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

GRUPO DE TECNOLOGÍAS DE LA INFORMACIÓN

UNIDAD ADMINISTRATIVA ESPECIAL DE ORGANIZACIONES SOLIDARIAS

POLITICA DE ADMINISTRACION DEL RIESGO

GLOSARIO

ETAPAS DE EADMINISTRACIÓN DEL RIESGO

CONTEXTO ESTRATÉGICO

IDENTIFICACIÓN DEL RIESGO

VALORACIÓN DEL RIESGO

SEGUIMIENTO DE LOS RIESGOS

MAPA DE RIESGOS

INTRODUCCIÓN

Durante los últimos años el Gobierno Nacional ha desarrollado estrategias para establecer en las entidades públicas una cultura de seguridad y prevención ante las amenazas que constantemente atentan a las instituciones del estado.

La información que manejan las entidades públicas es crucial para el funcionamiento y correcto desempeño sin importar el tipo de información que se maneje, esta es vital para el cumplimiento de la misión y los objetivos estratégicos de la entidad, por esta razón se debe resguardar y proteger todo tipo de información de cualquier posibilidad de alteración, mal uso, pérdida u otro evento.

Es así como en el modelo de Seguridad y Privacidad de la Información desarrollado por MinTIC la gestión de riesgos es parte primordial para el progreso, permanencia y mejora continua del Sistema de Gestión de Seguridad de la Información (SGSI) en la entidad. Con la formulación de este plan se busca identificar los posibles riesgos que puedan atentar contra el cumplimiento de la misión institucional, logrando de esta manera prevenir y resguardar la información crucial para la institución.

OBJETIVO GENERAL

Establecer la metodología para una adecuada gestión del riesgo a partir de su identificación, manejo y seguimiento.

OBJETIVOS ESPECIFICOS

- Identificar los riesgos de seguridad y privacidad de la información que atenten contra los procesos de gestión de la entidad.

- Concientizar a los funcionarios, procesos, colaboradores de la entidad sobre la importancia de la identificación y tratamiento de los riesgos de seguridad de la información.

- Establecer mediante la adecuada gestión del riesgo una base sólida para la adecuada toma de decisiones y planificación institucional.

ALCANCE

Este plan proporciona la metodología establecida por el Grupo de Tecnologías de la Información para realizar una adecuada gestión del riesgo a nivel de procesos; orienta en el establecimiento del contexto estratégico, la identificación de los riesgos, su análisis, valoración, seguimiento y la definición de las opciones de manejo que pueden requerir la formulación de acciones adicionales para garantizar una adecuada gestión del riesgo.

DEFINICIONES

- **Administración de Riesgos:** Conjunto de elementos de control que al interrelacionarse permiten a la entidad pública evaluar aquellos eventos negativos tanto internos como externos, que puedan afectar o impedir el logro de sus objetivos institucionales o los eventos positivos que permitan identificar oportunidades para un mejor cumplimiento de su función. Se constituye en el componente de control que al interactuar sus diferentes elementos le permite a la entidad pública autocontrolar aquellos eventos que pueden afectar el cumplimiento de sus objetivos.

- **Aceptar el riesgo:** No se adopta ninguna medida que afecte la probabilidad o el impacto del riesgo.

- **Análisis de Riesgos:** Elemento de control que permite establecer la probabilidad de ocurrencia de los eventos positivos y/o negativos y el impacto de sus consecuencias, calificándolos y evaluándolos a fin de determinar la capacidad de la entidad pública para su aceptación y manejo. Se debe llevar a cabo un uso sistemático de la información disponible para determinar qué tan frecuentemente pueden ocurrir eventos especificados y la magnitud de sus consecuencias.

- **Amenaza:** Eventos que pueden desencadenar un incidente en la organización, produciendo daños materiales o pérdidas inmateriales en sus activos.

- **Ataque:** Cualquier acción deliberada encaminada a violar los mecanismos de seguridad de un sistema de información.

- **Causa:** Todos aquellos factores internos o externos que solos o en combinación con otros pueden producir la materialización del riesgo.

- **Calificación del Riesgo:** Estimación de la probabilidad de ocurrencia del riesgo y el impacto que puede causar su materialización.

- **Compartir el Riesgo:** Se reduce la probabilidad o el impacto del riesgo, transfiriendo o compartiendo una parte del riesgo con una parte interesada que pueda gestionarlo con más eficacia.

- **Contexto Estratégico:** son las condiciones internas y del entorno, que pueden generar eventos que originan oportunidades o afectan negativamente el cumplimiento de la misión y objetivos de una institución.

- **Control:** Acción o conjunto de acciones que minimiza la probabilidad de ocurrencia de un riesgo o el impacto producido ante su materialización.

- **Control preventivo:** Conjunto de acciones que eliminan o mitigan las causas del riesgo; está orientado a disminuir la probabilidad de ocurrencia del riesgo.
- **Control correctivo:** Conjunto de acciones que eliminan o mitigan las consecuencias del riesgo; está orientado a disminuir el nivel de impacto del riesgo.

- **Debilidad:** Situación interna que la entidad puede controlar y que puede afectar su operación.

- **Declaración de Aplicabilidad (SOA):** Documento que enlista los controles de seguridad de la información establecidos en la norma ISO/IEC 27001 (114 controles agrupados en 35 objetivos de control). Es utilizado como una referencia para la implementación de medidas de protección de la información.

- **Degradación:** Pérdida de valor de un activo como consecuencia de la materialización de una amenaza.

- **Evaluación del Riesgo:** Resultado del cruce cuantitativo de las calificaciones de probabilidad e impacto, para establecer la zona donde se ubicará el riesgo.

- **Evitar el riesgo:** Opción de manejo que determina la formulación de acciones donde se prevenga la materialización del riesgo mediante el fortalecimiento de controles identificado.

