizacional, su estructura y estrategia. A continuación en la Tabla II, se presentan ejemplos de preguntas para realizar entrevistas que ayudaran a establecer el contexto interno.

TABLA II
EJEMPLOS DE PREGUNTAS PARA ENTREVISTAS [3]

| Ítem | Ejemplo Pregunta |
|---|---|
| Objetivo principal de la organización | ¿Cuál es el propósito de la organización<br>¿Cuáles son sus objetivos? |
| El negocio | ¿Cuál es su negocio?<br>¿Cuál es el propósito de lo que se produce/desarrolla? |
| La misión | ¿Cuál es su misión?<br>¿Para qué existe?<br>¿Lo que la organización se propone hacer?<br>¿Para quién? |

| Ítem | Ejemplo Pregunta |
|---|---|
| La visión de futuro | ¿Cuál es su visión de futuro?<br>¿Qué se espera de la organización en el tiempo? |
| Los valores | ¿Cuáles son sus valores?<br>¿Cómo se muestran? |
| Estructura organizacional | ¿Cómo está organizada y estructurada?<br>¿Y la seguridad de la información?<br>¿Y las responsabilidades por la seguridad? |
| El organigrama | ¿Cuál es su organigrama?<br>¿Quién es en qué sector trabaja?<br>¿Hay oficina de seguridad de la información? |
| Estrategias | ¿Cuáles son las principales estrategias del negocio?<br>¿Y de seguridad de la información? |
| Los productos | ¿Cuáles son sus productos?<br>¿Cuál es el principal producto de apalancamiento del negocio? |
| Los socios | ¿Quiénes son sus socios?<br>¿Cómo se eligen?<br>¿Cómo colaboran?<br>¿Cómo es la relación de seguridad de la información con ellos?<br>¿Cuáles son las obligaciones de seguridad de la información? |
| Los terceros | ¿Quiénes son los terceros?<br>¿Cómo se eligen?<br>¿Cómo colaboran?<br>¿Cómo es la relación de seguridad de la información con ellos?<br>¿Cómo es el contrato?<br>¿Cuáles son las obligaciones de seguridad de la información? |
| Instalaciones | ¿Cómo se divide el personal de la organización?<br>¿Dónde están los servidores?<br>¿Existe algún mecanismo para prevenir un incendio?<br>¿Cómo está hecha la protección física?<br>¿Cómo son los accesos? |
| Los funcionarios | ¿Cómo son contratados?<br>¿Hay capacitación en seguridad de la información? |

*f. Alcance y Limites*

En esta etapa se limita en qué áreas o procesos se requiere implementar la gestión del riesgo y cómo estos tienen relación con los objetivos de la organización, al igual, se debe tomar en cuenta variables como estimación de tiempos, viabilidad y presupuesto.

Se debe determinar:

- Cobertura del proceso.
- Resultados.
- Entregables.

Debe ser claro, bien definido y comprensible, con base en:

- Los objetivos y políticas de la organización.
- Estructura y funciones de la organización.
- Procesos de negocio.
- Activos.
- Expectativas.
- Restricciones:
  - Técnicas.
  - Financieras.
  - Ambientales.
  - Temporales.
  - Organizacionales.

Ejemplo de alcance y límites:

- Una aplicación de las TI.
- Un proceso de negocio.
- Una filial.
- El servicio de correo electrónico de la organización.
- El proceso de control de acceso físico de la organización.
- El datacenter de la organización.
- El servicio de callcenter.
- La red local.
- Restricción al sector, departamento o área.

## IV. PROCESO DE ANÁLISIS DEL RIESGO

Este proceso de análisis se hace para gestionar aquellos riesgos que estén bajo control o no de la organización, además de esto se deberá asesorar sobre todos los posibles incidentes que puedan ocasionar pérdidas potenciales. Al respecto conviene decir que esta tarea se realiza para evitar que en etapas posteriores se descarte algún riesgo y este se convierta en una amenaza significativa para la organización.

Dicho de otro modo, se debe realizar para conocer los posibles incidentes con potencial para causar pérdidas y ha de describirse cómo pueden suceder los eventos y tomar en cuenta los resultados, ya que estos serán los datos de entrada, de la etapa de estimación del riesgo.

Para realizar una adecuada identificación de riesgos, es necesario tener identificar claramente:

- Activos.
- Amenazas.
- Controles existentes.
- Vulnerabilidades.
- Consecuencias.

*a. Identificación de Activos [13]*

Un activo es un componente de información con valor para la organización. La norma ISO27001 nos dice que todos los activos de información deben ser identificados de una forma clara y se tiene que realizar y mantener un inventario en el que aparezcan todos los activos de información importantes.

Una empresa tiene que tener identificados todos sus activos y documentados en función de su importancia. El inventario de activos tiene que incluir toda la información que resulte necesaria con el fin de recuperarse ante un desastre, en que se incluya el tipo de activo, el formato, la ubicación, la información de respaldo, la información de licencia y el valor de negocio.

El inventario de activos no puede ser duplicado sin necesidad, pero debe estar completamente seguro de que el contenido se encuentra alineado a otros inventarios, se debe realizar una clasificación según los niveles de protección necesarios en función de la importancia de cada activo.

Sabemos que existen muchísimos tipos de activos, aunque lo más comunes son los de información, entre los que podemos incluir:

- Activos de información: son archivos, bases de datos, documentación del sistema, manuales de usuarios, material de formación, procedimientos, planes de continuidad, configuración de soporte, etc.
- Activos de software: software de aplicación, software del sistema, herramientas y programas de desarrollo, etc.
- Activos físicos: equipo de cálculo, equipo de comunicación, etc.
- Servicios: servicios de cálculo y comunicaciones,

generales, etc.
- Personas
- Activos intangibles: reputación, imagen de la organización, etc.

