[redacted]

Versión 1.0

Metodología de análisis de riesgo según ISO 27005:2018 e ISO 31000:2018

Tabla de contenido

1 INTRODUCCION

Identificar y gestionar los riesgos a los cuales están expuestos los activos de información, para preservar su confidencialidad, integridad y disponibilidad, utilizando un proceso sistemático para lograr un adecuado tratamiento de los riesgos e implementación de controles efectivos. Para este propósito nos apoyaremos en la norma ISO 27005:2018 y la ISO 31000:2018:

Ilustración 1. Gestión de riesgos.

ISO 31000:2018 solo formula recomendaciones y eso significa que no permite la implementación de un sistema de gestión certificable. Sin embargo, los principales cambios en ISO 31000:2018 resultan importantes ya que se alinean con el enfoque basado en el riesgo, presente en normas como ISO 9001 e ISO 14001.

- Lenguaje novedoso y simplificado dentro de una estructura de referencias.
- Énfasis a lo largo de toda la norma sobre el papel de liderazgo de la Alta Dirección y la responsabilidad que debe asumir para garantizar que la gestión de riesgos se integre transversalmente en la organización.
- Énfasis a la naturaleza dinámica y cambiante de la gestión de riesgos, que exige la necesidad de que las organizaciones evalúen sus riesgos y sus impactos, a la luz de nuevas circunstancias o factores en el contexto externo o interno.
- Un enfoque genérico que permite que la norma se utilizada en varios campos de la industria.

2 METODOLOGÍA PARA LA GESTIÓN DE RIESGOS SEGÚN ISO 31000:2018

2.1 DESCRIPCIÓN

Ejecutar acciones que protejan adecuadamente los sistemas de información y activos de la organización, al igual que implementar controles de seguridad, requiere desarrollar un proceso de Gestión de riesgos (*Ver ilustración 1*), basado en los activos y los factores tanto internos como externos.

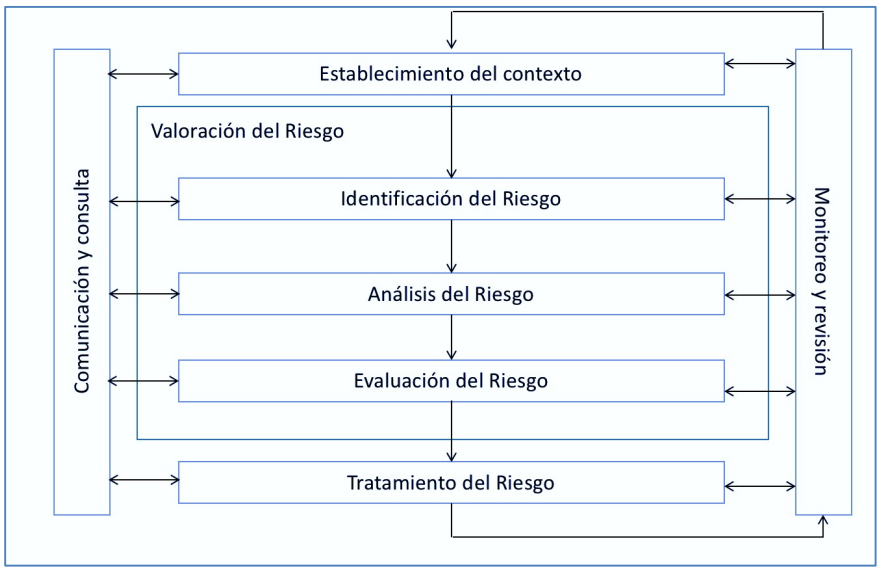
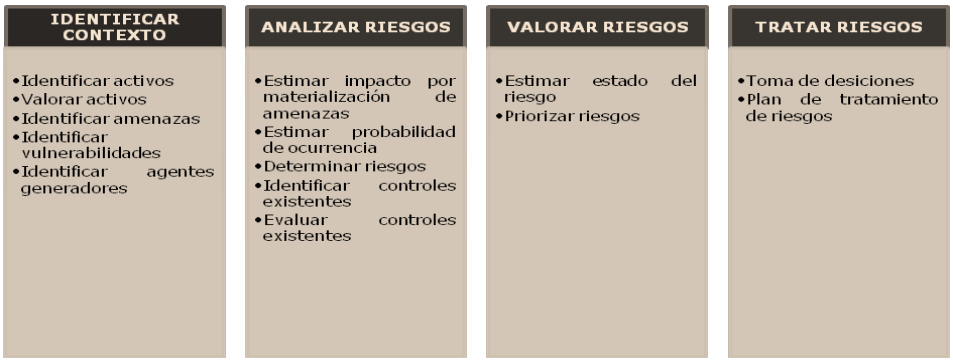


