TABLA DE CONTENIDO

1. INTRODUCCIÓN 3

2. OBJETIVO 4

3. ALCANCE 5

4. METODOLOGÍA 6

4.1 COMPROMISO DE LA DIRECCIÓN GENERAL 7

4.2 ROLES Y RESPONSABILIDADES 7

4.3 LINEAMIENTOS PARA LAS MESAS DE TRABAJO PARA LA IDENTIFICACIÓN Y GESTIÓN DE RIESGOS
8

4.3.1 Definir el personal involucrado en los talleres o mesas de trabajo 8

4.3.2 Programación de los Talleres o mesas de Riesgos 8

4.4 DILIGENCIAMIENTO MATRIZ DE RIESGOS 8

4.4.1 Identificador del riesgo 8

4.4.2 Selección del Proceso 8

4.4.3 Selección del activo de información a analizar 9

4.4.4 Identificación de Impacto 9

4.4.5 Identificación de causa inmediata o Vulnerabilidades 9

4.4.6 Causa Raíz 11

4.4.7 Descripción de Riesgos del Proceso 12

4.4.8 Clasificación del riesgo 12

4.4.9 Frecuencia con la cual se realiza la actividad 13

4.4.10 Criterios de impacto 13

4.4.11 Controles 14

4.4.12 Opciones de tratamiento 25

4.5 MONITORIZACIÓN 27

GLOSARIO

Amenaza: Es un ente o escenario interno o externo que puede hacer uso de una vulnerabilidad para generar un perjuicio o impacto negativo en el instituto. (Materializar el riesgo).

Riesgo en la seguridad de la información: Es un escenario bajo el cual una amenaza determinada puede explotar las vulnerabilidades de los activos o grupos de activos generando un impacto negativo a la Cooperativa y evitando que ésta pueda cumplir con sus objetivos.

Vulnerabilidad: Es una falencia o debilidad que puede estar presente en la tecnología, las personas o en las políticas y procedimientos del instituto.

Amenazas: Es un ente o escenario interno o externo que puede hacer uso de una vulnerabilidad para generar un perjuicio o impacto negativo en el instituto. (Materializar el riesgo), o medios potenciales por los cuales las vulnerabilidades pueden ser explotadas u ocasionadas.

Probabilidad: Es la posibilidad que la amenaza aproveche la vulnerabilidad para materializar el riesgo.

Impacto: Son las consecuencias que genera un riesgo una vez se materialice.

Controles: Acciones o mecanismos definidos para prevenir o reducir el impacto de los eventos que ponen en riesgo, la adecuada ejecución de las actividades y tareas requeridas para el logro de objetivos de los procesos de una entidad.

1. INTRODUCCIÓN

El Ministerio de las Tecnologías y las Comunicaciones - MinTIC lidera la Política de Gobierno Digital, que tiene como propósito garantizar el máximo aprovechamiento de las Tecnologías de la información y las Comunicaciones, con el objetivo de contribuir con la construcción de un Estado más participativo, eficiente y más transparente.

En el contexto de las dinámicas asociadas al manejo y administración de la información institucional, se vienen produciendo amenazas y vulnerabilidades a la Seguridad de la Información de las entidades del orden nacional y territorial. Teniendo en cuenta, que la información es uno de los activos más importantes y estratégicos de las entidades públicas, se hace necesario definir la metodología y herramientas de administración de riesgos de Seguridad Digital aplicada al IDEAM, la actual dinámica contempla un crecimiento exponencial de la vulnerabilidad de las entidades, ante posibles ataques cibernéticos y tecnológicos, que obligan al Instituto a establecer una metodología y herramientas para la gestión de sus riesgos de seguridad de la información.

Dentro del marco del Sistema de Gestión de Seguridad de la Información -SGSI-, se debe contemplar la gestión de amenazas, y establecer controles que permitan mitigar y contener la potencial materialización de los riesgos asociados a la Seguridad de la Información en la Entidad. Esta actividad permite: identificar, analizar, evaluar y definir el manejo de los riesgos, para así apoyar el cumplimiento de los objetivos del Instituto, y administrar la materialización de dichos riesgos estableciendo controles y planes de mitigación que garanticen una adecuada y oportuna cobertura del riesgo y cumplimiento de los objetivos institucionales.

Es así que este documento técnico, enmarcado en los alcances del Modelo de seguridad y Privacidad de la Información pretende apropiar a todos los colaboradores (servidores públicos, pasantes y contratistas) y grupos de valor, acerca de la importancia del manejo responsable de la información.

2. OBJETIVO

Proteger la entidad ante la posible materialización de riesgos de seguridad de la información, de manera articulada con la metodología de Administración de Riesgos del Departamento Administrativo de la Función Pública, así como lo establecido por el Ministerio de las Tecnologías de información y las comunicaciones; y tiene como propósito fundamental salvaguardar los activos de información, entendidos estos como procesos, hardware, software, información del IDEAM, a través de la identificación, análisis, valoración, tratamiento y monitoreo de riesgos de seguridad de la información de la entidad.

Objetivos Específicos:

- Garantizar la gestión de la información y las comunicaciones y el mejoramiento continuo del modelo de seguridad y privacidad de la información de la entidad.
- Potencializar las competencias de los colaboradores del IDEAM, para identificar, reportar y gestionar los riesgos de seguridad de información, con estrategias de sensibilización y capacitación.
- Implementar, mantener y mejorar de manera periódica los controles de seguridad de la información recomendados por el modelo de seguridad y privacidad de la información, atendiendo las necesidades de grupos de valor y grupos de interés.

3. ALCANCE

Este instructivo es de obligatorio cumplimiento, y aplicable a todos los procesos y/o dependencias del IDEAM, así como a todos los colaboradores y tiene como propósito, la descripción de los criterios técnicos para la administración de los riesgos de seguridad de la información y ciberseguridad, por parte de los líderes de proceso/dependencia y su adecuada gestión, reporte y divulgación.

4. METODOLOGÍA

El enfoque de riesgos presentado se basa en la identificación de las amenazas y vulnerabilidades presentes en la información, la tecnología y las comunicaciones de todos los procesos. Se desarrolla bajo los siguientes lineamientos.