*b. Identificación de Amenazas*

Una amenaza es un evento de ataque a una vulnerabilidad con potencial de causar daños o pérdidas para la organización.

Estas amenazas pueden ser de origen natural o humano, también ser accidentales o deliberadas, provenientes de fuera o dentro de la organización, que afectan uno o más activos, lo cual genera impactos dependiendo de la magnitud del evento y del proceso que se ve afectado por la ocurrencia del mismos, por lo que es necesario diseñar y establecer controles efectivos, para responder oportunamente para minimizar la pérdida de información o el tiempo de recuperación.

En la Tabla IV, se presentan las actividades propuestas para la identificación de las amenazas:

TABLA IV.
ACTIVIDADES PARA LA IDENTIFICANDO LAS AMENAZAS [3]

| | |
|---|---|
| Entrada | Información.<br>Análisis crítico de incidentes.<br>Información de los responsables.<br>Catálogo de amenazas. |
| Tarea | Identificar las amenazas y su fuente.<br>NTC-ISO/ICE 27005 - 8.2.3 [4]. |
| Salida | Lista de amenazas.<br>Tipo y fuente de las amenazas. |

De otra parte, en la Tabla V, se presenta un ejemplo de amenazas humanas comunes clasificándolas por fuente de amenaza, motivación y acciones amenazantes.

TABLA V.
AMENAZAS HUMANAS [2]

| Fuente de Amenaza | Motivación | Acciones Amenazantes |
|---|---|---|
| Pirata informático, intruso ilegal. | Reto.<br>Ego.<br>Rebelión.<br>Estatus.<br>Dinero. | Piratería.<br>Ingeniería Social.<br>Intrusión, accesos forzados al sistema.<br>Acceso no autorizado. |
| Criminal de la computación. | Destrucción de la información.<br>Divulgación ilegal de la información.<br>Ganancia monetaria.<br>Alteración no autorizada de los datos. | Crimen por computador.<br>Acto fraudulento.<br>Soborno de la información.<br>Suplantación de identidad.<br>Intrusión en el sistema. |
| Terrorismo. | Chantaje.<br>Destrucción.<br>Explotación.<br>Venganza. Ganancia política.<br>Cubrimiento de los medios de comunicación. | Bomba / terrorismo.<br>Guerra de la información.<br>Ataques contra el sistema DDoS.<br>Penetración en el sistema.<br>Manipulación en el sistema. |
| Espionaje industrial (inteligencia, empresas, gobiernos extranjeros, otros intereses). | Ventaja competitiva.<br>Espionaje económico. | Ventaja de defensa.<br>Ventaja política.<br>Explotación económica.<br>Hurto de información.<br>Intrusión en privacidad personal.<br>Ingeniería social. |
| | | Penetración en el sistema<br>Acceso no autorizado al sistema. |
| Intrusos (Empleados con entrenamiento deficiente, descontentos, malintencionados, negligentes, deshonestos o despedidos). | Curiosidad.<br>Ego.<br>Inteligencia.<br>Ganancia monetaria.<br>Venganza.<br>Errores y omisiones no intencionales:<br>Error en el ingreso de datos, error de programación. | Asalto a un empleado.<br>Chantaje.<br>Observar información reservada.<br>Uso inadecuado del computador.<br>Fraude y hurto Soborno de información.<br>Ingreso de datos falsos o corruptos.<br>Interceptación de código malicioso.<br>Venta de información personal.<br>Errores en el sistema.<br>Intrusión al sistema.<br>Sabotaje del sistema.<br>Acceso no autorizado al sistema. |

*c. Identificación de los Controles Existentes*

El control es cualquier procedimiento administrativo, físico u operacional capaz de mitigar el riesgo para evitar un incidente de seguridad. La Tabla VI, hace referencia a las actividades que se deben desarrollar para la identificación de controles existentes en una organización.

TABLA VI
ACTIVIDADES PARA LA IDENTIFICACIÓN DE LOS CONTROLES EXISTENTES [3]

| | |
|---|---|
| Entrada | Documentos de los controles.<br>Planes de implementación. |
| Tarea | Identificar los controles existentes.<br>NTC-ISO/ICE 27005 - 8.2.4 [4] |
| Salida | Lista de controles existentes.<br>Su implementación y estado de uso. |

Para identificar los controles se deberá realizar: entrevistas con responsables de la seguridad y usuarios, analizar documentación existente, hacer inspecciones físicas y visitas, detectar controles complementarios requeridos, ineficaces o insuficientes, valorar la suficiencia de los controles previstos.

*d. Identificación de Vulnerabilidades*

Para la correcta identificación de las vulnerabilidades se deberá tener en cuenta los siguientes factores: la organización, los procesos y procedimientos, las rutinas de gestión y documentación, los recursos humanos (incluyendo contratistas y proveedores de servicios), las instalaciones físicas y prediales, la configuración de los sistemas de información (incluidos los sistemas operacionales y aplicaciones), el hardware, software, equipos de comunicación y las dependencias de entidades externas.

En este sentido encontramos que las vulnerabilidades de los sistemas informáticos (SI) se pueden agrupar en función de:

- Diseño:
  - Debilidad en el diseño de protocolos utilizados en las redes.
  - Políticas de seguridad deficientes e inexistentes.
- Implementación:

- Errores de programación.
- Existencia de "puertas traseras" en los sistemas informáticos.
- Descuido de los fabricantes.