- **Frecuencia:** Tasa de ocurrencia de una amenaza.

- **Gestión de Riesgos:** Es la selección e implantación de las medidas de seguridad adecuadas para conocer, prevenir, impedir, reducir o controlar los riesgos identificados y así reducir al mínimo su potencialidad o sus posibles perjuicios. La gestión de riesgos se basa en los resultados obtenidos en el análisis de los riesgos.

- **Identificación del riesgo:** Etapa en la que se deben establecer las fuentes o factores de riesgo, los eventos o riesgos, sus causas (factores internos y externos) y sus consecuencias.

- **Impacto:** Medida para estimar cuantitativa y cualitativamente el efecto producido por la materialización del riesgo.

- **Impacto residual:** Impacto remanente en el sistema tras la implantación de los controles determinados en el plan de seguridad de la información.

- **Incidente:** Evento con consecuencias

- **MSPI:** Es un instrumento de evaluación creado por el Ministerio de las Tecnologías de la Información, con el fin de identificar el nivel de madurez en la implementación del modelo de seguridad y privacidad de la información, permitiendo establecer el estado de la gestión y adopción de controles técnicos y administrativos al interior de las entidades públicas.

- **Mapa de Riesgos:** Documento que de manera sistemática muestra el desarrollo de las etapas de la administración del riesgo.

- **Materialización del Riesgo:** Ocurrencia del riesgo identificado.

- **Opciones de manejo:** posibilidades disponibles para administrar el riesgo posterior a la valoración de los controles definidos (asumir, reducir, evitar compartir o transferir el riesgo residual).

- **Probabilidad:** Se entiende como la posibilidad de ocurrencia del riesgo, esta puede ser medida con criterios de frecuencia o factibilidad.

- **Reducir el Riesgo:** Se adoptan las medidas para reducir la probabilidad o impacto del riesgo, o ambos; por lo general conlleva a la implementación de controles.

- **Riesgo:** Eventualidad que tendrá un impacto negativo sobre los eventos institucionales o de los procesos realizados por la entidad, los riesgos pueden clasificarse de acuerdo al tipo de eventualidad que se pueda presentar.

- **Riesgo Estratégico:** Se asocia con la forma en que se administra la Entidad. El manejo del riesgo estratégico se enfoca en asuntos globales relacionados con la misión y el cumplimiento de los objetivos estratégicos, la clara definición de las políticas, diseño y conceptualización de la entidad por parte de la Dirección.

- **Riesgos de Imagen:** Están relacionados con la percepción y la confianza por parte de la ciudadanía hacia la entidad.

- **Riesgos Operativos:** Riesgos provenientes del funcionamiento y operatividad de los sistemas de información institucionales, de la definición de los procesos, de la estructura de la entidad, de la articulación de las dependencias.

- **Riesgos Financieros:** Se relacionan con el manejo de los recursos de la entidad que incluyen: la ejecución presupuestal, la elaboración de los estados financieros, los pagos, manejos de excedentes de tesorería y el manejo sobre los bienes.

- **Riesgos de Cumplimiento:** Se asocian con la capacidad de la entidad para cumplir con los requisitos legales, contractuales, de ética pública y en general con su compromiso ante la comunidad.

- **Riesgos de Tecnología:** Están relacionados con la capacidad tecnológica de la entidad para satisfacer sus necesidades actuales y futuras y el cumplimiento de la misión.

- **Riesgos de Corrupción:** Posibilidad de que por acción u omisión se use el poder para desviar la gestión de lo público hacia un beneficio privado.

- **Riesgo Residual:** riesgo que permanece después de aplicar los controles definidos en el sistema de administración del riesgo.

- **Sistema de gestión de seguridad de la información (SGSI):** Sistema de gestión de la entidad basado en el enfoque de riesgos del negocio para establecer, implementar, operar, monitorear, mantener y mejorar la seguridad de la información.

- **Tratamiento de Riesgos:** Es la respuesta establecida ante el análisis del riesgo para la mitigación de los diferentes riesgos. Los líderes de proceso pueden tomar varias acciones ante el tratamiento del riesgo ya sea: aceptar el riesgo, reducir el riesgo, evitar el riesgo o compartir el riesgo. Cabe resaltar que los riesgos de corrupción no pueden ser aceptados.

- **Valoración del riesgo:** Establece la identificación y evaluación de los controles para prevenir la ocurrencia del riesgo o reducir los efectos de su materialización. En la etapa de valoración del riesgo se determina el riesgo residual, la opción de manejo a seguir y si se necesita.

POLÍTICA DE ADMINISTRACIÓN DEL RIESGO

La Unidad Administrativa Especial de Organizaciones Solidarias, implementa el sistema de administración de riesgos de gestión y corrupción, para ejercer control sobre aquellos riesgos que puedan impedir el logro de sus objetivos institucionales, el logro de los objetivos por procesos, o impacten económicamente la Unidad, por ello establece elementos de control a los riesgos de corrupción con el objeto de identificar, valorar, y definir acciones de control mediante estrategias para evitar, reducir, compartir o transferir y asumir los riesgos de acuerdo con su nivel de riesgo residual.

Para ello la Unidad cuenta con personas comprometidas en el mejoramiento continuo de sus procesos, quienes evaluarán la efectividad de las acciones y de los controles establecidos a través de un monitoreo permanente que asegure un efectivo manejo del riesgo. Adicionalmente la Alta Dirección de la Unidad proporciona los recursos requeridos para la implementación del sistema.

Respecto a los riesgos de gestión, aquellos identificados en las zonas de riesgo altas y/o extremas, el líder del proceso debe establecer e implementar acciones inmediatas para su respectivo tratamiento. Los únicos riesgos que la Unidad permite asumir son los riesgos que se encuentran en zona de riesgo baja para riesgos de gestión. Por su parte todo riesgo de corrupción identificado debe contar con controles y no se asumirá ningún riesgo de corrupción.

