



ANEXO B

Guía para la metodología de gestión de riesgos

CTIC-SE-P1-v.1.0



AGETIC

agencia de gobierno electrónico y
tecnologías de información y comunicación

GUÍA PARA LA METODOLOGÍA DE GESTIÓN DE RIESGOS

1 . Introducción

Los lineamientos para la elaboración del Plan Institucional de Seguridad de la Información establecen que la entidad o institución pública deberá adoptar un estándar y/o metodología de gestión de riesgos dentro de los alcances del Plan, con el objetivo de implementar controles de seguridad o mejorar la eficacia de los controles ya existentes.

La presente guía brinda orientación para elaborar la metodología de gestión de riesgos acorde a las directrices establecidas en los lineamientos para la elaboración del Plan Institucional de Seguridad de la Información.

La entidad o institución pública es libre de elegir el método o metodología para la Gestión de riesgos.

2 . Objetivo

La presente guía tiene el objetivo de orientar en la metodología de gestión de riesgos a partir del cual se realizará:

- a) Identificación, Clasificación y Valoración de Activos de Información.
- b) La Evaluación del Riesgo.
- c) Tratamiento del Riesgo.
- d) Controles Implementados y por Implementar.

Esta guía toma como referencia la Metodología de Análisis y Gestión de Riesgos MAGERIT. Sin embargo, la entidad o institución pública es libre de elegir el método o metodología que considere adecuada para realizar la gestión de riesgos siempre y cuando esta se encuentre bajo algún estándar nacional o internacional.

3 . Referencias

La presente guía toma como referencia el inventario de activos de información que sugiere la metodología de análisis y gestión de riesgos MAGERIT.

4 . Documentos relacionados

La presente guía tiene relación con los siguientes documentos:

- Lineamientos para la elaboración e implementación de los Planes Institucionales de Seguridad de la Información de las Entidades del Sector Público.

- MAGERIT - Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información Versión 3.
- Estándares de la Familia ISO 27000 de Tecnologías de la Información – Técnicas de Seguridad – Sistemas de Gestión de la Seguridad de la Información.
- Si bien la presente guía hace referencia a buenas prácticas de gestión de riesgos del estándar NB/ISO/IEC 27005:2010, la misma no obliga su adopción. Existen normas, estándares y marcos de trabajo y metodologías como la NB/ISO 31000:2014, Objetivos de Control para Información y Tecnologías Relacionadas (COBIT), Biblioteca de Infraestructura de Tecnologías de Información (ITIL) entre otros y dependerá de la necesidad y experiencia de cada entidad o institución pública en gestión de riesgos.

5 . Términos y definiciones

Activo.- En general, activo es todo aquello que tiene valor para la entidad o institución pública.

Activo de información.- Conocimientos o datos que tienen valor para la organización.¹

Responsable del activo de información.- Servidor público de nivel jerárquico quien tiene la responsabilidad y las atribuciones de establecer los requisitos de seguridad y la clasificación de la información relacionada al activo, según el alcance definido del proceso al cual pertenece la misma.

Custodio del activo de información.- El servidor público encargado de administrar y hacer efectivo los controles de seguridad, que el responsable del activo de información haya definido.

Confidencialidad: Propiedad que determina que la información no esté disponible ni sea revelada a individuos, entidades o procesos autorizados.²

Integridad: Propiedad de salvaguardar la exactitud y completitud de los activos.³

Disponibilidad.- Propiedad de ser accesible y utilizable por solicitud de una entidad autorizada.⁴

Amenaza.- Causa potencial de un incidente no deseado, que puede dar lugar a daños en un sistema o en una organización.⁵

Riesgo.- Combinación de la probabilidad de un evento adverso y su consecuencia.⁶

1 Términos y Definiciones NB/ISO/IEC 27000:2010

2 Términos y Definiciones NB/ISO/IEC 27000:2010

3 Términos y Definiciones NB/ISO/IEC 27000:2010

4 Términos y Definiciones NB/ISO/IEC 27000:2010

5 Términos y Definiciones NB/ISO/IEC 27000:2010

6 Términos y Definiciones NB/ISO/IEC 27000:2010

Vulnerabilidad.- Debilidad de un activo o control, que puede ser explotada por una amenaza.⁷

Impacto.- Cambio adverso en la operación normal de un proceso de la institución pública.⁸

6 . Identificación, clasificación y valoración de activos de información

La identificación del inventario de activos de información permite clasificar y valorar el activo en términos cuantitativos o cualitativos, para brindar un mejor tratamiento y protección se debe identificar, especificar claramente sus características y la función al interior de los procesos alineados con los objetivos y alcances definidos.