Ilustración 2. Proceso de gestión de Riesgos

A continuación se exponen las actividades de cada una de las etapas del proceso de Gestión de Riegos, con el fin de identificar con claridad la situación de cada uno de sus activos: su valor, vulnerabilidades, y cómo están protegidos frente a amenazas.

Ilustración 3. Actividades de la gestión de riesgo.

1. Identificar contexto
2. Analizar riesgos
3. Valores del riesgo
4. Tratamiento de los riesgos



2.2 IDENTIFICAR EL CONTEXTO DE LA ORGANIZACION

2.2.1 Propósito

Conocer los eventos potenciales, estén o no bajo el control de la organización y que ponen en riesgos sus activos de información.

2.2.2 Actividades a realizar

2.2.3 Identificación de activos de información

Un activo es: "cualquier elemento al cual se le asigna un valor y por tanto debe protegerse", lo cual puede entenderse igualmente como aquello que requiere la organización para el cumplimiento de sus objetivos.

1. Tipos de activos

2. Clases de activos:

Activos de información y físicos		
Activos físicos	Infraestructura física	Oficinas
	Hardware	Servidores, dispositivos de comunicaciones, computadoras de escritorio.
	Tecnología Software	Aplicaciones
Activos de información	Electrónica	Información importante para el negocio.
	Documentos	Información importante para el negocio
personal	Dueños de información	Nivel directivo dueño de la información que asigna permisos para leer utilizar y modificar la información.
		Personal que utiliza la información para su trabajo.
Servicios		Correo electrónico

Tabla 1. Tipos de activos

2.2.4 Valoración de los activos de información

Una vez identificados los activos se realizará la valoración de cada uno de ellos en términos de valor para el negocio según:

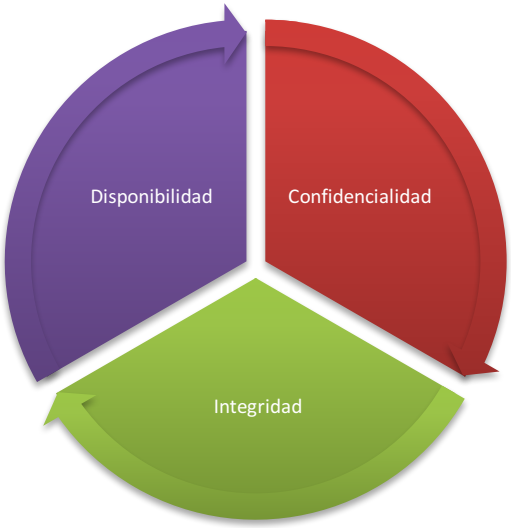


Ilustración 4. Pilares de la seguridad de la información ISO 27001:2013

Disponibilidad:

Los activos de una determinada organización tendrán mayor valor en la medida que si no están disponibles se impactará gravemente el negocio. Igualmente, un activo que al no estar disponible no afecte de ningún modo el negocio, tendrá un menor valor.