En la Unidad los mapas de riesgos tienen dos evaluaciones, la primera denominada monitoreo, la cual es realizada por parte de los líderes de proceso, la segunda denominada seguimiento la cual será realizada por parte de la oficina de control interno, estas evaluaciones se realizarán de acuerdo con las fechas establecidas en las directrices emitidas por los entes rectores, determinando su implementación y efectividad.

ETAPAS DE ADMINISTRACIÓN DEL RIESGO

En la siguiente imagen se presenta el proceso para la administración del riesgo en la seguridad y privacidad de la información desde un contexto estratégico considerando cada una de las etapas que se deben tener en cuenta para la valoración de los riesgos y su tratamiento.

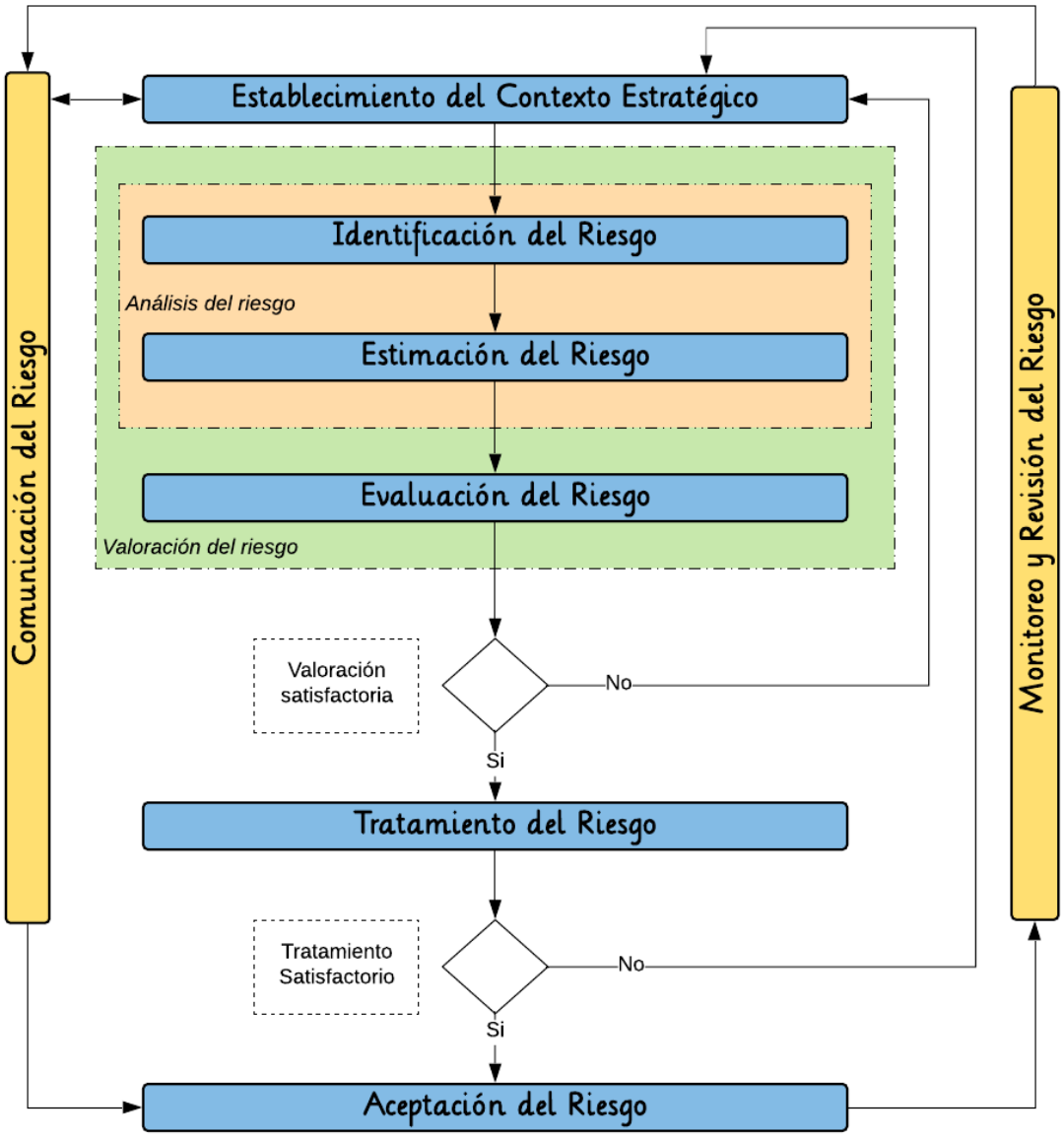


Imagen 1. Tomado de la NTC- ISO/IEC 27005.

De acuerdo a la imagen anterior se observa que la primera actividad a realizar es el análisis del contexto estratégico, seguido de la valoración del riesgo, una vez identificados los riesgos debe definirse el tratamiento que se les dará a los riesgos, entre las categorías de tratamiento se encuentran (Aceptar el riesgo, Reducir el riesgo, Evitar el riesgo y Compartir el riesgo).

La actividad de aceptación del riesgo debe asegurar que los riesgos residuales son aceptados explícitamente por los directores de la entidad.

Para el caso de los riesgos de corrupción es importante resaltar que ningún riesgo de este tipo puede ser aceptado.

El proceso de gestión de los riesgos de seguridad y privacidad de la información deben estar alineados a las etapas enmarcadas en el instrumento de evaluación del MSPI, por lo que se presenta un cuadro resumen de la interacción entre las dos.