Las directrices establecidas en el Anexo A sobre Gestión de Activos de Información mencionan la responsabilidad por los activos de información que contemple: el inventario, propiedad, custodia y el uso aceptable de los mismos.

Las actividades para realizar y gestionar el inventario de activos de información son la identificación, valoración, revisión y actualización.

6.1 . Identificación

Consiste en determinar e identificar qué activos de información formarán parte del inventario. El Responsable de Seguridad de la Información debe orientar la correcta identificación de los mismos conjuntamente con los responsables o dueños de los procesos institucionales, dentro de los alcances definidos en el Plan Institucional de Seguridad de la Información.

Para la identificación de activos de información se sugiere la siguiente clasificación:

Información

En esta clasificación ingresan procesos relevantes para la institución e información en cualquier medio de soporte físico o digital. Los tipos de información que ingresarían son: información estratégica, información relacionada con el archivo personal, información relacionada a la documentación administrativa, legal, procesos de adjudicación y otros que tengan un coste económico y de cumplimiento con la normativa legal. También, en esta categoría está la información de archivos tales como respaldos, documentos, credenciales de acceso, entre otros.

Claves criptográficas

Algunos de los ejemplos de activos en esta categoría son: claves para cifrar, firmar, certificados x509, entre otros.

Servicios

En esta categoría ingresan: servicios de acceso remoto, transferencia de archivos, correo electrónico, servicios web, servicio de directorio, entre otros.

7 Términos y Definiciones NB/ISO/IEC 27000:2010

8 Términos y Definiciones NB/ISO/IEC 27000:2010

Software – aplicaciones informáticas

En esta categoría se encuentran: sistemas desarrollados y/o adquiridos, software de aplicación, sistemas operativos, software de virtualización, entre otros.

Equipamiento informático (Hardware)

En esta categoría están los medios físicos que soportan los procesos como ser: servidores, equipamiento de escritorio, periféricos, dispositivos de red perimetral, dispositivos de red, corta fuegos, entre otros.

Redes de comunicaciones

Están los servicios de comunicaciones como ser: la red telefónica, redes de datos, internet, entre otros.

Soportes de información

En esta categoría están: discos virtuales y físicos, memorias usb, discos y cintas, material impreso, entre otros.

Equipamiento auxiliar

En esta categoría están: fuentes de alimentación, generadores eléctricos, equipos de climatización, cableado eléctrico, mobiliario, entre otros.

Instalaciones

Edificio, vehículos, instalaciones de refuerzo, entre otros.

Personal

Incluye personal fijo, eventual, terceros, entre otros.

También se debe identificar a los responsables y custodios de la información asociada al activo; esto es importante porque a través de la identificación se realizará una mejor valoración para resguardar la información. Los custodios podrían ser los mismos servidores públicos o en otros casos una persona ajena a la entidad o institución pública.

6.2 . Valoración

La valoración de activos de información tiene como objetivo asegurar que la información asociada a los mismos reciba niveles de protección adecuados, ya que en base a su valor y otras características particulares se requerirá implementar o mejorar controles de seguridad.

Las características o atributos hacen que un activo sea valioso, estas se utilizan para valorar las consecuencias de la materialización de una amenaza, que a su vez produce perjuicio a los procesos relacionados y la afectación de activo en una o todas las propiedades de la información: disponibilidad, integridad y confidencialidad, además de otras como la autenticidad, trazabilidad y no repudio. Si se ve conveniente la entidad o institución pública tomará la decisión de valorar el activo en las dimensiones que requiera.

A continuación se conceptualizan las propiedades de la información asociadas a activos para la valoración:

Disponibilidad

Un activo tiene gran valor, desde el punto de vista de disponibilidad, si es que una amenaza afectase su disponibilidad con consecuencias graves para el normal desarrollo de las actividades. Por el contrario, un activo carece de un valor apreciable cuando puede no estar disponible por largos periodos de tiempo sin afectar o causar daño a las actividades de la entidad o institución pública.