- Uso:
  - Configuración inadecuada de los sistemas informáticos.
  - Desconocimiento y falta de sensibilización de los usuarios y de los responsables de informática.
  - Disponibilidad de herramientas que facilitan los ataques.
  - Limitación gubernamental de tecnologías de seguridad.
- Vulnerabilidad del día cero
  - Cuando no exista una solución "conocida" para una vulnerabilidad, pero si se conoce como explotarla, entonces se le conoce como "vulnerabilidad 0 days".

En la Tabla VII, se observan las actividades que sugiere la Guía de gestión de riesgos del MINTIC, para identificar las vulnerabilidades dentro de una organización del sector público, basados en la información previamente establecida.

TABLA VII
ACTIVIDADES PARA LA IDENTIFICACIÓN DE VULNERABILIDADES [3]

| | |
|---|---|
| Entrada | Lista de amenazas.<br>Lista de activos.<br>Lista de controles existentes. |
| Tarea | Identificar las vulnerabilidades.<br>NTC-ISO/IEC 27005 - 8.2.5 [4] |
| Salida | Lista de vulnerabilidades asociadas a los activos, a las amenazas y a los controles.<br>Lista de vulnerabilidades que no se relacionan con ninguna amenaza identificada. |

Existen diferentes metodologías para la identificación de vulnerabilidades, una de estas es el método proactivo, cuyo objetivo es crear una lista con las vulnerabilidades asociadas a los activos, las amenazas y los controles. Esta actividad se podrá apoyar en las herramientas automatizadas de búsqueda e identificación de las vulnerabilidades, así como evaluación y pruebas de seguridad, prueba de intrusión (IDS), análisis crítico de código (seguridad en el SDLC).

Las anteriores actividades se pueden realizar de dos maneras:

- De afuera hacia adentro: que se pregunta ¿qué contenido puede ser revelado de forma no autorizada? o ataques que otorguen mayores privilegios.
- De adentro hacia fuera, que consiste en revisar privilegios, vulnerabilidades que puedan atacarse, sistemas que puedan ser atacados por personal interno.

Ciertamente, las actividades que se sugieren realizar son: el monitoreo de vulnerabilidades, entrevistas en dependencias dentro del alcance o el uso de métodos proactivos tales como: ethical hacking, herramientas automatizadas, pruebas de seguridad, pruebas de intrusión, análisis de código (SDLC).

Para apoyarse en la identificación de vulnerabilidades y ejemplos de amenazas, se puede utilizar la Tabla VIII, tomada de Guía de gestión de riesgos MINITIC.

TABLA VIII
EJEMPLOS DE VULNERABILIDADES Y AMENAZAS POR TIPO DE ACTIVO [2]

| Tipo de activo | Ejemplos de vulnerabilidades | Ejemplos de amenazas |
|---|---|---|
| HARDWARE | Mantenimiento insuficiente / Instalación fallida de los medios de almacenamiento. | Incumplimiento en el mantenimiento del sistema de información. |
| | Ausencia de esquemas de reemplazo periódico. | Destrucción de equipos o medios. |
| | Susceptibilidad a la humedad, el polvo y la suciedad. | Polvo, corrosión y congelamiento. |
| | Sensibilidad a la radiación electromagnética. | Radiación electromagnética. |
| | Ausencia de un eficiente control de cambios en la configuración. | Error en el uso. |
| | Susceptibilidad a las variaciones de voltaje. | Pérdida del suministro de energía. |
| | Susceptibilidad a las variaciones de temperatura. | Fenómenos meteorológicos. |
| | Almacenamiento sin protección. | Hurtos medios o documentos. |
| | Falta de cuidado en la disposición final. | Hurtos medios o documentos. |
| | Copia no controlada. | Hurtos medios o documentos. |
| SOFTWARE | Ausencia o insuficiencia de pruebas de software. | Abuso de los derechos. |
| | Defectos bien conocidos en el software. | Abuso de los derechos. |
| | Ausencia de "terminación de sesión" cuando se abandona la estación de trabajo. | Abuso de los derechos. |
| | Disposición o reutilización de los medios de almacenamiento sin borrado adecuado. | Abuso de los derechos. |
| | Ausencias de pistas de auditoria. | Abuso de los derechos. |
| | Asignación errada de los derechos de acceso. | Abuso de los derechos. |
| | Software ampliamente distribuido. | Corrupción de datos. |
| | En términos de tiempo utilización de datos errados en los programas de aplicación. | Corrupción de datos. |
| | Interfaz de usuario compleja. | Error en el uso. |
| | Ausencia de documentación. | Error en el uso. |
| | Configuración incorrecta de parámetros. | Error en el uso. |
| | Fechas incorrectas. | Error en el uso. |
| | Ausencia de mecanismos de identificación y autentificación, como la autentificación de usuario. | Falsificación de derechos. |
| | Tablas de contraseñas sin protección. | Falsificación de derechos. |
| | Gestión deficiente de las contraseñas. | Falsificación de derechos. |
| | Habilitación de servicios innecesarios. | Procesamiento ilegal de datos. |
| | Software nuevo o inmaduro. | Mal funcionamiento del software. |
| | Especificaciones incompletas o no claras para los desarrolladores. | Mal funcionamiento del software. |
| | Ausencia de control de cambios eficaz. | Mal funcionamiento del software. |
| | Descarga y uso no controlado de software. | Manipulación con software. |
| | Ausencia de copias de respaldo. | Manipulación con software. |