Con base en los lineamientos definidos en la Política de Seguridad Digital del Modelo Integrado de Planeación y Gestión, los estándares ISO 27001:2013 e ISO 27002:2005, el desarrollo de esta metodología consta de los siguientes puntos:

- Definir el enfoque organizacional para la valoración del riesgo:
  - Desarrollar criterios para la aceptación de riesgos, e identificar los niveles de riesgo aceptables teniendo en cuenta la metodología aplicada en el IDEAM.

- Identificar los Riesgos:
  - Identificar las amenazas a los activos relacionados previamente.
  - Identificar las vulnerabilidades que podrían ser aprovechadas por las amenazas.

- Analizar y evaluar los riesgos:
  - Estimar los niveles de los riesgos.
  - Determinar la aceptación del riesgo o la necesidad de su tratamiento.

- Identificar y evaluar las opciones para el tratamiento de los riesgos.
- Seleccionar los controles para el tratamiento de los riesgos.

Así, el objetivo de este instructivo es generar los lineamientos adecuados para la administración de riesgos; y a su vez generar un plan de tratamiento de riesgos que deberá ser ejecutado por el Instituto.

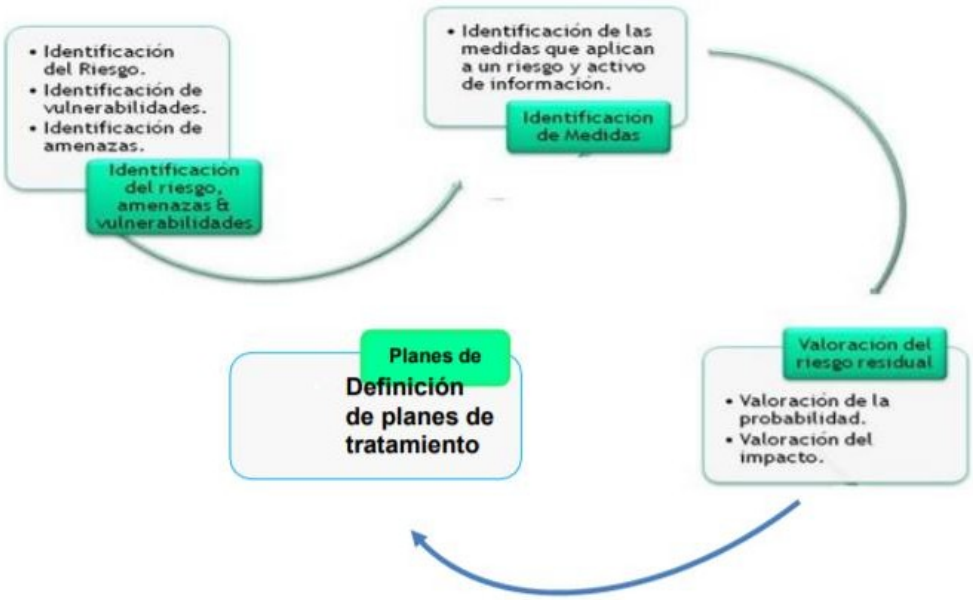

Figura 1. Actividades del Análisis de Riesgos.

4.1 COMPROMISO DE LA DIRECCIÓN GENERAL

Para el éxito en la implementación de una adecuada administración del riesgo, es indispensable el compromiso de la Dirección General del IDEAM como encargada, en primera instancia, de estimular la cultura de la identificación y prevención de riesgos y en segunda instancia de definir las políticas de administración de riesgos de seguridad de la información. Para lograrlo es importante la definición de canales directos de comunicación y el apoyo a todas las acciones emprendidas en este sentido, propiciando los espacios y asignando los recursos necesarios. Así mismo, debe designar a un directivo de primer nivel que asesore y apoye todo el proceso de diseño e implementación del componente de administración del riesgo.

4.2 ROLES Y RESPONSABILIDADES

- Líderes de proceso: serán los responsables de identificar, gestionar y realizar el seguimiento a los riesgos de seguridad de la información en las herramientas definidas para tal fin.
- Oficina de Tecnología: acompañará y asesorará a los procesos en la administración de los riesgos de seguridad de la información.
- Oficina Asesora de Planeación: asesorará a la Oficina de Tecnología en la metodología de administración de riesgos y diseño de controles, además orientará sobre el registro de la

caracterización de los riesgos en las herramientas definidas y realizará el seguimiento al monitoreo de los riesgos previamente aprobados por la Oficina de Tecnología.

- Oficina de Control Interno: realizará periódicamente los seguimientos a la gestión de riesgos de la Entidad y publicará el informe final.

4.3 LINEAMIENTOS PARA LAS MESAS DE TRABAJO PARA LA IDENTIFICACIÓN Y GESTIÓN DE RIESGOS

4.3.1 Definir el personal involucrado en los talleres o mesas de trabajo

Se debe tener en cuenta que el personal que realice la identificación de riesgos debe tener pleno conocimiento del proceso, al cual pertenecen los activos de información y de la interacción de éstosen el proceso, la caracterización y el contexto. El personal encargado de realizar el análisis de riesgos sobre los activos de información en lo posible debe ser el mismo que realizó la identificación y valoración de los activos de información de cada uno de los procesos.

4.3.2 Programación de los Talleres o mesas de Riesgos

La programación de los talleres de riesgos se realizará por procesos, es decir, que todos los procesos se citarán a reunión. Cuando se tengan activos de información que han sido identificados en todos los procesos o en varios de los procesos, se recomienda que las actividades de identificación y valoración sea realizada de forma conjunta entre todos los procesos que tienen injerencia o requieren el activode información, es así como pueden programarse reuniones conjuntas entre personal de diferentes procesos.

A partir de la identificación de activos de información los coordinadores o jefes de cada proceso, identificaran los riesgos asociados a los activos de información si hubiese lugar de acuerdo al presente instructivo y de manera articulada con la “Guía para la administración del riesgo y el diseño de controles en entidades públicas”, este proceso se debe dar en el siguiente trimestre después de la identificación y valoración de activos de información.