Para determinar el impacto que sobre el negocio genera la indisponibilidad del activo se utilizarán los criterios relacionados en la siguiente tabla:

	Valoración de los activos			
	MINIMO (1)	MEDIO (3)	GRAVE (5)	CATASTRÓFICO (7)
Las pérdidas **económicas** por indisponibilidad del activo son:				
Los **servicios** prestados se ven afectados por la indisponibilidad del activo de la siguiente forma:	Interrupción leve o nula en suministro de servicios.	Obliga al cliente a cambiar de proveedor de forma transitoria.	Pérdida de algunos clientes de forma definitiva.	Pérdida de clientes clave.
La inidisponibilidad del activo afecta la **operación** asi:	Retrasos en funciones no vitales	Retrasos leves en funciones vitales.	Retrasos graves en funciones vitales	Interrupción inmediata de funciones vitales
La indisponibilidad del activo afecta la **imagen** en el sentido que:	No afectar la confianza en los productos o servicios.	Pérdida de confianza en un servicio específico o en una parte de la organización.	Pérdida de confianza de parte de los clientes.	Pérdida de confianza del mercado y daños a la imagen de marca.
La indisponibiliad del activo afecta el **cumplimiento** de oblicaciones en el sentido que:	Produce una falta leve en el cumplimiento de algún contrato.	Produce una falta en el cumplimiento de algún contrato que obliga a renegociar.	Produce una falta grave en el cumplimiento de algún contrato.	Deja a la organización al margen de la ley

Tabla 2. Criterios para valoración de disponibilidad

Se asigna un valor utilizando la siguiente escala:

VALORACIÓN	VALOR
Mínimo	1
Medio	3
Grave	5
Catastrófico	7

Tabla 3. Valoración de la disponibilidad

Confidencialidad:

Los activos de información reciben una valoración alta cuando su nivel de confidencialidad es mayor, teniendo en cuenta que la divulgación no autorizada de la misma puede afectar en alguna medida los intereses, imagen y operación de la compañía.

Para realizar la valoración de los activos en la dimensión de confidencialidad tendremos en cuenta los resultados obtenidos en la Herramienta para Clasificación de Información (y con base en la clasificación obtenida para cada activo asignaremos un valor.

CLASIFICACIÓN	VALOR
Publica	5
Uso Interno	10
Confidencial	15
Reservada	20

Tabla 4. Valoración de la confidencialidad

Integridad:

Los activos son valorados con mayor valor cuando su alteración puede generar daños graves a la organización.

La valoración en la dimensión integridad se realizará utilizando los siguientes criterios:

CRITERIO	VALOR
Información que afecta mucho la operación	20
Información que afecta moderadamente el negocio	15
Información que puede tener algunos errores o cambios sin afectar su sentido principal	10
Información o activos que pueden tener errores sin tener impactos al negocio.	5

Tabla 5. Criterios para la valoración de la integridad

Para calcular el valor del activo se realiza la sumatoria de todos los factores evaluados y se establecerá el valor de activo teniendo en cuenta lo siguiente:

VALORACIÓN DE ACTIVO	SUMATORIA DE LOS FACTORES CONSIDERADOS
MB: muy bajo	De 14 a 24
B: bajo	De 25 a 35
M: medio	De 36 a 46
A: alto	De 47 a 57
MA: muy alto	De 58 a 68

Tabla 6. Valoración de la confidencialidad del activo.

2.2.5 Identificación de amenazas posibles

Las amenazas son resultados de actos deliberados que pueden afectar nuestros activos o los activos de información, sin embargo, existen eventos naturales o accidentales que deben ser considerados por su capacidad de generar incidentes de seguridad.

CAUSA	EVENTO O AMENAZA
Eventos naturales	Terremotos o huracanes.
Eventos externos	Pérdida de proveedores, problemas de transporte, sobrecargas.
Condiciones internas	Problemas de transporte.
Actos deliberados	Fallas de hardware, fallas de software, fallas en la red,
Actos accidentales	Destrucción de información, Incendios.
Humano	Epidemias, indisponibilidad de personal.

Tabla 7. Listado de amenazas

2.2.6 Identificación de vulnerabilidades de los activos

Debe identificarse la forma como cada una de las amenazas podría materializarse, es decir, que vulnerabilidades permiten que las amenazas se conviertan en situaciones de riesgo reales.