| Tipo de activo | Ejemplos de vulnerabilidades | Ejemplos de amenazas |
|---|---|---|
| | Ausencia de protección física de la edificación, puertas y ventanas. | Hurto de medios o documentos. |
| | Fallas en la producción de informes de gestión. | Uso no autorizado del equipo. |
| RED | Ausencia de pruebas de envío o recepción de mensajes. | Negación de acciones. |
| | Líneas de comunicación sin protección. | Escucha encubierta. |
| | Tráfico sensible sin protección. | Escucha encubierta. |
| | Conexión deficiente de los cables. | Fallas del equipo de telecomunicaciones. |
| | Punto único de fallas. | Fallas del equipo de telecomunicaciones. |
| | Ausencia de identificación y autentificación de emisor y receptor. | Falsificación de derechos. |
| | Arquitectura insegura de la red. | Espionaje remoto. |
| | Transferencia de contraseñas en claro. | Espionaje remoto. |
| | Gestión inadecuada de la red (tolerancia a fallas en el enrutamiento). | Saturación del sistema de información. |
| | Conexiones de red pública sin protección. | Uso no autorizado del equipo. |
| PERSONAL | Ausencia del personal. | Incumplimiento en la disponibilidad del personal. |
| | Procedimientos inadecuados de contratación. | Destrucción de equipos y medios. |
| | Entrenamiento insuficiente en seguridad. | Error en el uso. |
| | Uso incorrecto de software y hardware. | Error en el uso. |
| | Falta de conciencia acerca de la seguridad. | Error en el uso. |
| | Ausencia de mecanismos de monitoreo. | Procesamiento ilegal de los datos. |
| | Trabajo no supervisado del personal externo o de limpieza. | Hurto de medios o documentos. |
| | Ausencia de políticas para el uso correcto de los medios de telecomunicaciones y mensajería. | Uso no autorizado del equipo |
| LUGAR | Uso inadecuado o descuidado del control de acceso físico a las edificaciones y los recintos. | |
| | Ubicación en área susceptible de inundación. | |
| | Red energética inestable. | |
| | Ausencia de protección física de la edificación (Puertas y ventanas). | |
| ORGANIZACION | Ausencia de procedimiento formal para el registro y retiro de usuarios. | Abuso de los derechos. |
| | Ausencia de proceso formal para la revisión de los derechos de acceso. | Abuso de los derechos. |
| | Ausencia de disposición en los contratos con clientes o terceras partes (con respecto a la seguridad). | Abuso de los derechos. |
| | Ausencia de procedimientos de monitoreo de los recursos de procesamiento de la información. | Abuso de los derechos. |
| | Ausencia de auditorías. | Abuso de los derechos. |
| | Ausencia de procedimientos de identificación y valoración de riesgos. | Abuso de los derechos. |

| Tipo de activo | Ejemplos de vulnerabilidades | Ejemplos de amenazas |
|---|---|---|
| | Ausencia de reportes de fallas en los registros de Abuso de los derechos administradores y operadores. | Abuso de los derechos. |
| | Respuesta inadecuada de mantenimiento del servicio. | Incumplimiento en el mantenimiento del sistema de información. |
| | Ausencia de acuerdos de nivel de servicio o insuficiencia de estos. | Incumplimiento en el mantenimiento del sistema de información. |
| | Ausencia de procedimientos de control de cambios. | Incumplimiento en el mantenimiento del sistema de información. |
| | Ausencia de procedimiento formal para la documentación del MSPI. | Corrupción de datos. |
| | Ausencia de procedimiento formal para la supervisión del registro del MSPI. | Corrupción de datos. |
| | Ausencia de procedimiento para la autorización de la información disponible al público. | Datos provenientes de fuentes no confiables. |
| | Ausencia de asignación adecuada de responsabilidades en seguridad de la información. | Negación de acciones. |
| | Ausencia de planes de continuidad. | Falla del equipo. |
| | Ausencia de políticas sobre el uso de correo electrónico. | Abuso de los derechos. |
| | Ausencia de procedimientos para introducción del software en los sistemas operativos. | Error en el uso. |
| | Ausencia de registros en bitácoras. | Error en el uso. |
| | Ausencia de procedimientos para el manejo de información clasificada. | Error en el uso. |
| | Ausencia de responsabilidad en seguridad de la información en la descripción de los cargos. | Error en el uso. |
| | Ausencia de los procesos disciplinarios definidos en caso de incidentes de seguridad de la información. | Hurto de equipo. |
| | Ausencia de política formal sobre la utilización de computadores portátiles. | Hurto de equipo. |
| | Ausencia de control de los activos que se encuentran fuera de las instalaciones. | Hurto de equipo. |
| | Ausencia de política sobre limpieza de escritorio y pantalla. | Hurto de medios o documentos. |
| | Ausencia de autorización de los recursos de procesamiento de información. | Hurto de medios o documentos. |
| | Ausencia de mecanismos de monitoreo establecidos para las brechas en seguridad. | Hurto de medios o documentos. |
| | Ausencia de revisiones regulares por parte de la gerencia. | Uso no autorizado de equipo. |
| | Ausencia de procedimientos para la presentación de informes sobre las debilidades en la seguridad. | Uso no autorizado de equipo. |

| Tipo de activo | Ejemplos de vulnerabilidades | Ejemplos de amenazas |
|---|---|---|
| | Ausencia de procedimientos del cumplimiento de las disposiciones con los derechos intelectuales. | Uso de software falsificado o copiado |

*e. Identificación de las Consecuencias*

La consecuencia es el resultado de un incidente de seguridad, y para identificarlas se debe tener en cuenta el escenario, que no es más que la descripción de una amenaza atacando una o más vulnerabilidades. La Tabla IX propone las siguientes actividades para la identificación de consecuencias:

TABLA IX
ACTIVIDADES PARA LA IDENTIFICACIÓN DE CONSECUENCIAS [3]

| | |
|---|---|
| Entrada | Lista de vulnerabilidades asociadas a los activos, a las amenazas y a los controles.<br>Lista de vulnerabilidades que no se refieren a ninguna amenaza identificada. |
| Tarea | Identificar las consecuencias.<br>NTC-ISO/ICE 27005 - 8.2.6 [4]. |
| Salida | Lista de escenarios de incidentes y sus consecuencias asociadas a los activos y los procesos de negocio. |

Entre las consecuencias operacionales se tiene la salud y seguridad de los profesionales involucrados, que involucra tiempo de investigación, de reparación, tiempo perdido de trabajo, costo financiero para reparar el daño, imagen y reputación.

Otro ejemplo de consecuencias son la ineficiencia o inestabilidad en el funcionamiento de los sistemas, pérdida de oportunidad de negocios y competitividad, imagen y reputación afectadas, violación de obligaciones reglamentarias, pérdidas financieras, como también pérdidas o daño de datos e información, revelación no autorizada de datos e información, la pérdida de vidas humanas.

## V. ESTIMACIÓN DEL RIESGO

Previo a evaluar los impactos en la organización como consecuencia de las amenazas a los activos críticos, se deberá revisar la información respecto a éstos y la amenaza que se habían documentado previamente durante la evaluación.

De igual modo, a de verificarse la estimación de valor para cada elemento identificado, ordenar el nivel de criticidad del riesgo y su mitigación, evaluar de forma cualitativa, cuantitativa o ambas. Para tal fin, ha de realizarse el cálculo de las consecuencias, como de la probabilidad de incidentes y estimación del nivel del riesgo, así como desarrollar un análisis cualitativo mediante la comparación de la probabilidad de ocurrencia del riesgo versus el impacto de este.

Para probabilidad:

- Alta, media y baja.
- Raro, poco probable, posible, probable y casi cierto.
- Improbable, probable y cierto.
- Pequeña, mediana y grande.
- Improbable, remota, ocasional, probable, frecuente.
- Para consecuencias (impactos):
- Alta, media y baja.
- Irrelevante, insignificante, marginal, crítico, extremo y catastrófico;
- Extremo, alto, medio, bajo y despreciable;
- Grande, mediana, pequeña y banales;
- Trastornos muy graves, graves, limitados, ligeros y muy ligeros.

TABLA X
MATRIZ DE CALIFICACIÓN, EVALUACIÓN Y RESPUESTA A LOS RIESGOS TOMADA DE LA GUÍA DE RIESGOS DAFP [1]

| PROBABILIDAD | IMPACTO | | | | |
|---|---|---|---|---|---|
| | Insignificante (1) | Menor (2) | Moderado (3) | Mayor (4) | Catastrófico (5) |
| Raro (1) | B | B | M | A | A |
| Improbable (2) | B | B | M | A | E |
| Posible (3) | B | M | A | E | E |
| Probable (4) | M | A | A | E | E |
| Casi Seguro (5) | A | A | E | E | E |

B: Zona de riesgo Baja: Asumir el riesgo
M: Zona de riesgo *Moderada:* Asumir el riesgo, Reducir el riesgo
A: Zona de riesgo *Alta*: Reducir el riesgo, Evitar, Compartir o Transferir
E: Zona de riesgo *Extrema*: Reducir el riesgo, Evitar, Compartir o Transferir

Etapas de la estimación de riesgos:

- Evaluación de las consecuencias.
- Evaluación de la probabilidad de incidentes.
- Estimación del nivel del riesgo.

*a. Evaluación de las Consecuencias*

El propósito de la evaluación de las consecuencias es valorar el impacto de un incidente de seguridad en la organización.

TABLA XI
ACTIVIDADES PARA LA IDENTIFICACIÓN DE VULNERABILIDADES [3]

| | |
|---|---|
| Entrada | Lista de escenarios de incidentes y sus consecuencias asociadas a los activos y procesos de negocio. |
| Tarea | Evaluación de las consecuencias.<br>NTC-ISO/ICE 27005. 8.3.2 [4] |
| Salida | Lista de consecuencias evaluadas. |

Los activos se pueden ordenar por medio del valor de reposición de este o a través de las consecuencias para el negocio. Ya para medir el impacto de un escenario, este se deberá determinar mediante la valoración y criticidad de los activos, para ello, se debe crear una lista de consecuencias evaluadas sobre un escenario, con base en los activos y criterios de impacto a través del valor de reposición del activo que involucra el costo financiero de recuperación o reposición y también del valor de la información que contenga. Así como también, las consecuencias al negocio.

*b. Evaluación de la Probabilidad de Incidentes*

Esta actividad se realiza observando la probabilidad de ocurrencia de algún incidente por escenario y midiendo su impacto.

La Tabla XII presenta las actividades a realizar para evaluar la probabilidad.

TABLA XII
ACTIVIDADES PARA EVALUAR LA PROBABILIDAD [3]

| | |
|---|---|
| Entrada | Lista de escenarios de incidentes, incluidos los activos afectados, vulnerabilidades atacadas y consecuencias para los activos y negocios. |
| Tarea | Evaluación de probabilidad.<br>NTC-ISO/ICE 27005. 8.3.3 [4] |
| Salida | Probabilidad de los escenarios de incidentes. |

La evaluación de la probabilidad de incidentes, se puede realizar con base a información previamente recolectada. Por ejemplo:

- Histórico: "Hace cerca de *tres años* ocurrió una falla de disponibilidad del servidor por imperfección del hardware".
- Frecuencia: "Se encontraron fallos de software y 'bloqueo' del servidor de correo electrónico y luego vuelve a funcionar. Esto ha ocurrido *cinco veces en los últimos dos mes*es".
- Facilidad: "El servidor de correo está en la sala del almacén. El personal accede directamente al servidor de correo electrónico. Esto *no es un entorno cerrado*, hay nueve personas que trabajan allí".