4.4 DILIGENCIAMIENTO MATRIZ DE RIESGOS

4.4.1 Identificador del riesgo

Corresponde a un número consecutivo asignado a cada riesgo identificado.

4.4.2 Selección del Proceso

Se relaciona el proceso donde fue identificado el riesgo de seguridad de la información.

4.4.3 Selección del activo de información a analizar (Nombre)

De los activos de información del proceso se debe seleccionar uno a uno los activos de información para realizar el análisis de riesgo.

4.4.4 Descripción del Activo de Información

Una vez identificado el contenedor del activo de información con su respectivo nombre, se procede a realizar una breve descripción del mismo, describiendo características que se consideren importantes además de su uso e importancia para la entidad.

4.4.5 Identificación de Impacto

Se identifica el tipo de impacto, este hace referencia al análisis de las consecuencias que puede ocasionar a la organización, la materialización del riesgo, en términos de afectación de la reputación, afectación económica o ambas.

4.4.6 Identificación de Causa Inmediata o Vulnerabilidades

Las vulnerabilidades son falencias o debilidades que pueden estar presentes en la tecnología, las personas o en las políticas y procedimientos de una compañía.

- Para la identificación de las vulnerabilidades se debe tener en cuenta el activo de información que se está analizando, el tipo de activo los análisis técnicos (hacking ético), físicos (controles de acceso físico), y humanos (ingeniería social) de vulnerabilidades.
- Por cada Activo de información se pueden identificar diferentes vulnerabilidades
- Para la selección de causa inmediata o vulnerabilidades se puede tener en cuenta el catálogo de vulnerabilidades disponible. Catálogo de Vulnerabilidades, sin embargo, se debe tener en cuenta que se deben identificar todas las vulnerabilidades de un activo de información independientemente de si esta se encuentra o no en el catálogo.

Vulnerabilidades
Falta de capacitación y entrenamiento para las funciones asignadas.
Inadecuado control de acceso lógico y/o físico a los activos de información.
Errores en la información obtenida de la fuente primaria.
Inexistencia de mantenimientos predictivos, preventivos y/o correctivos o no adecuados de acuerdo con lo estipulado por el fabricante.
Inadecuada ubicación de las estaciones
Se encuentra configurado un servicio FTP plano
Fallas en el disco duro
No existe gestión de vulnerabilidades técnicas
El servidor es visible desde Internet y allí se encuentra el servicio de DA
Fallas técnicas
Deficiencias en el control de acceso físico
Existencia de otras aplicaciones en el mismo servidor
Credenciales de Administración compartidas (Sistemas de Información Geográfica y Administrador Hydras)
Fallas en el suministro eléctrico
Ancho de banda deficiente
Deficiencias en el diseño del modelo de la BD y el desarrollo de la aplicación
Inadecuada gestión de cambios
Fallas en el suministro eléctrico / Falta de mantenimiento preventivo a los servidores
Deficiencias en los controles de acceso de personal externo (soporte técnico) Los proveedores externos que hacen mantenimiento tienen acceso a producción

Falta de conocimiento sobre seguridad de la información
Falta de conciencia sobre la seguridad de la información
Carencia de un presupuesto para operación y mantenimiento de TI, y/o dificultad para su ejecución
Carencia de personal idóneo para el uso de tecnologías y/o software
Falta de Abastecimiento de servicios públicos básicos: energía, agua, gas, aire acondicionado
Falta de documentación de los servicios y/o aplicaciones
Falta de políticas/normas/procedimientos de seguridad de la información
Falta de segregación de las funciones
Falta y/o inadecuada clasificación de activos de información
Inconformidad de los empleados y/o mal ambiente de trabajo
Inexistencia de respaldo y/o custodia de los activos de información
No existencia de un proceso de gestión de incidentes
Planeación de la capacidad de la plataforma inexistente o poco eficiente
Inadecuada prevención y detección de incendios
Inadecuada selección de personal para ingreso a la organización
Falta de mecanismos de monitoreo
Falta de revocación de los derechos de acceso al activo de información una vez el funcionario cambie de
rol o se retire de la organización
Carencia de procedimientos adecuados de reutilización de medios y computadores
Acceso físico no autorizado.
Ataques de Phishing
Falta de protección contra virus y código malicioso

Falla en la custodia de credenciales
Inadecuada ubicación de las estaciones
Se encuentra configurado un servicio FTP plano
Fallas en el disco duro
No existe gestión de vulnerabilidades técnicas
El servidor es visible desde Internet y allí se encuentra el servicio de DA
Fallas técnicas
Deficiencias en el control de acceso físico
Existencia de otras aplicaciones en el mismo servidor
Credenciales de Administración compartidas (Sistemas de Información Geográfica y Administrador Hydras)
Fallas en el suministro eléctrico
Ancho de banda deficiente
Deficiencias en el diseño del modelo de la BD y el desarrollo de la aplicación
Inadecuada gestión de cambios
Fallas en el suministro eléctrico / Falta de mantenimiento preventivo a los servidores
Deficiencias en los controles de acceso de personal externo (soporte técnico) Los proveedores externos que hacen mantenimiento tienen acceso a producción
Falta de conocimiento sobre seguridad de la información
Falta de conciencia sobre la seguridad de la información
Carencia de un presupuesto para operación y mantenimiento de TI, y/o dificultad para su ejecución
Carencia de personal idóneo para el uso de tecnologías y/o software
Falta de Abastecimiento de servicios públicos básicos: energía, agua, gas, aire acondicionado
Falta de documentación de los servicios y/o aplicaciones

Falta de políticas/normas/procedimientos de seguridad de la información
Mantenimiento relacionado con la infraestructura física, soporte eléctrico, ambiental y tecnológico.
Fallas en la infraestructura de IT.
Uso de protocolos inseguros.
Fallas en la transmisión de los datos porque la batería se descarga (panel solar), lo que genera rangos negativos y otro tipo de inconsistencias.

Tabla 1. Vulnerabilidades.