Integridad

Una valoración alta de esta propiedad se da por el grado de afectación (daño grave) causado por la alteración voluntaria o no intencionada de los datos. Por el contrario, una valoración menor se da cuando su modificación no supone preocupación alguna.

Confidencialidad

La valoración de esta característica está en función del grado de afectación que ocasionaría la revelación o divulgación de información a personas no autorizadas.

En la presente guía se toma la valoración cualitativa, pero no limita a que la entidad realice la valoración cuantitativa y defina su propia escala de valoración, siempre y cuando esta se encuentre respaldada y aprobada.

La valoración la debe dar el reponsable del activo de información. Estas pueden ser en base a percepción, eventos anteriores relacionados a las propiedades de la información y otros.

La escala recomendada para la valoración cualitativa de las características del activo de información se presenta en la siguiente figura.

Figura 1. Escala de Valoración de Activos

Escala de Valoración	
1	Muy Bajo
2	Bajo
3	Medio
4	Alto
5	Muy Alto

La entidad está en libertad de establecer sus propias escalas para valorar los activos de información.

También es conveniente realizarse las siguientes preguntas para clarificar la valoración asociada a cada característica del activo de información.

Tabla 1. Preguntas para Valoración de Activos

Disponibilidad	¿Qué importancia tendría que el activo no estuviera disponible?
Integridad	¿Qué importancia tendría que la información asociada al activo fuera modificada sin control?
Confidencialidad	¿Qué importancia tendría que la información asociada al activo fuera conocida por personas no autorizadas?

La valoración de cada una de las características estará en función a la escala y la posterior valoración final del activo, que será el promedio de las tres características.

6.2.1 . Ejemplo

Imaginemos que el responsable del activo de información es el Responsable de Tecnologías de Información de la entidad y este identifica un activo: “Servidor de Correo Institucional” que es el servicio por el cual se mantienen la comunicación y envío de archivos al interior y exterior de la entidad. Se le pide que valore el servicio en términos de disponibilidad, confidencialidad e integridad de la información, asociada al servicio identificado y este es el resultado:

Tabla 2. Ejemplo de la Valoración de Activos

Disponibilidad	Alto
Integridad	Muy Alto
Confidencialidad	Medio

Además identifica que los custodios del activo son los usuarios que hacen uso del servicio. La valoración final del activo se da promediando las tres propiedades, por lo tanto su valoración llega a ser: Alto.

6.2.2 . Matriz de inventario y valoración

Para materializar la Identificación, Clasificación y Valoración de Activos de Información se sugiere el uso de la siguiente matriz:

Figura 2. Matriz de Inventario y Valoración

1	A	B	C	D	E	F	G	H	I	K	M	P	Q	R
2	INSTITUCIÓN:													
3	FECHA ELABORACIÓN:													
4	FECHA APROBACIÓN:													
5														
6	INVENTARIO DE ACTIVOS IDENTIFICADOS								VALORACIÓN DE ACTIVOS			VALORACIÓN FINAL	GESTIÓN	
7	#	Activo	Descripción	Tipo	Ubicación	Unidad Responsable	Responsable	Custodio	Disponibilidad	Integridad	Confidencialidad		Fecha de Ingreso	Fecha de Salida
8														
9														
10														
11														
12														
13														
14														
15														
16														
17														
18														
19														
20														
21														
22														
23														
24														
25														
26														
27	Elaborado por:					Aprobado por:								
28	Firma:					Firma:								
29	Cargo:					Cargo:								
30														

La información del encabezado consta del nombre de la institución, fecha de elaboración y fecha de aprobación.