Adicionalmente se debe considerar la ocurrencia de amenazas de dos tipos, las denominadas amenazas intencionales y las accidentales:

- Amenazas intencionales: Estas suceden de manera previa a que alguien decide ejecutarlas y generalmente suceden por las siguiente circunstancias:
  - Motivación para atacar: conflictos con superiores e insatisfacción laboral.
  - Habilidades y conocimientos: conocimiento técnico para ciertas vulnerabilidades, para explotar otras simplemente desconectando la energía.
  - Conocimiento de la vulnerabilidad: no todos la perciben, algunos pueden conocer más detalles.
  - Poder de atracción de los activos: para causar gran daño, un servidor de e-mail puede no ser suficiente. Para otro atacante con el objetivo de sacar el servidor del aire, si lo es.
- Amenazas accidentales: Hace referencias a las que ocurren por situaciones esporádicas no controladas ni premeditadas. Por ejemplo:
  - Ubicación: Proximidad a lugares con condiciones que pueden dañar los equipos.
  - Eventos climáticos: Tales como tormentas eléctricas, inundaciones y tormentas de viento.
  - Factores facilitadores: Por un error humano accidental (como la manipulación por personal no capacitado) se generan problemas.

Al analizar un activo con base en los factores, él se puede obtener el siguiente resultado:

- Cualitativo*:* Alta probabilidad de ocurrir una falla de disponibilidad, ya que el equipo está situado en un área de alta humedad.
- Cuantitativo: Probabilidad de 75% de ocurrir un fallo de disponibilidad, ya que el equipo está situado en una zona con alta humedad.

*c. Estimación del Nivel de Riesgo*

Para el desarrollo de esta etapa se deberá medir el nivel del riesgo, usando los resultados obtenidos en las etapas anteriores y de esta manera se confieren valores a la probabilidad y consecuencias del riesgo, y además se debe dar inicio a la construcción de la tabla de análisis de riesgo. Las Tablas XIII y XIV muestran respectivamente, las actividades para la estimación del riesgo y la calificación frente al nivel de riesgo, que propone la Guía de gestión del riesgo de MINTIC.

TABLA XIII
ACTIVIDADES PARA LA ESTIMACIÓN DEL RIESGO [3]

| | |
|---|---|
| Entrada | Lista de escenarios de incidentes y sus consecuencias asociadas a los activos y procesos de negocio. |
| Tarea | Evaluación de las consecuencias.<br>NTC-ISO/ICE 27005. 8.3.2 [4] |
| Salida | Lista de consecuencias evaluadas. |

TABLA XIV
NIVEL DE RIESGO [3]

| Nivel de riesgo | Valor | Descripción |
|---|---|---|
| Extremo | 5 | De acuerdo con la organización |
| Altísimo | 4 | De acuerdo con la organización |
| Alto | 3 | De acuerdo con la organización |
| Medio | 2 | De acuerdo con la organización |
| Bajo | 1 | De acuerdo con la organización |
| Irrelevante | 0.5 | De acuerdo con la organización |

## VI. EVALUACIÓN DEL RIESGO

Para la realización de esta actividad se debe tener en cuenta las decisiones tomadas en función del nivel del riesgo aceptable, la confidencialidad, integridad, disponibilidad, la unión de riesgos pequeños y medianos que pueden generar uno más significativo, considerar la normatividad vigente y sumado a esto, es prudente cotejar los riesgos estimados con los criterios de evaluación de la fase contexto.

TABLA XV
ACTIVIDADES PARA EVALUAR EL RIESGO [3]

| | |
|---|---|
| Entrada | Lista de riesgos con niveles de valores y criterios para la evaluación de riesgos. |
| Tarea | Evaluación de riesgos.<br>NTC-ISO/ICE 27005. 8.4 [4] |
| Salida | Lista de riesgos ordenados con prioridad según los criterios de evaluación. |

Ejemplo:

A cada uno de los riesgos identificados se le asigna una probabilidad de ocurrencia, según la siguiente escala:

- Probabilidad baja = 1
- Probabilidad media = 2
- Probabilidad alta = 3

A cada uno de los riesgos identificados asígnele un valor de impacto suponiendo que se llegase a materializar, según la siguiente escala:

- Impacto bajo = 1
- Impacto medio = 2
- Impacto alto = 3

Una vez asignados los valores de probabilidad e impacto, ahora multiplique la probabilidad por el impacto para establecer la severidad del riesgo, así:

Ejemplo:

Severidad del Riesgo = Probabilidad X Impacto

El nivel de aceptación de riesgo es 3.

Eso significa que aquellos riesgos cuya severidad esté por encima de 3 serán tratados con controles y los que están por debajo de 3 solo se monitorearán.

Luego de las etapas anteriores se evalúa el trabajo realizado y en caso de que se considere insatisfactorio o incompleto, se regresa hasta la definición del contexto. De lo contrario se

continúa con esta etapa.

Se debe responder a los riesgos identificados en: la evaluación del tratamiento del riesgo ya realizado, la viabilidad técnica y financiera (costos de implementación del control), la eficacia de los controles y del tratamiento, si los niveles del riesgo residual son tolerables, las características del negocio de la organización (viabilidad económica).