ETAPAS DEL MSPI	Gestión del Riesgo en Seguridad de la Información
Planear	Establecer Contexto Valoración del Riesgo Planificación del tratamiento del Riesgo Aceptación del Riesgo
Implementar	Implementación del Plan de Tratamiento de Riesgos
Gestionar	Monitoreo y Revisión Continua de los Riesgos
Mejora Continua	Mantener y Mejorar el Proceso de Gestión del Riesgo en la Seguridad de la Información

ANÁLISIS DEL CONTEXTO ESTRATÉGICO

El contexto estratégico comprende el análisis de los factores internos y del entorno que puedan llegar a afectar a la entidad negativamente con el cumplimiento de la misión y de sus objetivos estratégicos, los cuales se contemplan como causas potenciales para la generación de riesgos en la entidad.

Las condiciones del entorno pueden estar asociadas a factores de carácter social, cultural, económico, político, y legal, ya sea regional o internacional, dependiendo el caso del análisis.

Las condiciones internas están relacionadas con la estructura organizacional, el modelo de operación de la entidad, el nivel de cumplimiento de los planes y programas, los procesos, los procedimientos, el recurso humano, y los recursos financieros con los que cuente la entidad.

Para la Unidad Administrativa Especial de Organizaciones Solidarias se han identificado los siguientes factores, que pueden llegar a repercutir negativamente con la operación y el cumplimiento de la entidad.

FACTORES EXTERNOS		FACTORES INTERNOS	
ECONÓMICOS	• Dificultades para la consolidación de ventajas competitivas de las organizaciones solidarias. • Mortalidad empresarial de las organizaciones solidarias. • Costos de transacción para la creación de organizaciones solidarias. • Presupuesto regional bajo, que no permite que los convenios de asociación tengan un mayor alcance y/o cobertura.	INFRAESTRUCTURA	• No existen actualmente Dependencias de la Unidad a nivel regional. • Infraestructura locativa cuenta con un número fijo de puestos de trabajo, el cual es reducido dada las nuevas necesidades que requiere la Unidad. • No se cuenta con vehículos adecuados para la labor misional en territorio
MEDIOAMBIENTALES	• Condiciones climáticas inadecuadas para el ejercicio de la labor misional en territorio.	PERSONAL	• Reducido número de personas con formación profesional y/o especializada en temas del sector solidario. • Bajo nivel de los procesos de inducción y reinducción. • Baja comprensión de los servidores públicos de la entidad sobre los riesgos y el proceso de gestión del riesgo. • Supervisión limitada por carencia de personal suficiente y por la dispersión geográfica. • Ambiente de control inadecuado por bajo conocimiento de los fines del Estado, su función y sus objetivos.

POLÍTICOS	• Condiciones climáticas inadecuadas para el ejercicio de la labor misional en territorio. • Obstáculos normativos que impiden el desarrollo de las organizaciones del sector y desestimulan su competencia en igualdad de condiciones con otro tipo de organizaciones (Por eje. Comercializadoras Internacionales). • No continuidad o culminación de planes, programas y proyectos, por cambio de gobierno. • No contar con un marco jurídico que desarrolle y potencialice el sector solidario. • Falta de Políticas Públicas para el sector solidario. • Existencia de políticas y programas de comunicaciones para el uso de nuevas tecnología de información y comunicaciones, con aplicación limitada en territorio.	**PROCESOS**	• Escasa participación en espacios de coordinación y planificación por parte de los Servidores Públicos. • Modelo que genera y consolida estadísticas internas y externas del sector solidario en etapa primaria. • Falta de transversalidad del modelo solidario. • No priorizar las necesidades de fomento y fortalecimiento. • No contar con la información y las herramientas adecuadas para determinar un Inventario (información) de las organizaciones que conforman el sector solidario y su ubicación a nivel nacional.
SOCIALES	• Concentración de las Organizaciones Solidarias en sectores del País. • Situaciones de desplazamiento social. • La sociedad no considera el sector solidario como un Modelo alternativo de desarrollo empresarial.	**RECURSOS FINANCIEROS**	• Presupuesto asignado reducido para una Entidad que debe tener mayor presencia a nivel Nacional. • Bajo presupuesto asignado para Educación y Capacitación.
		TECNOLÓGICOS	• No cuenta con equipos suficientes, actualizados y adecuados para el desarrollo de procesos misionales en territorio. • La Unidad cuenta con el uso de mecanismos de comunicación interna como: correo electrónico y aplicativo de gestión documental, así mismo cuenta con mecanismos externos como página WEB e internet, lo anterior presenta una amenaza en cuanto a que se presenten fallas tecnológicas en sus comunicaciones, sistemas de conexión y actualizaciones

Tabla 1. Factores Internos y Externos del Riesgo

El propósito de determinar el contexto estratégico es el de dar soporte y continuidad al modelo de seguridad de la información al interior de la entidad, planteando un plan de repuesta para incidentes.

Para realizar la identificación de las causas que pueden llegar a generar los riesgos en los procesos de la entidad, es necesario que participen los líderes de los procesos junto a un integrante del Grupo de Tecnologías de la Información, una vez se tengan identificados los factores internos y externos, se debe diligenciar el formato de "*Contexto Estratégico*".

ORGANIZACIONES SOLIDARIAS	CONTEXTO ESTRATÉGICO		
PROCESO:			
OBJETIVO:			
FECHA:			
FACTORES EXTERNOS	**CAUSAS**	**FACTORES INTERNOS**	**CAUSAS**

En la primera parte se diligenciaran los factores internos a los cuales se les vincularan las causas, realizando el mismo procedimiento con los factores externos. El contexto estratégico es la base para la identificación de los riesgos.

A continuación se presenta un ejemplo sobre la aplicación de la metodología[1]

[1] Tomado de la Guía para la Administración del Riesgo DAFP.