4.4.7 Causa Raíz

Es la causa principal o básica, corresponden a las razones por la cuales se puede presentar el riesgo, son la base para la definición de controles en la etapa de valoración del riesgo. Se debe tener en cuenta que para un mismo riesgo pueden existir más de una causa o subcausas que pueden ser analizadas, la diferencia con la anterior es que la causa inmediata hace referencia a los factores que generan el riesgo.

4.4.8 Descripción de Riesgos del Proceso

Consiste en la descripción del riesgo teniendo en cuenta que el riesgo corresponde al aprovechamiento de la vulnerabilidad encontrada y la causa raíz. Para la descripción del riesgo se puede seguir la siguiente estructura.

Figura 2. Imagen de redacción del riesgo Guía del DAFP

La descripción del riesgo debe contener todos los detalles que sean necesarios y que sea fácil de entender tanto para el líder del proceso como para personas ajenas al proceso.

La anterior estructura evita la subjetividad en la redacción y permite entender la forma como se puede manifestar el riesgo, así como sus causas inmediatas y causas principales o raíz, esta es información esencial para la definición de controles en la etapa de valoración del riesgo.

4.4.9 Clasificación del riesgo

Consiste en la selección de la clasificación del riesgo de acuerdo a su descripción la lista desplegable contiene las siguientes opciones: i) Daños Activos Físicos, ii) Ejecución y Administración de procesos, iii) Fallas Tecnológicas, iv) Fraude Externo, v) Fraude Interno, vi) Relaciones Laborales, vii) Usuarios, productos y practicas organizacionales.

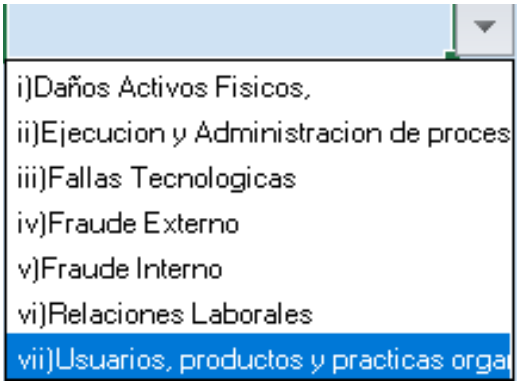

Figura 3. Clasificación del riesgo.

4.4.10 Probabilidad Inherente (frecuencia con la cual se realiza la actividad)

Defina el # de veces que se ejecuta la actividad durante el año, (Recuerde la probabilidad de ocurrencia del riesgo se define como el No. de veces que se pasa por el punto de riesgo en el periodo de 1 año). La matriz automáticamente hará el cálculo para el nivel de probabilidad inherente (Columnas L-M) Estas dos columnas no deben de ser diligenciadas dado que estas se rellenan automáticamente.

	Frecuencia de la Actividad	Probabilidad
Muy Baja	La actividad que conlleva el riesgo se ejecuta como máximos 2 veces por año	20%
Baja	La actividad que conlleva el riesgo se ejecuta de 3 a 24 veces por año	40%
Media	La actividad que conlleva el riesgo se ejecuta de 24 a 500 veces por año	60%
Alta	La actividad que conlleva el riesgo se ejecuta mínimo 500 veces al año y máximo 5000 veces por año	80%
Muy Alta	La actividad que conlleva el riesgo se ejecuta más de 5000 veces por año	100%

Figura 4. Frecuencia de la actividad.

4.4.11 Impacto Inherente (criterios de impacto)

Este valor se establece teniendo en cuenta: las consecuencias de materialización del riesgo (relación amenaza - vulnerabilidad), los controles existentes enfocados a reducir el impacto en caso de materialización y el tipo de recurso (Personas, Recursos Financieros, Desarrollo de procesos, Cumplimiento de Objetivos, Medio Ambiente, Información) afectado. Por cada tipo de recurso se cuenta con una escala que debe ser tomada como referencia para definir el valor.

ESCALA DE IMPACTO REPUTACIONAL		
100 %	Catastrófico	El riesgo afecta la imagen de la entidad a nivel nacional, con efecto publicitarios sostenible a nivel país
80%	Mayor	El riesgo afecta la imagen de la entidad con efecto publicitario sostenido a nivel de sector administrativo, nivel departamental o municipal
60%	Moderado	El riesgo afecta la imagen de la entidad con algunos usuarios de relevancia frente al logro de los objetivos
40%	Menor	El riesgo afecta la imagen de la entidad internamente, de conocimiento general nivel interno, de junta directiva y accionistas y/o de proveedores
20%	Leve	El riesgo afecta la imagen de alguna área de la organización

Tabla 2. Escala de impacto reputacional.

ESCALA DE IMPACTO DEL RECURSO FINANCIERO (SMMLV)		
100 %	Catastrófico	Mayor a 500 SMLMV
80%	Mayor	Entre 100 y 500 SMLMV
60%	Moderado	Entre 50 y 100 SMLMV
40%	Menor	Entre 10 y 50 SMLMV
20%	Leve	Afectación menor a 10 SMLMV

Tabla 3. Escala de impacto al recurso financiero.

ESCALA DE IMPACTO A LA INFORMACIÓN		
100 %	Catastrófico	El evento afecta información confidencial o estratégica o indispensable Para continuidad del negocio.
80%	Mayor	El evento puede afectar información confidencial o estratégica o Importante para la continuidad del negocio.
60%	Moderado	El evento no afecta información confidencial ni estratégica o poco Importante para la continuidad del negocio.
40%	Menor	El evento no afecta información confidencial ni estratégica o no Importante para la continuidad del negocio.
20%	Leve	No existe afectación al recurso

Tabla 4. Escala de impacto a la información.

4.4.12 Controles

Los controles deben ser identificados teniendo en cuenta la relación por amenaza- vulnerabilidad y la descripción del riesgo, estos controles pueden ser identificados tanto en las entrevistas de valoración de riesgos, como por resultado de auditorías o análisis tipo brecha de controles enmarcados en la gestión de la seguridad, los funcionarios deben validar si los controles identificados son empleados para la mitigación de los diferentes riesgos.