## VII. TRATAMIENTO DEL RIESGO

Luego de las etapas anteriores se evalúa el trabajo realizado y en caso de que se considere incompleto, se regresa hasta la definición del contexto de lo contrario se continúa.

Se debe responder a los riesgos identificados con base en la evaluación del tratamiento del riesgo ya realizado, viabilidad técnica y financiera (costos de implementación del control), la eficacia de los controles, eficacia del tratamiento, los niveles del riesgo residual son tolerables, características de la organización.

TABLA XVI
ACTIVIDADES PARA EL TRATAMIENTO DEL RIESGO [3]

| | |
|---|---|
| Entrada | Lista de riesgos ordenados por prioridad. |
| Tarea | Tratamiento del riesgo.<br>NTC-ISO/ICE 27005. 9 [4]. |
| Salida | Plan de tratamiento del riesgo y de los riesgos residuales sujeto a aprobación. |

Después del análisis sobre los controles, se debe seleccionar la mejor opción para reducir el riesgo a un nivel aceptable o hasta un mínimo posible que se explica a continuación:

*a. Reducir el Riesgo*

Para reducir el riesgo se debe realizar mediante la selección de controles hasta que el riesgo residual pueda ser evaluado como aceptable y una forma de identificar los controles es seguir la norma NTC ISO/IEC 27002.

Para la integración de controles nuevos y existentes, se debe tener en cuenta las restricciones para seleccionar el control más adecuado:

- De tiempo.
- Financieras.
- Técnicas.
- Operativas.
- Culturales.
- Éticas.
- Ambientales.
- Legales.
- Facilidad de uso.
- Personal.

Los controles deben proporcionar uno o más tipos de protección, como *corrección* de cualquier anormalidad, *eliminación* de posibles errores y vulnerabilidades o fuentes de errores y vulnerabilidades, pero sin eliminar el riesgo, sólo reduciéndolo, *prevención* de ataques sobre las vulnerabilidades, *minimizar* el impacto, así como controles que reducen o limitan los daños, *disuasión* para hacer cambiar de intención o idea, *detección* de errores o anomalías, *recuperación* para regresar a la situación normal, *monitoreo* de señales de advertencia de vulnerabilidades, amenazas y riesgos.

Estos controles se diseñan con el fin de prevenir, generar *conciencia* con actividades de capacitación para orientar sobre la seguridad de la información, de modo que todos los usuarios estén al tanto, para aplicar los conocimientos relacionados en su rutina personal y profesional.

*b. Retener el Riesgo*

Con base en la evaluación, si el riesgo compensa los criterios para su aceptación, no es necesario implementar controles adicionales y el riesgo se puede retener.

*c. Evitar el Riesgo*

Evitar la actividad o acción que da origen al riesgo, cuando estos son muy altos o los costos de mitigación exceden los beneficios, se puede considerar: retirar la(s) actividad(es) que lo origina(n), cambiar las condiciones relacionadas.

Ejemplo: cambiar de ubicación las instalaciones a donde no haya algún riesgo natural.

*d. Transferir el Riesgo*

Es el método para compartir algunos riesgos que puede implicar la creación de unos nuevos y tratamientos adicionales, esto se puede realizar con: la adquisición de seguros (todo riesgo, entre otros), o la contratación de servicios de terceros (celaduría, vigilancia, custodia de valores, …).

*e. Riesgos Residuales*

Son los riesgos restantes luego de implementar los controles para evitarlos, transferirlos o mitigarlos. Ciertamente es factible que uno o varios controles no sean suficientes para mitigar totalmente un riesgo.

Es por ello por lo que el riesgo residual debe ser identificado y tratado a través de la implementación de los controles, si se encuentra por encima del nivel de aceptación del riesgo establecido por la organización, puede ser necesario realizar una nueva iteración.

También son riesgos residuales aquellos con poca importancia, o que deben ser aceptados.

*f. Aceptación del Riesgo*

Es el análisis del documento formal del plan de tratamiento del riesgo, el cual es realizado por la dirección y lo propone el equipo que ejecuta el proceso.

TABLA XVII
ACTIVIDADES PARA LA ACEPTACIÓN DEL RIESGO [3]

| | |
|---|---|
| Entrada | Plan de tratamiento del riesgo y análisis de los riesgos residuales. |
| Tarea | Aceptación del riesgo.<br>NTC-ISO/ICE 27005. 9 [4] |
| Salida | Lista de riesgos aceptados y las Justificaciones. |

Este documento forma parte de la llamada “Declaración de aplicabilidad”, en el que la organización presenta los controles que no son procedentes y justificados (no se incluirán en el SGSI de acuerdo con la NTC ISO/IEC 27001).

## VIII. COMUNICACIÓN DEL RIESGO

Esta actividad se desarrolla a lo largo del proceso de análisis de riesgo y se realiza un intercambio, documentado, intencional y continuo de información, conocimientos y percepciones sobre

el riesgo.

TABLA XVIII
ACTIVIDADES PARA LA COMUNICACIÓN DEL RIESGO [3]

| | |
|---|---|
| Entrada | Toda la información sobre los riesgos obtenidos en las actividades. |
| Tarea | Comunicación del riesgo.<br>NTC-ISO/ICE 27005 - 11 [4] |
| Salida | Comprensión continúa del proceso de gestión del riesgo. |

Estas actividades deben contener mayor detalle sobre los riesgos:

- La existencia de la amenaza, vulnerabilidad y riesgo.
- La naturaleza y forma de la acción.
- Probabilidad, impacto y posibles consecuencias.
- Tratamiento y aceptación del riesgo.
- La comunicación facilitará y agilizará la toma de decisiones, es bidireccional, permitirá:
- Una mejor percepción de los riesgos y de los beneficios de su rápido tratamiento.
- Realizar un trabajo de concientización acerca de la gestión del riesgo y la seguridad de la información.
- Grupo profesional integrado por las diferentes áreas y niveles.
- Reuniones periódicas de avance con directivos.