CONTEXTO ESTRATÉGICO			
PROCESO: ATENCIÓN AL USUARIO			
OBJETIVO: Dar trámite oportuno a las solicitudes provenientes de las diferentes partes interesadas, permitiendo atender las necesidades y expectativas de los usuarios, todo dentro de una cultura de servicio y de acuerdo a las disposiciones legales vigentes.			
FACTORES EXTERNOS	**CAUSAS**	**FACTORES INTERNOS**	**CAUSAS**
Nueva tecnología disponible	No se realizan las actualizaciones de hardware y software.	Tecnología	Número de equipos insuficiente y algunos obsoletos.
Normatividad	Cambios normativos.	Talento humano	- Desconocimiento de la normatividad aplicada - Resistencia al cambio. - Desmotivación.
Relación con otras entidades.	Demoras en la respuesta de comunicaciones enviadas a otras entidades relacionadas.	Sistemas de información	-Proceso manual que puede generar registros erróneos o falta de registros. -Información desactualizada
Necesidades de la comunidad.	Incremento en el número de solicitudes por alta demanda de usuarios, desbordando la capacidad instalada.	Procedimientos	Fallas en el seguimiento a los procedimientos del proceso.

IDENTIFICACIÓN DEL RIESGO

Esta etapa permite conocer los eventos potenciales que pueden llegar a poner en riesgo el cumplimiento de la misión y los objetivos estratégicos de la entidad. Actualmente la entidad cuenta con un software de calidad llamado “Isolución” el cual posee un módulo para la gestión y administración del sistema de seguridad y privacidad de la información.

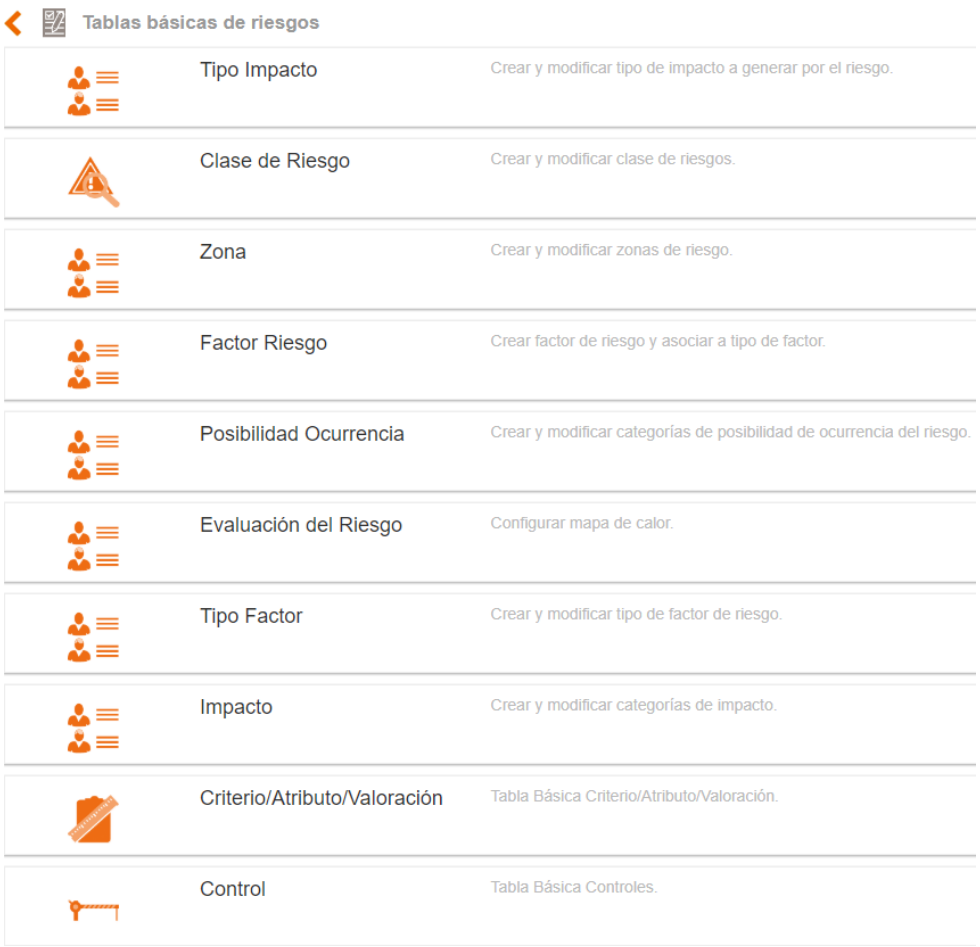
El módulo permite la gestión de las principales actividades que hacen parte de la seguridad y privacidad de la información como:

- Gestión de activos de información
- Gestión de Riesgos Dafp SI
- Matriz de Requisitos Legales
- Administración de Incidentes

- Administración SOA
- Administración GAP

La gestión de riesgos es una actividad clave para el resguardo de los activos de información de la entidad y en consecuencia protege la capacidad de cumplir sus principales objetivos. Es un proceso constante que permite a la administración balancear los costos operacionales y económicos causados por la interrupción de las actividades y la pérdida de activos, con los costos de las medidas de protección a aplicar sobre los sistemas de información y los datos que dan soporte al funcionamiento de la organización, reduciendo los riegos que presentan los activos de información a niveles aceptables para la misma.