Para la selección de controles se puede tener en cuenta el siguiente catálogo:

Basados en el anexo A de la ISO 27001 se incluye la lista de los controles asociados a los riesgos de seguridad de la información y ciberseguridad, despliegue el listado:

5.1.1 - Políticas para la seguridad de la información: Se debería definir un conjunto de políticas para la seguridad de la información, aprobada por la dirección, publicada y comunicada a los empleados y partes externas pertinentes.

5.1.2 - Revisión de las políticas para seguridad de la información: Las políticas para seguridad de la información se deberían revisar a intervalos planificados o si ocurren cambios significativos, para asegurar su conveniencia, adecuación y eficacia continuas.
6.1.1 - Roles y responsabilidades para la seguridad de la información: Se deberían definir y asignar todas las responsabilidades de la seguridad de la información.
6.1.2 - Separación de deberes: 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.
6.1.3 - Contacto con las autoridades: Se deberían mantener contactos apropiados con las autoridades pertinentes.
6.1.4 - Contacto con grupos de interés especial: Es conveniente mantener contactos apropiados con grupos de interés especial u otros foros y asociaciones profesionales especializadas en seguridad.
6.1.5 - Seguridad de la información en la gestión de proyectos: La seguridad de la información se debería tratar en la gestión de proyectos, independientemente del tipo de proyecto.
6.2.1 - Política para dispositivos móviles: Se deberían adoptar una política y unas medidas de seguridad de soporte, para gestionar los riesgos introducidos por el uso de dispositivos móviles.
6.2.2 - Teletrabajo: 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.
7.1.1 - Selección: 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.
7.1.2 - Términos y condiciones del empleo: Los acuerdos contractuales con empleados y contratistas, deberían establecer sus responsabilidades y las de la organización en cuanto a la seguridad de la información.
7.2.1 - Responsabilidades de la dirección: 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.
7.2.2 - Toma de conciencia, educación y formación en la seguridad de la información: Todos los empleados de la organización, y en donde sea pertinente, los contratistas, deberían recibir la educación y la formación en toma de conciencia apropiada, y actualizaciones regulares sobre las políticas y procedimientos pertinentes para su cargo.
7.2.3 - Proceso disciplinario: 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.

7.3.1 - Terminación o cambio de responsabilidades de empleo: Las responsabilidades y los deberes de seguridad de la información que permanecen válidos después de la terminación o cambio de contrato se deberían definir, comunicar al empleado o contratista y se deberían hacer cumplir.
8.1.1 - Inventario de activos: 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.
8.1.2 - Propiedad de los activos: Los activos mantenidos en el inventario deberían tener un propietario.
8.1.3 - Uso aceptable de los activos: 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.
8.1.4 - Devolución de activos: 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.
8.2.1 - Clasificación de la información: La información se debería clasificar en función de los requisitos legales, valor, criticidad y susceptibilidad a divulgación o a modificación no autorizada.
8.2.2 - Etiquetado de la información: 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.
8.2.3 - Manejo de activos: Se deberían desarrollar e implementar procedimientos para el manejo de activos, de acuerdo con el esquema de clasificación de información adoptado por la organización.
8.3.1 - Gestión de medios removibles: Se deberían implementar procedimientos para la gestión de medios removibles, de acuerdo con el esquema de clasificación adoptado por la organización.
8.3.2 - Disposición de los medios: Se debería disponer en forma segura de los medios cuando ya no se requieran, utilizando procedimientos formales.
8.3.3 - Transferencia de medios físicos: Los medios que contienen información se deberían proteger contra acceso no autorizado, uso indebido o corrupción durante el transporte.
9.1.1 - Política de control de acceso: 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.
9.1.2 - Acceso a redes y a servicios en red: Solo se debería permitir acceso de los usuarios a la red y a los servicios de red para los que hayan sido autorizados específicamente.
9.2.1 - Registro y cancelación del registro de usuarios: Se debería implementar un proceso formal de registro y de cancelación de registro de usuarios, para posibilitar la asignación de los derechos de acceso.
9.2.2 - Suministro de acceso de usuarios: 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.
9.2.3 - Gestión de derechos de acceso privilegiado: Se debería restringir y controlar la asignación y uso de derechos de acceso privilegiado.

9.2.4 - Gestión de información de autenticación secreta de usuarios: La asignación de información de autenticación secreta se debería controlar por medio de un proceso de gestión formal.
9.2.5 - Revisión de los derechos de acceso de usuarios: Los propietarios de los activos deberían revisar los derechos de acceso de los usuarios, a intervalos regulares.
9.2.6 - Retiro o ajuste de los derechos de acceso: Los derechos de acceso de todos los empleados y de usuarios externos a la información y a las instalaciones de procesamiento de información se deberían retirar al terminar su empleo, contrato o acuerdo, o se deberían ajustar cuando se hagan cambios.
9.3.1 - Uso de información de autenticación secreta: Se debería exigir a los usuarios que cumplan las prácticas de la organización para el uso de información de autenticación secreta.
9.4.1 - Restricción de acceso a la información: 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.
9.4.2 - Procedimiento de ingreso seguro: Cuando lo requiere la política de control de acceso, el acceso a sistemas y aplicaciones se debería controlar mediante un proceso de ingreso seguro.
9.4.3 - Sistema de gestión de contraseñas: Los sistemas de gestión de contraseñas deberían ser interactivos y deberían asegurar la calidad de las contraseñas.
9.4.4 - Uso de programas utilitarios privilegiados: 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.
9.4.5 - Control de acceso a códigos fuente de programas: Se debería restringir el acceso a los códigos fuente de los programas.
10.1.1 - Política sobre el uso de controles criptográficos: Se debería desarrollar e implementar una política sobre el uso de controles criptográficos para la protección de la información.
10.1.2 - Gestión de llaves: 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.
11.1.1 - Perímetro de seguridad física: Se deberían definir y usar perímetros de seguridad, y usarlos para proteger áreas que contengan información sensible o crítica, e instalaciones de manejo de información.
11.1.2 - Controles físicos de entrada: Las áreas seguras se deberían proteger mediante controles de entrada apropiados para asegurar que solamente se permite el acceso a personal autorizado.
11.1.3 - Seguridad de oficinas, recintos e instalaciones: Se debería diseñar y aplicar seguridad física a oficinas, recintos e instalaciones.
11.1.4 - Protección contra amenazas externas y ambientales: Se debería diseñar y aplicar protección física contra desastres naturales, ataques maliciosos o accidentes.
11.1.5 - Trabajo en áreas seguras: Se deberían diseñar y aplicar procedimientos para trabajo en áreas seguras.