Algunos tipos de vulnerabilidades*:*

- Ausencia de políticas
- Configuraciones no seguras
- Empleado descontento
- Empleado deshonesto (sobornado o víctima de chantaje)
- Errores de configuración.
- Falta de actualizaciones
- Uso de servicios inseguros
- Uso de protocolos inseguros

2.3 ANALIZAR RIESGOS SOBRE LOS ACTIVOS

2.3.1 Propósito

Establecer la probabilidad de ocurrencia de los riesgos y el impacto de sus consecuencias, calificándolos y evaluándolos, a fin de determinar la capacidad de la organización para su aceptación o manejo.

2.3.2 Desarrollo de actividades

2.3.3 Estimar el impacto sobre los activos

El impacto es la medida de daño causado por un incidente en el supuesto de que ocurra, afectando así, el valor de los activos, está perdida de valor la denominamos degradación del activo.

La medición del impacto la realizaremos utilizando la siguiente matriz:

VALORACION DEL ACTIVO	AFECTACION DEL ACTIVO				
	5%	25%	50%	75%	100%
MA: muy alto	A	A	A	A	MA
A: alto	M	M	A	A	A
M: medio	B	M	M	A	A
B: bajo	MB	MB	M	M	M
MB: muy bajo	MB	MB	MB	B	M

Tabla 8. Matriz de estimación del impacto sobre activos.

La estimación del impacto puede ser entonces**:**

1. **MA:** Muy alto
2. **A:** Alto
3. **M:** Medio
4. **B:** Bajo
5. **MB:** Muy bajo

2.3.4 Estimar probabilidad de ocurrencia

La probabilidad de ocurrencia se calcula con base en la siguiente tabla:

1) Cualitativa: La probabilidad de ocurrencia se establece acorde a la siguiente tabla:

VALOR	OCURRENCIA	FRECUENCIA
Es probable que se materialice la amenaza a diario	100	Muy frecuente
Es probable que se materialice la amenaza semanalmente	10	Frecuente
Es probable que se materialice la amenaza anualmente	1	Normal
Es probable que se materialice la amenaza cada varios años	1/10	Poco frecuente

Tabla 9. Valoración cualitativa de la frecuencia.

2) Cuantitativo: a partir de los datos históricos que la organización haya acumulado en el tiempo. La frecuencia se considera como numero de ocurrencias de la amenaza en un año.

FRECUENCIA	PROBABILIDAD
Más de 100 al año	Muy frecuente
Entre 10 y 20 al año	Frecuente
Entre 1 y 5 al año	Normal
Menos de 1/10 al año	Poco frecuente

Tabla 10. Valoración de la frecuencia

2.3.5 Estimar riesgos

Conociendo el impacto de las amenazas sobre los activos es posible determinar el nivel de riesgo, teniendo en cuenta la frecuencia de ocurrencia de los incidentes.

IMPACTO				
MA: muy alto	Zona de riesgo importante	Zona de riesgo importante	Zona de riesgo importante	Zona de riesgo inaceptable
A: alto	Zona de riesgo moderado	Zona de riesgo moderado	Zona de riesgo importante	Zona de riesgo importante
M: medio	Zona tolerable del riesgo	Zona de riesgo moderado	Zona de riesgo importante	Zona de riesgo importante
B: bajo	Zona aceptable de riesgo	Zona tolerable del riesgo	Zona de riesgo moderado	Zona de riesgo moderado
MB: muy bajo	Zona aceptable de riesgo	Zona aceptable de riesgo	Zona tolerable del riesgo	Zona tolerable del riesgo
	Poco frecuente	Normal	Frecuente	Muy frecuente

FRECUENCIA

Tabla 11. Matriz para determinación de riesgos.

2.3.6 Identificar controles existentes

Los controles existentes son las medidas con que se cuentan para reducir la exposición a los riesgos: procedimientos, mecanismos, controles tecnológicos, etc. Para identificar los controles existente puede utilizarse como referencia el anexo A del estándar ISO/IEC 27001/2013.