Para iniciar con el proceso de gestión del riesgo es necesario diligenciar la información solicitada por las tablas básicas para la administración del riesgo:



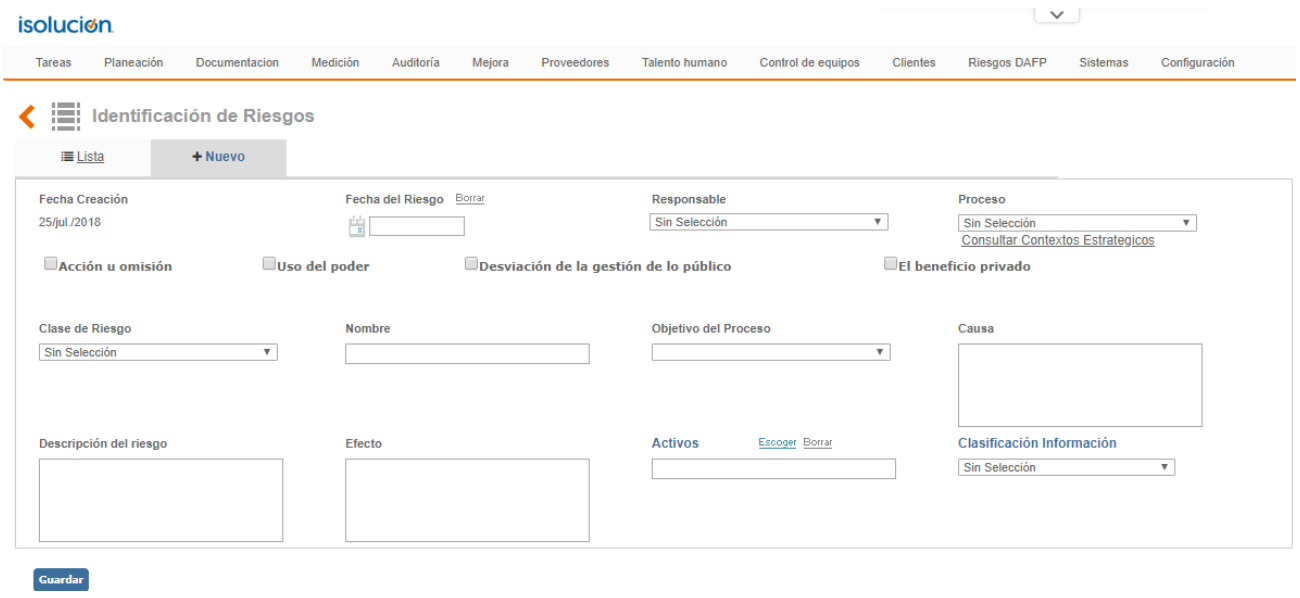
Es importante resaltar que las tablas básicas deben diligenciarse teniendo en cuenta los criterios establecidos en la guía de administración del riesgo del DAFP, tales como impacto, probabilidad y valoración del riesgo:

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

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

Fuente: Guía de riesgos DAFP

Una vez diligenciadas las tablas básicas se procede a identificar el riesgo, esta etapa comprende la determinación de la siguiente información:

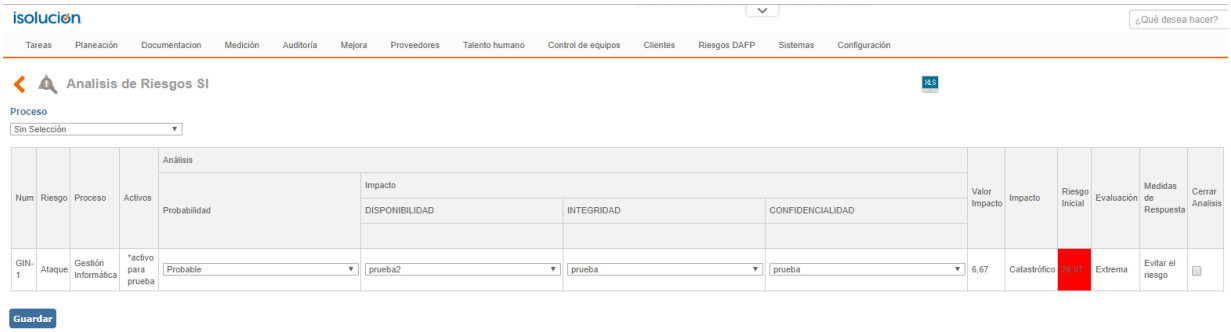


- **Fecha de Creación:** Fecha en la que se está realizando la actividad de identificación del riesgo.
- **Fecha del Riesgo:** Fecha en la que se identificó el riesgo.
- **Responsable:** Nombre del responsable del proceso de gestión del riesgo.
- **Proceso:** Nombre del proceso al cual el riesgo identificado puede llegar a afectar.
- **Clase de Riesgo:** Se selecciona la clase de riesgo, este puede ser (estratégico, operativo, corrupción etc.)
- **Nombre:** Nombre del riesgo.
- **Objetivo del Proceso:** Se selecciona el objetivo del proceso.
- **Causas (Amenazas y Vulnerabilidades):** Se determinan las causas que originan la materialización de los riesgos.
- **Descripción del Riesgo:** Breve descripción del riesgo identificado.
- **Efecto:** Descripción del efecto que se presentaría si el riesgo se materializara.
- **Activos:** Se selecciona el activo de información que pueda afectarse con el riesgo identificado.
- **Clasificación Información:** Se selecciona de la lista el valor asociado al nivel de clasificación del riesgo.

ANÁLISIS DEL RIESGO

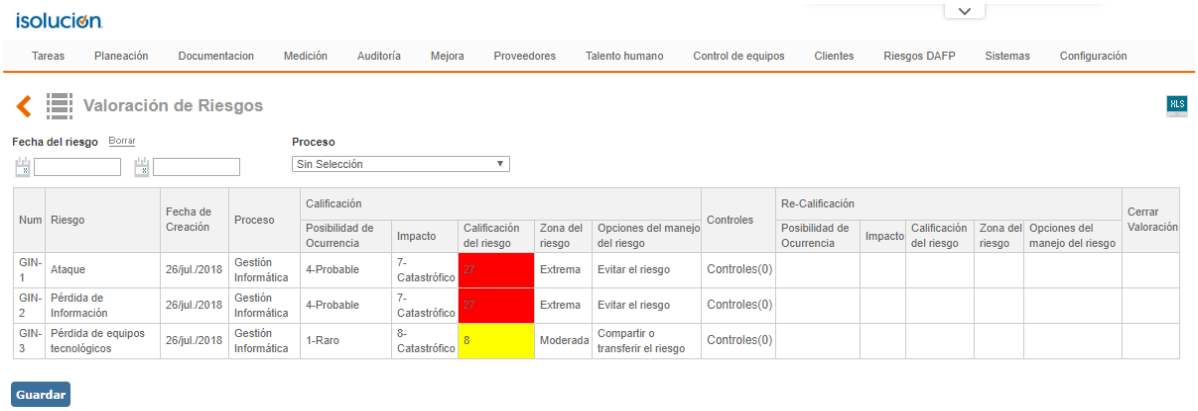
Esta etapa comprende el análisis del riesgo en términos de probabilidad e impacto, que tan probable es que el riego ocurra y el impacto que este podría llegar a generar en los procesos o en la entidad.