11.1.6 - Áreas de despacho y carga: 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.
11.2.1 - Ubicación y protección de los equipos: Los equipos deberían estar ubicados y protegidos para reducir los riesgos de amenazas y peligros del entorno, y las oportunidades para acceso no autorizado.
11.2.2 - Servicios de suministro: Los equipos se deberían proteger contra fallas de energía y otras interrupciones causadas por fallas en los servicios de suministro.
11.2.3 - Seguridad del cableado: El cableado de potencia y de telecomunicaciones que porta datos o soporta servicios de información debería estar protegido contra interceptación, interferencia o daño.
11.2.4 - Mantenimiento de equipos: Los equipos se deberían mantener correctamente para asegurar su disponibilidad e integridad continuas.
11.2.5 - Retiro de activos: Los equipos, información o software no se deberían retirar de su sitio sin autorización previa.
11.2.6 - Seguridad de equipos y activos fuera de las instalaciones: 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.
11.2.7 - Disposición segura o reutilización de equipos: 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 sobre escrito en forma segura antes de su disposición o reuso.
11.2.8 - Equipos de usuario desatendidos: Los usuarios deberían asegurarse de que a los equipos desatendidos se les dé protección apropiada.
11.2.9 - Política de escritorio y pantalla limpios: 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.
12.1.1 - Procedimientos de operación documentados: Los procedimientos de operación se deberían documentar y poner a disposición de todos los usuarios que los necesiten.
12.1.2 - Gestión de cambios: 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.
12.1.3 - Gestión de capacidad: 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.
12.1.4 - Separación de los ambientes de desarrollo, pruebas y operación: Se deberían separar los ambientes de desarrollo, prueba y operación, para reducir los riesgos de acceso o cambios no autorizados al ambiente de operación.

12.2.1 - Controles contra códigos maliciosos: 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.
12.3.1 - Respaldo de la información: 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.
12.4.1 - Registro de eventos: Se deberían elaborar, conservar y revisar regularmente los registros acerca de actividades del usuario, excepciones, fallas y eventos de seguridad de la información.
12.4.2 - Protección de la información de registro: Las instalaciones y la información de registro se deberían proteger contra alteración y acceso no autorizado.
12.4.3 - Registros del administrador y del operador: Las actividades del administrador y del operador del sistema se deberían registrar, y los registros se deberían proteger y revisar con regularidad.
12.4.4 - Sincronización de relojes: Los relojes de todos los sistemas de procesamiento de información pertinentes dentro de una organización o ámbito de seguridad se deberían sincronizar con una única fuente de referencia de tiempo.
12.5.1 - Instalación de software en sistemas operativos: Se deberían implementar procedimientos para controlar la instalación de software en sistemas operativos.
12.6.1 - Gestión de las vulnerabilidades técnicas: 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.
12.6.2 - Restricciones sobre la instalación de software: Se deberían establecer e implementar las reglas para la instalación de software por parte de los usuarios.
12.7.1 - Controles sobre auditorías de sistemas de información: 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.
13.1.1 - Controles de redes: Las redes se deberían gestionar y controlar para proteger la información en sistemas y aplicaciones.
13.1.2 - Seguridad de los servicios de red: 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.
13.1.3 - Separación en las redes: Los grupos de servicios de información, usuarios y sistemas de información se deberían separar en las redes.
13.2.1 - Políticas y procedimientos de transferencia de información: 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.
13.2.2 - Acuerdos sobre transferencia de información: Los acuerdos deberían tener en cuenta la transferencia segura de información del negocio entre la organización y las partes externas.

13.2.3 - Mensajería electrónica: Se debería proteger adecuadamente la información incluida en la mensajería electrónica.

13.2.4 - Acuerdos de confidencialidad o de no divulgación: 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.

14.1.1 - Análisis y especificación de requisitos de seguridad de la información: 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.

14.1.2 - Seguridad de servicios de las aplicaciones en redes públicas: 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.

14.1.3 - Protección de transacciones de los servicios de las aplicaciones: 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.

14.2.1 - Política de desarrollo seguro: Se deberían establecer y aplicar reglas para el desarrollo de software y de sistemas, a los desarrollos que se dan dentro de la organización.

14.2.2 - Procedimientos de control de cambios en sistemas: 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.

14.2.3 - Revisión técnica de las aplicaciones después de cambios en la plataforma de operación: 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.

14.2.4 - Restricciones en los cambios a los paquetes de software: 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.

14.2.5 - Principios de construcción de sistemas seguros: Se deberían establecer, documentar y mantener principios para la construcción de sistemas seguros, y aplicarlos a cualquier actividad de implementación de sistemas de información.

14.2.6 - Ambiente de desarrollo seguro: 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.

14.2.7 - Desarrollo contratado externamente: La organización debería supervisar y hacer seguimiento de la actividad de desarrollo de sistemas contratados externamente.

14.2.8 - Pruebas de seguridad de sistemas: Durante el desarrollo se deberían llevar a cabo pruebas de funcionalidad de la seguridad.