El detalle de los campos del inventario se describen a continuación:

- **Activo:** Nombre del activo de información identificado.
- **Descripción:** Descripción del activo inventariado.
- **Tipo:** Clasificación del activo de acuerdo a MAGERIT u otro que se estime necesario.
- **Ubicación:** Detalle del lugar físico donde se encuentra el activo agregando condiciones de seguridad en las que se encuentra el activo.
- **Unidad Responsable:** La unidad organizacional responsable del activo.
- **Responsable:** Nombre y cargo de la persona responsable del activo; con frecuencia es la persona más idónea para determinar el valor que el activo tiene para la institución. El responsable puede no tener derechos de propiedad sobre el activo, pero tiene la responsabilidad de su producción, desarrollo, mantenimiento, uso y seguridad según corresponda.
- **Custodio:** Nombre y cargo del encargado de resguardar la información.
- **Valoración de Activos:** De acuerdo a la confidencialidad, integridad y disponibilidad.
- **Valoración Final:** Valoración final promedio de la confidencialidad, disponibilidad e integridad.
- **Fecha de Ingreso:** Fecha de ingreso del activo de información en el inventario.
- **Fecha de Salida:** Fecha de exclusión del activo de información del inventario.

El inventario elaborado debe ser coordinado y aprobado por las partes interesadas (responsable del activo de información) de los procesos identificados.

6.3 . Revisión y actualización

La revisión es la verificación que se lleva a cabo para determinar si un activo continua siendo parte del inventario.

El inventario puede ser revisado o validado en cualquier momento a solicitud del responsable de seguridad de la información. Entre las razones por la que se debería realizar una revisión son:

- Actualizaciones al proceso al que pertenece el activo.
- Inclusión de nuevos procesos y procedimientos.
- Inclusión de un nuevo activo.
- Desaparición de una unidad organizacional, proceso o cargo en la entidad que tenía asignado el rol de responsable o custodio.
- Cambios o migraciones de sistemas de información en donde se almacenan o reposan activos de la ubicación ya inventariados.
- Cambios físicos de la ubicación de activos de información.

La actualización, fruto de la revisión, debe estar sujeta a control de cambios que permita identificar la fecha, el autor, los motivos por el cual se actualiza y otros que son necesarios para el control.

6.4 . Reserva

El inventario de activos de información debe ser un documento de carácter no público con medidas de restricción para evitar su modificación.

El Responsable de Seguridad de la Información debería tener acceso para modificar el inventario, además de ser el responsable de resguardarlo.

7 . Evaluación del riesgo

La evaluación del riesgo permitirá identificar las debilidades en cuanto a controles de seguridad inexistentes o ineficaces. Se sugiere que la evaluación se realice por tipo de activo agrupado por similares características.

La evaluación de riesgos es el proceso que permite determinar y categorizar las amenazas potenciales y vulnerabilidades asociadas a activos de información. El resultado de este proceso permitirá determinar la identificación de controles que reducirán los riesgos.

7.1 . Identificación

La identificación de amenazas y vulnerabilidades sobre activos de información es importante para determinar cuáles tienden a degradar las propiedades de Disponibilidad, Integridad y Confidencialidad de la información.

Las amenazas pueden generarse de diferentes fuentes: amenazas externas e internas, usualmente las internas son de más alto riesgo, más aún cuando no se cuentan con medidas ni controles apropiados para mitigar el riesgo.

Tabla 3. Catálogo de Amenazas (MARGERIT) (1)

Amenaza	Degradación del activo		
	Disponibilidad	Integridad	Confidencialidad
Desastres Naturales			
Fuego (Incendios)	x		
Daños por agua (Inundaciones)	x		
Desastres Naturales	x		
De origen industrial			
Fuego (Incendios)	x		
Daños por agua (Inundaciones)	x		
Desastres industriales	x		
Contaminación mecánica	x		
Contaminación electromagnética	x		
Avería de origen físico o lógico	x		
Corte del suministro eléctrico	x		
Condiciones inadecuadas de temperatura o humedad	x		
Fallo de servicios de comunicaciones	x		
Interrupción de otros servicios y suministros esenciales	x		
Degradación de los soportes de almacenamiento de la información	x		
Emanaciones electromagnéticas			x
Errores y fallos no intencionados			
Errores de los usuarios	x	x	x
Errores del administrador	x	x	x
Errores de monitorización (log)		x	
Errores de configuración		x	
Deficiencias en la organización	x		
Difusión de software dañino	x	x	x
Errores de [re-]encaminamiento			x
Errores de secuencia		x	
Escapes de información		x	x
Alteración accidental de la información		x	
Destrucción de información	x		
Fugas de información			x
Vulnerabilidades de los programas (software)	x	x	x
Errores de mantenimiento / actualización de programas (software)		x	x
Errores de mantenimiento / actualización de equipos (hardware)	x		
Caída del sistema por agotamiento de recursos	x		
Pérdida de equipos	x		x
Indisponibilidad del personal	x		
Ataques intencionados			
Manipulación de los registros de actividad (log)		x	
Manipulación de la configuración	x	x	x
Suplantación de la identidad del usuario	x	x	x
Abuso de privilegios de acceso	x	x	x
Uso no previsto	x	x	x
Difusión de software dañino	x	x	x
[Re-]encaminamiento de mensajes			x
Alteración de secuencia		x	
Acceso no autorizado		x	x
Análisis de tráfico			x