Al determinar la probabilidad y los valores de disponibilidad, integridad y confidencialidad que afectan al activo de información, el sistema genera automáticamente los resultados de valor impacto, impacto, valor del riesgo inicial, evaluación y la medida de tratamiento del riesgo.

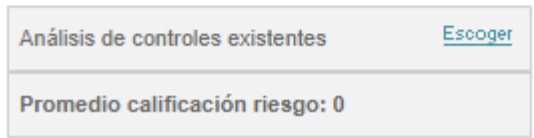


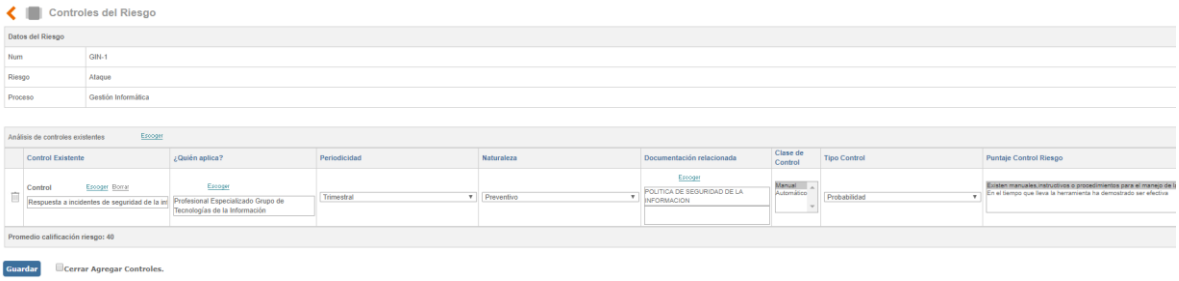
VALORACIÓN DEL RIESGO

Esta etapa consiste en la identificación de controles y el cálculo del riesgo residual. Los controles a aplicar son los establecidos en el Anexo A de la norma NTC: ISO/IEC 27001. Se pueden aplicar varios controles con la finalidad reducir el impacto u ocurrencia del mismo, la valoración del riesgo en el software Isolución se realiza de la siguiente manera:



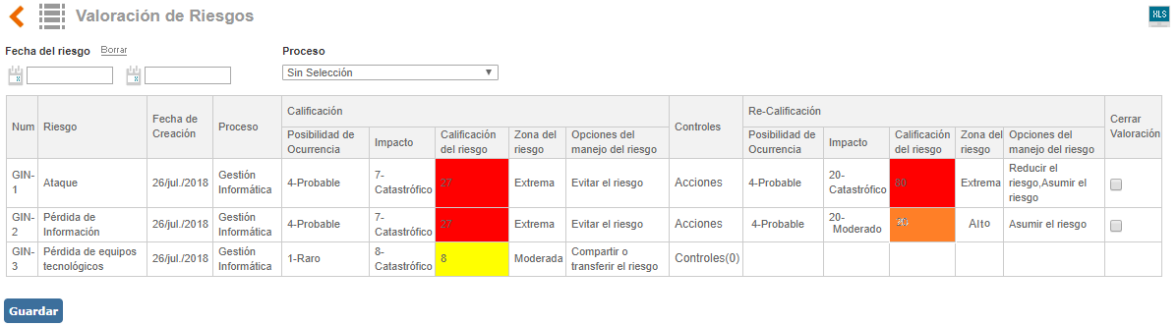
Num	Riesgo	Fecha de Creación	Proceso	Calificación					Controles	Re-Calificación					Cerrar Valoración
				Posibilidad de Ocurrencia	Impacto	Calificación del riesgo	Zona del riesgo	Opciones del manejo del riesgo		Posibilidad de Ocurrencia	Impacto	Calificación del riesgo	Zona del riesgo	Opciones del manejo del riesgo	
GIN-1	Ataque	26/jul./2018	Gestión Informática	4-Probable	7-Catastrófico	27	Extrema	Evitar el riesgo	Controles(0)						
GIN-2	Pérdida de Información	26/jul./2018	Gestión Informática	4-Probable	7-Catastrófico	27	Extrema	Evitar el riesgo	Controles(0)						
GIN-3	Pérdida de equipos tecnológicos	26/jul./2018	Gestión Informática	1-Raro	8-Catastrófico	8	Moderada	Compartir o transferir el riesgo	Controles(0)						





La elección de los controles para la mitigación del riesgo da como resultado un puntaje de “efectividad”, el cual será determinante para la valoración del riesgo residual. La efectividad de los controles está dada por el estado en el que se encuentren (documentados, en desarrollo o no creados).