14.2.9 - Prueba de aceptación de sistemas: Para los sistemas de información nuevos, actualizaciones y nuevas versiones, se deberían establecer programas de prueba para aceptación y criterios de aceptación relacionados.
14.3.1 - Protección de datos de prueba: Los datos de ensayo se deberían seleccionar, proteger y controlar cuidadosamente.
15.1.1 - Política de seguridad de la información para las relaciones con proveedores: Los requisitos de seguridad de la información para mitigar los riesgos asociados con el acceso de proveedores a los activos de la organización se deberían acordar con estos y se deberían documentar.
15.1.2 - Tratamiento de la seguridad dentro de los acuerdos con proveedores: 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.
15.1.3 - Cadena de suministro de tecnología de información y comunicación: 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.
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.
15.2.2 - Gestión de cambios en los servicios de los proveedores: Se deberían gestionar los cambios en el suministro de servicios por parte de los proveedores, incluido el mantenimiento y la mejora delas 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.
16.1.1 - Responsabilidades y procedimientos: 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.
16.1.2 - Reporte de eventos de seguridad de la información: Los eventos de seguridad de la información se deberían informar a través de los canales de gestión apropiados, tan pronto como sea posible.
16.1.3 - Reporte de debilidades de seguridad de la información: 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.
16.1.4 - Evaluación de eventos de seguridad de la información y decisiones sobre ellos: 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.
16.1.5 - Respuesta a incidentes de seguridad de la información: Se debería dar respuesta a los incidentes de seguridad de la información de acuerdo con procedimientos documentados.

16.1.6 - Aprendizaje obtenido de los incidentes de seguridad de la información: El conocimiento adquirido al analizar y resolver incidentes de seguridad de la información se debería usar para reducir la posibilidad o el impacto de incidentes futuros.
16.1.7 - Recolección de evidencia: La organización debería definir y aplicar procedimientos para la identificación, recolección, adquisición y preservación de información que pueda servir como evidencia.
17.1.1 - Planificación de la continuidad de la seguridad de la información: 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.
17.1.2 - Implementación de la continuidad de la seguridad de la información: 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.
17.1.3 - Verificación, revisión y evaluación de la continuidad de la seguridad de la información: 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 válidos y eficaces durante situaciones adversas.
17.2.1 - Disponibilidad de instalaciones de procesamiento de información.: Las instalaciones de procesamiento de información se deberían implementar con redundancia suficiente para cumplir los requisitos de disponibilidad.
18.1.1 - Identificación de la legislación aplicable y de los requisitos contractuales: Todos los requisitos estatutarios, reglamentarios y contractuales pertinentes, y el enfoque de la organización para cumplirlos, se deberían identificar y documentar explícitamente y mantenerlos actualizados para cada sistema de información y para la organización.
18.1.2 - Derechos de propiedad intelectual: 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.
18.1.3 - Protección de registros: Los registros se deberían proteger contra pérdida, destrucción, falsificación, acceso no autorizado y liberación no autorizada, de acuerdo con los requisitos legislativos, de reglamentación, contractuales y de negocio.
18.1.4 - Privacidad y protección de información de datos personales.: 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.
18.1.5 - Reglamentación de controles criptográficos: Se deberían usar controles criptográficos, en cumplimiento de todos los acuerdos, legislación y reglamentación pertinentes.
18.2.1 - Revisión independiente de la seguridad de la información: El enfoque de la organización para la gestión de la seguridad de la información y su implementación (es decir, los objetivos de control, los controles, las políticas, los procesos y los procedimientos para seguridad de la información) se

deberían revisar independientemente a intervalos planificados o cuando ocurran cambios significativos.

18.2.2 - Cumplimiento con las políticas y normas de seguridad: 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.

18.2.3 - Revisión del cumplimiento técnico: Los sistemas de información se deberían revisar periódicamente para determinar el cumplimiento con las políticas y normas de seguridad de la información.

4.4.12.1 Atributos de los Controles

Los controles orientados a atacar la causa raíz para prevenir la materialización del riesgo tienen en cuenta que cada líder de proceso o su representante deben definir, implementar y monitorear los controles establecidos.

Para establecer el control se tendrá en cuenta:

- La identificación del cargo que es responsable del control.
- La acción del control se redacta como verbo en infinitivo.
- El complemento o los detalles que identifican el objeto de control.

Atributos de Eficiencia

Características			Descripción	Peso
Atributos de Eficiencia	Tipo	Preventivo	Va hacia las causas del riesgo, aseguran el resultado final esperado.	35%
		Detectivo	Detecta que algo ocurre y devuelve el proceso a los controles preventivos. Se pueden generar procesos	15%
		Correctivo	Dado que permiten reducir el impacto de la materialización del riesgo, tienen un costo en su implementación.	10%
	Implementación	Automático	Son actividades de procesamiento o validación de información que se ejecutan por un sistema y/o aplicativo de manera automática sin la intervención de personas para su realización.	30%

		Manual	Controles que son ejecutados por una persona., tiene implícito el error humano.	**15%**

Tabla 5. Atributos de los Controles Eficiencia

Atributos de Formalización

Características			Descripción	Peso
Atributos de Formalización	**Documentación**	**Documentado**	Controles que están documentados en el proceso, ya sea en manuales, procedimientos, flujogramas o cualquier otro documento propio del proceso.	**10%**
		Sin Documentar	Identifica a los controles que pese a que se ejecutan en el proceso no se encuentran documentados en ningún documento propio del proceso	**2%**
	Frecuencia	**Continua**	Este atributo identifica a los controles quese ejecutan siempre que se realiza la actividad originadora del riesgo.	**15%**
		Aleatoria	Este atributo identifica a los controles que no siempre se ejecutan cuando se realiza la actividad originadora del riesgo	**5%**
	Evidencia	**Con Registro**	El control deja un registro que permite evidenciar la ejecución del control	**10%**
		Sin Registro	El control no deja registro de la ejecución del control	**2%**

Tabla 6. Atributos de los Controles formalización

Una vez se establecen los controles, se da un movimiento en los ejes de probabilidad o impacto, de acuerdo con el tipo de control aplicado. Los controles de prevención y detección atacan la probabilidad de ocurrencia; y, los controles de corrección atacan el impacto una vez se ha materializado el riesgo. En caso de no contar con controles de corrección, el impacto residual es el mismo calculado inicialmente. Es importante señalar que en este caso no será posible su movimiento en la matriz para el impacto.

El nivel de riesgo final es el resultado del movimiento en los ejes de acuerdo con el tipo de control aplicado.