2.3.7 Evaluar controles existentes

Una vez identificados los controles existentes es necesario evaluar su efectividad frente a los riesgos que se pretenden mitigar.Para medir la efectividad de los controles utilizaremos los siguientes criterios:

EVALUACION DEL CONTROL	VALORES				
	NULO	DEFICIENTE	REGULAR	BUENO	EXCELENTE
El control está formalmente establecido.	0%	25%	50%	75%	100%
El control está perfectamente desplegado, configurado y mantenido.	0%	25%	50%	75%	100%
Existen procedimientos claros de uso del control y en caso de incidencias.	0%	25%	50%	75%	100%
Los usuarios están formados y concienciados sobre la aplicación del control.	0%	25%	50%	75%	100%
El control es funcional desde el punto de vista teórico y operacional.	0%	25%	50%	75%	100%

Tabla 12. Criterios para valoración de controles existentes

La eficiencia del control se estima con base en la siguiente tabla:

Efectividad = Promedio de las valoraciones realizadas

SUMA	EFECTIVIDAD DEL CONTROL
Mayor de 89%	EXCELENTE
De 65% y 89%	BUENA
De 40% y 64%	REGULAR
De 15% y 39%	DEFICIENTE
Menor de 15%	NULA

Tabla 13. Valoración de controles

2.4 VALORACIÓN DE RIESGOS

2.4.1 Objetivo

Determinar el nivel o grado de exposición de la organización a los impactos del riesgo, estimando las prioridades para su tratamiento.

2.4.2 Desarrollo de actividades

2.4.3 Estimar riesgo

El riesgo se establece considerando los controles existentes, orientados a prevenir que el incidente se presente.

Controles orientados a prevenir el incidente:

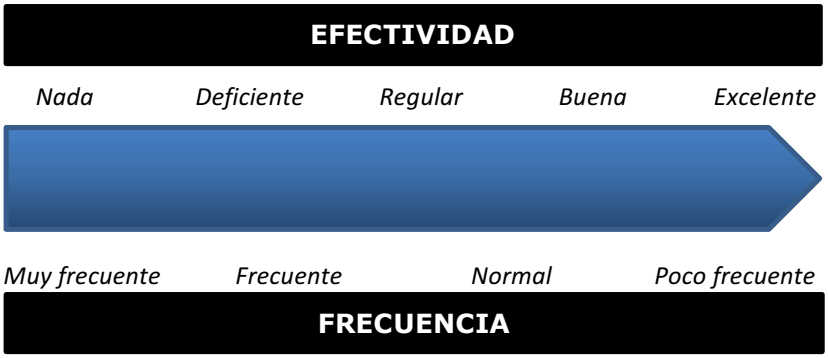


Ilustración 5. Efectividad de control y frecuencia.

En la ilustración No.5 se aprecia como a medida que la efectividad del control aumenta, la frecuencia de ocurrencia de incidentes disminuye. Controles que limitan la degradación de activos:

Ilustración 6. Efectividad de control y degradación.

En la ilustración No 6, se aprecia que la efectividad del control aumenta, la degradación del activo es menor.

Si los controles tienen niveles adecuados de efectividad la degradación de los activos ó la frecuencia de los incidentes debe ser menor a los valores hallados inicialmente.

2.4.4 Priorizar los riesgos sobre los activos

El riesgo nos muestra el grado de exposición frente a las amenazas evaluadas, es posible distinguir entre los riesgos aceptables, tolerables, moderados, importantes o inaceptables, y establecer la prioridad de las acciones requeridas para su tratamiento. Las acciones que se deben ejecutar se harán con base en la siguiente tabla:

Riesgo	Prioridad	Tiempo de ejecución de acciones
Inaceptable	Muy Alta	Inmediata
Importante	Alta	De 0 a 4 meses
Moderado	Media	De 4 a 7 meses
Tolerable	Baja	De 7 a 12 meses
Aceptable	Muy baja	De 12 a 16 meses

Tabla 14. Priorización de riesgos.