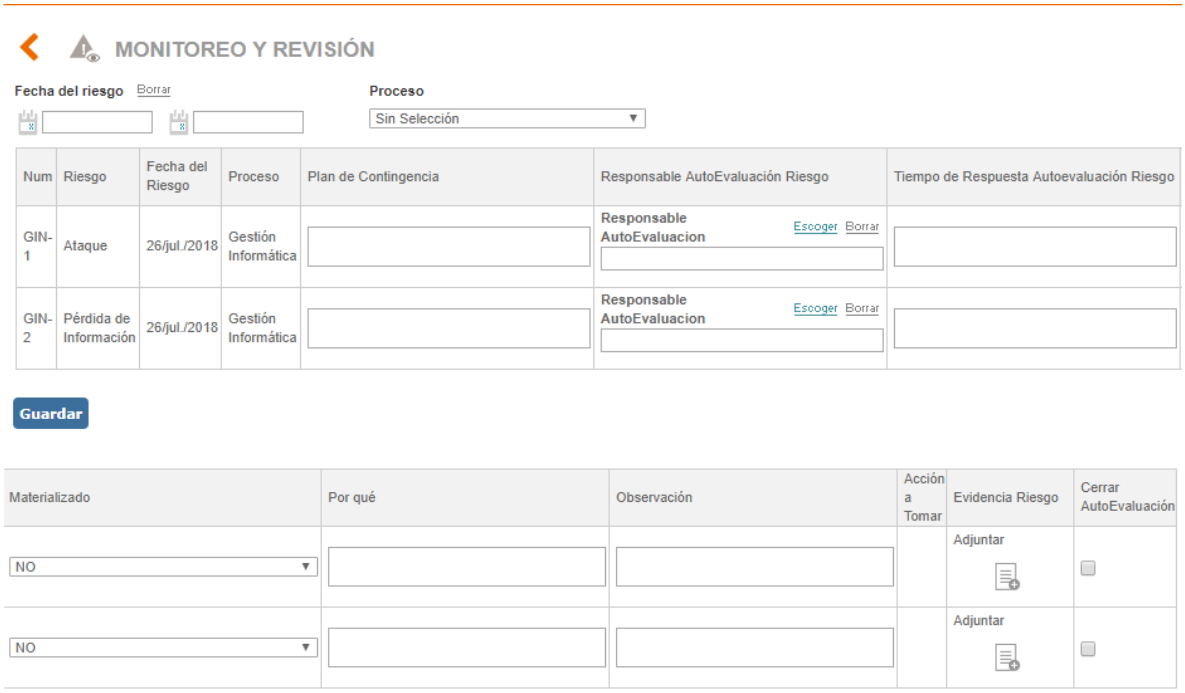
Una vez se establezcan los controles se obtiene como resultado el riesgo residual:



Num	Riesgo	Fecha de Creación	Proceso	Calificación					Controles	Re-Calificación					Cerrar Valoración
				Posibilidad de Ocurrencia	Impacto	Calificación del riesgo	Zona del riesgo	Opciones del manejo del riesgo		Posibilidad de Ocurrencia	Impacto	Calificación del riesgo	Zona del riesgo	Opciones del manejo del riesgo	
GIN-1	Ataque	26/jul./2018	Gestión Informática	4-Probable	7-Catastrófico	80	Extrema	Evitar el riesgo	Acciones	4-Probable	20-Catastrófico	80	Extrema	Reducir el riesgo,Asumir el riesgo	
GIN-2	Pérdida de Información	26/jul./2018	Gestión Informática	4-Probable	7-Catastrófico	80	Extrema	Evitar el riesgo	Acciones	4-Probable	20-Moderado	40	Alto	Asumir el riesgo	
GIN-3	Pérdida de equipos tecnológicos	26/jul./2018	Gestión Informática	1-Raro	8-Catastrófico	8	Moderada	Compartir o transferir el riesgo	Controles(0)						

SEGUIMIENTO DEL RIESGO

Luego de elegir los controles adecuados para la mitigación de los riesgos obteniendo un nivel aceptable se debe realizar el tratamiento de los riesgos, en el cual se evaluarán la efectividad de los controles elegidos y las acciones a tomar para la mitigación de los riesgos.



MAPA DE RIESGOS

Una vez se tenga identificada toda la información relacionada con los riesgos de seguridad de la información, esta se consolida automáticamente en el mapa de riesgos, el cual permite identificar claramente los riesgos, su evaluación (impacto y probabilidad), los controles efectuados y la nueva calificación que da como resultado el riesgo residual.

Mapa de Riesgos

Fecha del riesgo Borrar: 08/ago./2017 – 08/ago./2018 | Proceso: Sin Selección | Clase de Riesgo: Sin Selección | Zona de Riesgo: Sin Selección

Num	Proceso	Causa	Nombre Riesgo	Consecuencias Potenciales	Objetivo Proceso	Calificación				Controles	Valoración del riesgo				Acciones de control	Responsable
						Posibilidad de Ocurrencia	Impacto	Evaluación	Medidas de Respuesta		Posibilidad de Ocurrencia	Impacto	Evaluación	Medidas de Respuesta		
GIN-1	Gestión Informática	Falta de actualizaciones Falta de antivirus	Ataque	perdida de infromacion daño de equipos		4-Probable	20-Catastrófico	Extrema	Evitar el riesgo	Respuesta a incidentes de seguridad de la información	4-Probable	20-Catastrófico		Reducir el riesgo,Asumir el riesgo		
GIN-2	Gestión Informática	Backups mal realizados. No se prueban los backups. No se realiza seguimiento a la actividad de copias de seguridad de la información.	Pérdida de Información	Paralización de procesos. Retraso de actividades. Aumento de costos.		4-Probable	20-Catastrófico	Extrema	Evitar el riesgo	Procedimiento de ingreso seguro Pruebas de seguridad de sistemas	2-Improbable	20-Catastrófico		Asumir el riesgo		
GIN-3	Gestión Informática	Falta de controles de acceso al inventario físico. Falta de seguridad perímetral.	Pérdida de equipos tecnológicos	Retraso en actividades de la entidad. Aumento de los costos de tecnología.		1-Raro	20-Catastrófico	Moderada	Compartir o transferir el riesgo							