Tabla 4. Catálogo de Amenazas (MARGERIT) (2)

Amenaza	Degradación del activo		
	Disponibilidad	Integridad	Confidencialidad
Interceptación de información (escucha)			X
Modificación deliberada de la información		X	
Destrucción de información	X		
Divulgación de información			X
Manipulación de programas	X	X	X
Manipulación de los equipos	X		X
Denegación de servicio	X		
Robo	X		X
Ataque destructivo	X		
Ocupación enemiga	X		X
Indisponibilidad del personal	X		
Extorsión	X	X	X
Ingeniería social (picaresca)	X	X	X

El responsable del activo de información debe determinar; en base a sucesos, y la importancia que tiene el activo sobre las posibles amenazas y vulnerabilidades a las que está expuesto y realizar una descripción del escenario en el cual se puede dar la materialización de la amenaza, asumiendo que el responsable conoce y entiende los riesgos sobre el activo.

Una vulnerabilidad es toda aquella debilidad que presenta el activo de información, dada comúnmente por la inexistencia o ineficacia de un control.

Una amenaza es todo elemento que haciendo uso o aprovechando una vulnerabilidad, atenta o puede atentar contra la seguridad de un activo de información. Las amenazas surgen a partir de la existencia de vulnerabilidades, independientemente de que se comprometa o no la seguridad de un sistema.

Tabla 5. Ejemplo de Vulnerabilidades (NB7ISO/IEC 27005: 2010)

Tipo Activo	Vulnerabilidad
Equipamiento informático	Susceptibilidad a la humedad, el polvo y la suciedad
	Sensibilidad a la radiación electromagnética
	Ausencia de un eficiente control de cambios en la configuración
	Susceptibilidad a las variaciones de temperatura
	Almacenamiento sin protección
	Copia no controlada
	Otras ...
Software - Aplicaciones informáticas	Defectos bien conocidos de software

	Ausencia de terminación de la sesión cuando se abandona la estación de trabajo
	Ausencia de pistas de auditoría
	Asignación errada de los derechos de acceso
	Software ampliamente distribuido
	Interfaz de usuario compleja
	Ausencia de documentación
	Configuración incorrecta de parámetros
	Tablas de contraseñas sin protección
	Habilitación de servicios innecesarios
	Software nuevo o inmaduro
	Especificaciones incompletas o no claras para los desarrolladores
	Ausencia de control de cambios eficaz
	Ausencia de copias de respaldo
	Otros...
Redes de comunicaciones	Ausencia de pruebas de envío o recepción de mensajes
	Líneas de comunicación sin protección
	Tráfico sensible sin protección
	Conexión deficiente de los cables
	Punto único de falla
	Ausencia de identificación y autenticación de emisor y receptor
	Arquitectura insegura de la red
	Transferencia de contraseñas en claro
	Gestión inadecuada de la red (Tolerancia a fallos en el enrutamiento)
	Otros...
Personal	Ausencia del personal
	Procedimientos inadecuados de contratación
	Entrenamiento insuficiente en seguridad
	Uso incorrecto de software y hardware
	Falta de conciencia acerca de la seguridad
	Ausencia de mecanismos de monitoreo
	Trabajo no supervisado de personal externo o de

	limpieza
	Ausencia de políticas para el uso de los medios de telecomunicaciones y mensajería
	Otros...
Instalaciones	Uso inadecuado o descuidado del control de acceso físico a las edificaciones o recintos
	Ubicación en un área susceptible de inundación
	Red energética inestable
	Ausencia de protección física de la edificación, puertas y ventanas
	Otros...