2.5 LA GESTIÓN DE RIESGOS EN LOS ACTIVOS

2.5.1 Objetivo

Estructurar los criterios para la toma de decisiones respecto al tratamiento de los riesgos, en esta etapa se establece las guías de acción necesarias para coordinar y administrar los eventos que pueden comprometer la confidencialidad, integridad y disponibilidad de los activos.

2.5.2 Desarrollo de actividades

2.5.3 Toma de decisiones

Si el riesgo se ubica en la Zona de Riesgo Aceptable, permite a la Organización aceptarlo, es decir, el riesgo se encuentra en un nivel que puede asumirse sin necesidad de tomar otras medidas de control.

Si el riesgo se ubica en la Zona de Riesgo Inaceptable, es aconsejable eliminar la actividad que genera el riesgo en la medida que sea posible.

Si el riesgo se sitúa en cualquiera de las otras zonas (riesgo tolerable, moderado o importante) se deben tomar medidas para llevar los Riesgos a la Zona Aceptable, con la implementación de los respectivos controles.

Las medidas dependen del punto en la cual se ubica el riesgo:

ZONA	IMPACTO	FRECUENCIA	MEDIDA
Zona de riesgo importante	**MA:** muy alto	Poco frecuente	Prevenir riesgo: Implementar controles frente a impacto.
	MA: muy alto	Normal	Prevenir riesgo: Implementar controles frente a impacto.
	A: alto	Frecuente	Prevenir riesgo: Implementar ó mejorar controles frente a impacto y frecuencia.
	M: medio	Frecuente	Prevenir riesgo: Implementar ó mejorar controles frente a impacto y frecuencia.
	M: medio	Muy frecuente	Prevenir riesgo: Implementar ó mejorar controles frente a impacto y frecuencia.
Zona de riesgo moderado	**A:** alto	Poco frecuente	Compartir riesgos. Prevenir riesgo: Implementar ó mejorar controles frente a impacto.
	A: alto	Normal	Compartir riesgos. Prevenir riesgo: Implementar ó mejorar controles frente a impacto y frecuencia.
	M: medio	Normal	Compartir riesgos. Prevenir riesgo: Implementar ó mejorar controles frente a impacto y frecuencia.
	B: bajo	Frecuente	Realizar análisis costo beneficio para decidir si el riesgo se asume, se previene o se comparte.
	B: bajo	Muy frecuente	Realizar análisis costo beneficio para decidir si el riesgo se asume, se previene o se comparte.
Zona tolerable del riesgo	**M:** medio	Poco frecuente	Prevenir riesgo: Implementar ó mejorar controles frente a impacto.
	B: bajo	Normal	Realizar análisis costo beneficio parta decidir si el riesgo se asume, se previene o se comparte.
	MB: muy bajo	Frecuente	Realizar análisis costo beneficio parta decidir si el riesgo se asume, se previene o se comparte.
	MB: muy bajo	Muy frecuente	Realizar análisis costo beneficio parta decidir si el riesgo se asume, se previene o se comparte.

Tabla 15. Estimación de los riesgos sobre los activos.

La selección de controles se realizará tomando como referencia el Anexo A del estándar ISO/IEC 27001:2013.

Para seleccionar los controles frente a los riesgos establecidos, deberá realizarse un análisis costo-beneficio para evitar implementación de controles con costos superiores al costo de los riesgos reales.

2.5.4 Plan de tratamiento de riesgos

Una vez seleccionado los controles que serán implementados para mitigación de riesgos es necesario elaborar un plan de acción que garantice un efectivo despliegue de los mismos.

La elaboración del plan de tratamiento de riesgos será responsabilidad del Oficial de Seguridad y la respectiva aprobación de los mismos del Comité de Seguridad.

3 REFERENCIAS

- ISO 27005:2018
- ISO/IEC 31000:2018
- ISO/27001:2013
- ISO 22301:2012
- ISO 27005:2005
- ISO 31000:2009