## IX. MONITOREO DEL RIESGO

El monitoreo es el proceso sistemático de observación y registro permanente de las actividades y acciones de la gestión del riesgo para verificar su estado o avance. Asimismo, el análisis crítico es una evaluación general y detallada sobre los resultados y acciones de la gestión del riesgo con base en los requisitos preestablecidos, para identificar problemas y áreas de mejoría.

Del mismo modo, el monitoreo es un procedimiento paralelo a todo el proceso de gestión de riesgo, en el cual se ha de desarrollar dos actividades como es la vigilancia y el análisis crítico de los factores de riesgo.

*a. Vigilancia*

En esta etapa se debe identificar y asegurar el control del riesgo, monitoreando el riesgo residual e identificando nuevas amenazas, vulnerabilidades y riesgos, asegurando la ejecución de los planes de tratamiento del riesgo y evaluando su eficiencia y eficacia en la reducción de estos. La información sobre los riesgos obtenidos y actividades desarrolladas se ingresa para realizar el análisis crítico y mejora del proceso.

TABLA XIX
ACTIVIDADES PARA EL MONITOREO Y ANÁLISIS CRÍTICO DE LOS FACTORES DEL RIESGO [3]

| | |
|---|---|
| Entrada | Toda la información sobre los riesgos obtenidos en las actividades. |
| Tarea | Monitoreo y análisis crítico de los factores de riesgo.<br>NTC-ISO/ICE 27005 12.1. [4] |
| Salida | Alineación continúa de la gestión del riesgo con los objetivos de negocio y con los criterios de riesgo. |

*b. Análisis Crítico de los Factores de Riesgo*

Esta actividad tiene por objetivo garantizar que el proceso de gestión del riesgo esté realmente satisfaciendo a los requisitos estratégicos del negocio de la organización.

TABLA XX
ACTIVIDADES PARA EL MONITOREO, ANÁLISIS CRÍTICO Y MEJORAMIENTO DEL PROCESO DE LA GESTIÓN [3]

| | |
|---|---|
| Entrada | Toda la información sobre los riesgos obtenidos en las actividades. |
| Tarea | Monitoreo, análisis crítico y mejora del proceso.<br>NTC-ISO/ICE 27005. 12.2. [4]. |
| Salida | Garantía permanente del proceso de gestión del riesgo para los objetivos de negoció o de actualización. |

## X. CONCLUSIONES

La privacidad y seguridad de la información, es de vital importancia para las entidades del sector público, puesto que administran información sensible de la población, susceptible de ser usa con fines mal intencionados.

De ahí la necesidad de robustecer sus niveles de protección tanto físico, lógico y humano, por cuanto estos se encuentran presentes al momento de usar la tecnología, generando diferentes niveles de exposición a vulnerabilidades con una consecuente amenaza de riesgo asociado a la pérdida de activos.

El entorno político en el que se encuentran inmersas estas organizaciones, con frecuencia afecta su desarrollo de las mismas y genera amenazas intencionales que ocurren por diferencias en pensamiento u objetivos políticos.

Parte fundamental de este proceso de gestión de riesgos, es el de establecer controles efectivos, dado que un control que no se ejecute de manera correcta o que su diseño no se adecue a los requerimientos de una organización, no va a contribuir a la mitigación de los riesgos identificados y por el contrario puede generar una falsa seguridad que pondrá en riesgo los activos y a la población.

Por último, es necesario resaltar la trascendencia de la implementación de la gestión de riesgos, sin importar cuál sea la actividad que desarrolle una organización, ya que la toma de decisiones, medidas preventivas y la continuidad del negocio puede ser la diferencia en pérdidas e impactos positivos para una organización del sector público.

## REFERENCIAS

[1] Departamento Administrativo de la Función Pública (DAFP), «Guía para la administración del riesgo,» Bogotá, 2011.
[2] Ministerio de TIC Colombia, «Guía de gestión de riesgos,» Bogotá, 2016.
[3] Renata, «Diplomado en Gobierno y,» 2018.
[4] I. 27005, Tecnología de la información. Técnicas de seguridad. Gestión del riesgo de seguridad de la información.
[5] M. T. Colombia, «Guía Metodológica de Pruebas de Efectividad,» Bogotá, 2016.
[6] ICONTEC, NTC-ISO/IEC 27005, 2013.
[7] I. ITIL, Information Technology Infrastructure Library.
[8] N. G. 73, Gestión del riesgo. Vocabulario.
[9] I. 31010, Gestión del riesgo. técnicas para el proceso de evaluación del riesgo.
[10] I. 31000, Gestión del riesgo. Principios y directrices.

[11] H. Villamil, Gestión de la Seguridad de la Información, 2016.
[12] A. 4360, Administración de Riesgos.
[13] SGSI, Blog especializado en Sistemas de Gestión de Seguridad de la Información, 2018.

**Autor**

Luis Edwin Osorio Corredor, graduado en Ingeniería de Sistemas en la Corporación Universitaria Remington, Medellín Colombia, en el 2013 y candidato a Especialista en Seguridad Informática en la Universidad Piloto de Colombia.