Podrían existir más vulnerabilidades, pero eso dependerá de los análisis anteriores (que deberán ser documentados) que permitieron revelar falencias para evitar la materialización de amenazas. Es importante aclarar que una amenaza se aprovecha de una o más vulnerabilidades, de ahí la importancia de identificar las vulnerabilidades.

Para identificar las vulnerabilidades se pueden utilizar métodos proactivos, tales como evaluación de vulnerabilidades, pruebas de intrusión a sistemas de información, servicios como el protocolo de transferencia de archivos (FTP), correo electrónico y otros, en busca de vulnerabilidades potenciales que pueden ser explotadas. Entre los métodos para este fin están:

- Herramientas automáticas de explotación de vulnerabilidades.
- Prueba y evaluación de la seguridad.
- Pruebas de penetración.
- Revisión de código.
- Errores intencionados.

Una vez determinadas las amenazas, vulnerabilidades y el escenario posible, el siguiente paso es la medición del nivel de riesgo en términos de la probabilidad que suceda el incidente (materialización de la amenaza) y el impacto ocasionado sobre el activo de información en las propiedades de disponibilidad, integridad y confidencialidad.

7.2 . Análisis y valoración

El propósito de analizar y valorar el riesgo es establecer el nivel de riesgo que cada amenaza conlleva al activo de información. La determinación del riesgo para cada par activo/amenaza resulta de:

- La probabilidad de que ocurra el incidente, es decir, que la amenaza explote la vulnerabilidad.
- La magnitud del impacto que el evento produce sobre el activo.

El cómputo de la probabilidad de ocurrencia del evento adverso suele basarse en los valores históricos de frecuencia con la que ocurre (o podría ocurrir) un evento (en un periodo determinado de tiempo, por ejemplo: anual, semestral. En caso de no contar con referencias históricas, se debe tomar la percepción que da el responsable del activo.

La valoración del riesgo se da en función de la probabilidad y el impacto ocasionado sobre el activo en escalas cualitativas.

Tabla 6. Valoración Cualitativa

ESCALAS	
Probabilidad	Impacto
Cierta/Inminente	Crítico
Muy Probable	Severo
Probable	Moderado
Poco Probable	Menor
Improbable	Irrelevante

La probabilidad y el impacto se combinan en una tabla para calcular y valorar el riesgo en una matriz de probabilidad versus impacto.

Figura 3. Matriz Para Valorar el Riesgo

P R O B A B I L I D A D	Y	1	2	3	4	5
	Cierta/Inminente	Bajo	Medio	Alto	Crítico	Crítico
	Muy Probable	Bajo	Medio	Alto	Alto	Crítico
	Probable	Irrelevante	Bajo	Medio	Alto	Alto
	Poco Probable	Irrelevante	Bajo	Bajo	Medio	Medio
	Improbable	Irrelevante	Irrelevante	Irrelevante	Bajo	Bajo
IMPACTO		Irrelevante	Menor	Moderado	Severo	Crítico
		X				

La valoración cualitativa del riesgo no limita a la entidad o institución pública de utilizar valoraciones cuantitativas.

Los resultados de la valoración de riesgos con nivel “Crítico” deberían ser tratadas con prioridad, después los riesgos con nivel “Alto” y luego los riesgos con nivel “Medio”, de acuerdo al enfoque de gestión de riesgos que se haya definido con antelación.

7.3 . Ejemplo de evaluación del riesgo

Suponiendo que el activo de información está en la categoría: Redes de comunicaciones.

Una amenaza identificada tiene relación a fallas eléctricas al menos una vez al mes. La frecuencia de dicha amenaza será Muy Probable y el impacto por causa del evento sobre el activo podría ser Severo. Si ocurre una inundación cada cuatro años, la frecuencia de dicha amenaza será Poco Probable y el impacto ocasionado si ocurriese el evento podría ser Crítico.

7.3.1 . Matriz de valoración del riesgo

Se sugiere una matriz para la valoración del riesgo en función de las amenazas y vulnerabilidades y el impacto por tipo de activo, según las características similares.