4.4.12 Opciones de tratamiento

En esta casilla se determina la estrategia que se va a seguir con el fin de reducir el impacto del riesgo

4.4.12.1 Evitar o eliminar el riesgo

En este caso, se implementan las acciones para hacer que las condiciones o los factores que pueden generar el riesgo desaparezcan, y con ellos, el riesgo. Esta es una opción para aquellos casos de alta probabilidad de ocurrencia, con un muy alto impacto negativo

4.4.12.2 Reducir o mitigar

No siempre es posible eliminar el riesgo. O, quizás, eliminarlo completamente resulta mucho más costoso que las consecuencias negativas de que este llegara a suceder. En esos casos, procedemos a implementar acciones para reducir o mitigar

4.4.12.3 Transferir o compartir

Esto significa que pasamos el problema a alguien más. En nuestro primer ejemplo sobre el peligro de los archivos, la organización no cuenta inicialmente con las herramientas y los mecanismos para preservar con seguridad su información documentada. Así, decide “transferir” el problema a proveedores.

4.4.12.4 Aceptar el riesgo

Finalmente, cuando no tenemos otra opción, debemos aceptar el riesgo. Se trata de no hacer nada. Simplemente, sabemos que no tenemos como evitarlo y debemos convivir con él. Las organizaciones deciden aceptar un riesgo, cuando este es de muy baja probabilidad de ocurrencia. La posibilidad de que las instalaciones de la organización sean destruidas por un terremoto, es un ejemplo de ello.

4.4.13 Matriz opciones Riesgo

PROBABILIDAD		IMPACTO				
		Sin Afectación	Leve	Moderado	Crítico	Muy Crítico
		1	2	3	4	5
Casi Certeza	5	>Evitar el riesgo. >Reducir el riesgo. >Compartir o transferir los riesgos	>Evitar el riesgo. >Reducir el riesgo. >Compartir o transferir los riesgos	>Evitar el riesgo. >Reducir el riesgo. >Compartir o transferir los riesgos	>Evitar el riesgo. >Reducir el riesgo. >Compartir o transferir los riesgos	>Evitar el riesgo. >Reducir el riesgo. >Compartir o transferir los riesgos
Probable	4	>Evitar el riesgo. >Reducir el riesgo. Compartir o transferir los riesgos	>Evitar el riesgo. >Reducir el riesgo. >Compartir otransferir los riesgos	>Evitar el riesgo. >Reducir el riesgo. >Compartir o transferir los riesgos	>Evitar el riesgo. >Reducir el riesgo. >Compartir o transferir los riesgos	>Evitar el riesgo. >Reducir el riesgo. >Compartir o transferir los riesgos
Posible	3	>Asumir el riesgo	>Evitar el riesgo. >Reducir el riesgo. >Compartir o transferir los riesgos	>Evitar el riesgo. >Reducir el riesgo. >Compartir o transferir los riesgos	>Evitar el riesgo. >Reducir el riesgo. >Compartir o transferir los riesgos	>Evitar el riesgo. >Reducir el riesgo. >Compartir o transferir los riesgos
Improbable	2	>Asumir el riesgo	>Asumir el riesgo	>Evitar el riesgo. >Reducir el riesgo. >Compartir o transferir los riesgos	>Evitar el riesgo. >Reducir el riesgo. >Compartir o transferir los riesgos	>Evitar el riesgo. >Reducir el riesgo. >Compartir o transferir los riesgos
Raro	1	>Asumir el riesgo	>Asumir el riesgo	>Evitar el riesgo. >Reducir el riesgo. >Compartir o transferir los riesgos	>Evitar el riesgo. >Reducir el riesgo. >Compartir otransferir los riesgos	>Evitar el riesgo. >Reducir el riesgo. >Compartir otransferir los riesgos

Tabla 7. Matriz de Opciones de Tratamiento

4.4.14 Definición de planes de tratamiento (Plan de Acción)

Se deben definir actividades para alcanzar los planes de tratamiento para la aplicación de controles en los activos de información que se encuentren por fuera del nivel de riesgo aceptable.

Tal como lo contempla la Guía de Administración del Riesgo del DAFP (Departamento Administrativo de la Función Pública), los riesgos calificados como Extremos y Altos serán incluidos dentro de los planes de mitigación, y los riesgos calificados como Medios y Bajos serán monitoreados.

4.5 MONITORIZACIÓN

Una vez diseñado y validado el plan de acción para administrar los riesgos, en el mapa de riesgos, es necesario monitorearlo teniendo en cuenta que estos nunca dejan de representar una amenaza para el Instituto.

El monitoreo es esencial para asegurar que las acciones se están llevando a cabo y evaluar la eficacia en su implementación adelantando revisiones sobre la marcha para evidenciar todas aquellas situaciones o factores que pueden estar influyendo en la aplicación de las acciones preventivas.

A partir del análisis y calificación de riesgos, se debe formular un plan para el tratamiento de riesgos que identifique la gestión apropiada, los recursos, responsabilidad y prioridades para manejar los riesgos de seguridad de la información.

Se debe asignar un Responsable de la implementación de Plan de Acción, definir la fecha de implementación, contar con evidencias de seguimiento, registrar el Estado en porcentaje del avance en la implementación y realizar observaciones importantes.

El IDEAM debe ejecutar procedimientos de seguimiento y revisión para detectar oportunamente los errores en los procesamientos e identificar con prontitud incidentes e intentos de violación de seguridad, así como determinar si las acciones tomadas para solucionar un problema de seguridad fueron eficaces.

HISTORIAL DE CAMBIOS

VERSIÓN	FECHA	DESCRIPCIÓN
01	01/11/2017	Creación del documento
02	15/03/2018	Actualización del documento
03	21/12/2021	Actualización del documento Se cambió el nombre del **INSTRUCTIVO RIESGOS DE SEGURIDAD por INSTRUCTIVO RIESGOS DE SEGURIDAD DE LA INFORMACIÓN**
04	25/02/2022	Actualización Documento, re asignación peso a atributos de calificación de los controles, se ajustan tablas, se incluye casillas Responsable, Fecha Seguimiento, Estado y Observaciones

ELABORÓ:	REVISÓ:	APROBÓ:
Guillermo Otálora Luna Oficial de Seguridad Información	**Eduardo Emilio Ramírez** Coordinador GAESI	**Alicia Barón Leguizamón** Jefa de la Oficina de Informática