Figura 4. Matriz de Valoración del Riesgo

	A	B	C	D	E	F	G	H	I	K	M
1		INSTITUCIÓN:									
2		FECHA ELABORACIÓN:									
3		FECHA APROBACIÓN:									
4											
5											
6		VALORACIÓN DE RIESGOS							DEGRADACIÓN		
7	#	Activo	Amenaza	Situación	Vulnerabilidad	Probabilidad	Impacto	Nivel de Riesgo	Disponibilidad	Integridad	Confidencialidad
8											
9											
10											
11											
12											
13											
14											
15											
16											
17											
18											
19											
20											
21											
22											
23											
24											
25											
26											
27		Elaborado por:					Aprobado por:				
28		Firma:					Firma:				
29		Cargo					Cargo:				
30											

Por tipo de activo de información se debe identificar la(s) amenaza(s), vulnerabilidad(es), la situación en la que se produce la materialización de la amenaza, determinar la probabilidad y el impacto para establecer el nivel de riesgo del activo.

Determinar la dimensión de afectación de las propiedades del activo (Disponibilidad, Integridad y Confidencialidad) marcando con una X.

El resultado de valorar el riesgo asociado a cada activo será la identificación de aquellos riesgos a ser tratados con prioridad mediante la aplicación de controles que mitiguen el riesgo. Esta determinación debe ir en el sentido de aplicabilidad y mitigación de los riesgos importantes, entendiendo de mayor importancia aquel riesgo “crítico” y menor el riesgo “irrelevante”.

8 . Tratamiento del riesgo

El tratamiento del riesgo implica tomar decisiones para aceptar, reducir, retener, evitar o transferir los riesgos.

Aceptar el riesgo significa estar conscientes de la afectación que se produzca en caso de materializarse la amenaza o vulnerabilidad; para esto se deberían disponer de recursos ante una eventualidad. En el marco de la aceptación del riesgo, los que no sean considerados relevantes podrán ser excluidos de la selección de controles, pero se deberá incluir una justificación para no tratarlos.

Reducir el riesgo implica realizar una selección de Controles de Seguridad de la Información (ver Anexo A). O bien se pueden diseñar nuevos controles para cumplir con necesidades específicas que coadyuven a la reducción del riesgo.

Retener el riesgo implica establecer criterios para su aceptación, no es necesario implementar o seleccionar controles adicionales si el riesgo puede ser retenido.

El riesgo puede evitarse cuando estos se consideran muy altos, o si los costos para implementar otras opciones de tratamiento del riesgo exceden los beneficios. Se puede tomar una decisión que logre evitar por completo el riesgo, mediante el retiro de una actividad, condiciones o conjunto de actividades ya sean planificadas o existentes. Esto deberá estar debidamente justificado y documentado.

Transferir el riesgo implica derivar de forma parcial o total a terceros que puedan gestionar de manera más eficaz el riesgo.

La decisión que se tome en cuanto al tratamiento de riesgos debe indicar la forma en que estos serán tratados; es decir, los controles que se aplicarán. Los lineamientos para la Elaboración del Plan Institucional de Seguridad de la Información indica ciertos controles mínimos que deben ser aplicados.

9 . Controles implementados y por implementar

Los listados de los controles implementados y por implementar vienen como consecuencia de la decisión de las opciones de tratamiento de riesgos y los controles de seguridad que se decidan implementar. Esta declaración no se limita a los controles mínimos requeridos, la cual puede incluir otros controles o medidas necesarias para el tratamiento del riesgo (Ver punto 8).

Los controles implementados y por implementar deben indicar si un determinado control ya se ha implementado o no, junto con el medio de verificación que puede ser una referencia a documentación existente.

El listado permite ver de forma resumida aquellos controles mínimos requeridos y otros que se consideren necesarios. A continuación se muestra un cuadro que refleja los controles implementados y por implementar.

Tabla 7. Matriz de Controles Implementados y por Implementar

Control de Seguridad de la Información	Inclusión del Control	Control Existente	Justificación Inclusión	Justificación Exclusión	Documentación
Acuerdo de confidencialidad	Sí	No	Control mínimo requerido. Resultados de la evaluación de riesgos.		
Control de accesos	Sí	Sí	Control mínimo requerido. Resultados de la evaluación de riesgos.		Política de control de accesos. Procedimientos de altas y bajas de usuarios.
Uso de medios extraíbles	No	No		Aceptación del riesgo.	