INDICE:

Modificaciones respeto a la edición anterior:

1.- Objetivo

Establecer la metodología para la gestión de riesgos en la organización.

2.- Alcance

Cubre los riesgos derivados de:

- el análisis de contexto y partes interesadas (6.1.1 de ISO 27001)
- los propios de la seguridad de la información (6.1.2 de ISO 27001)

3. Referencias

- Norma ISO 27001
- ISO 31000

4.- Definiciones y abreviaturas

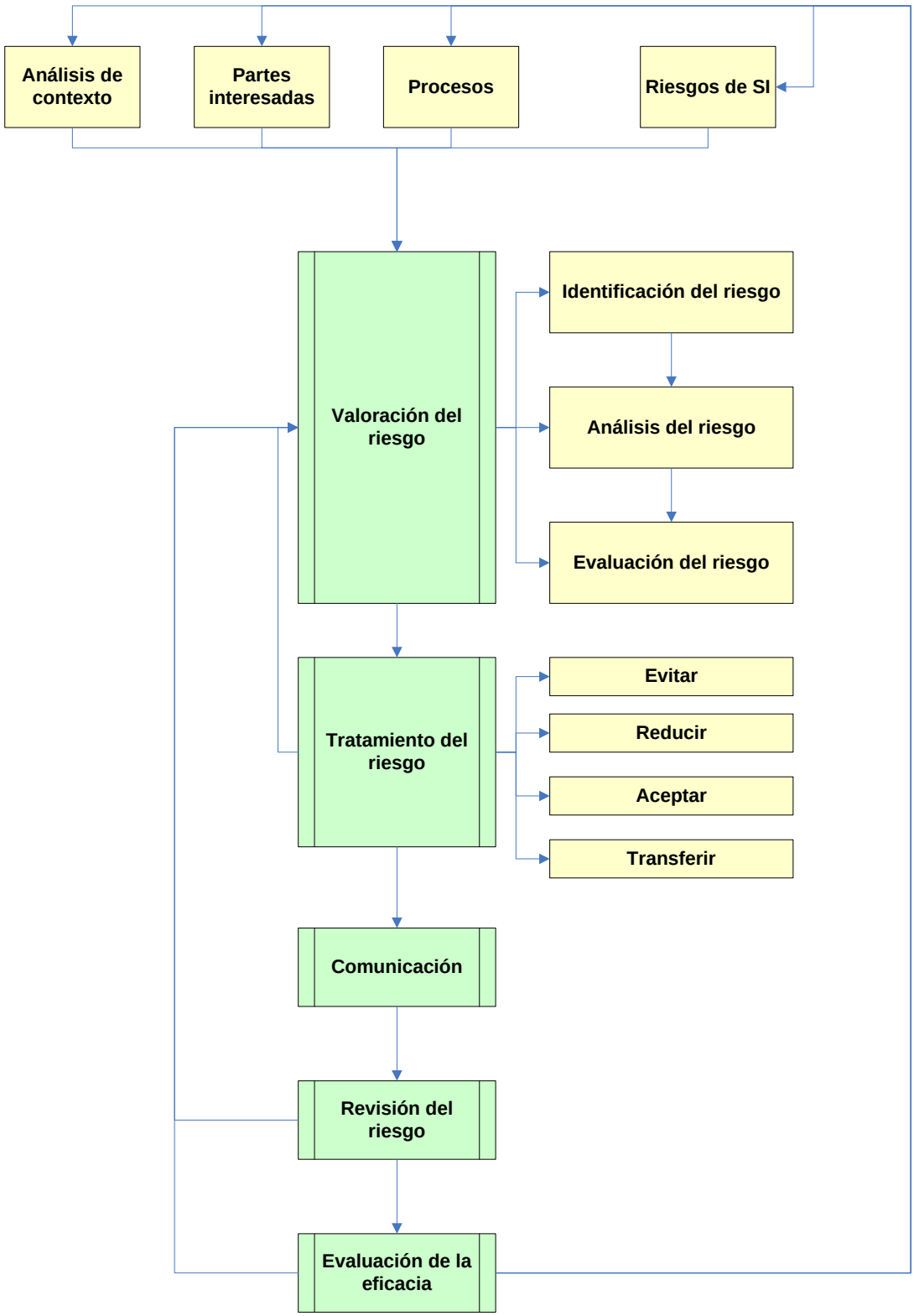
- Riesgo: Efecto de la incertidumbre sobre los objetivos de la organización. Se calcula como el producto de la probabilidad que ocurra el riesgo por su severidad (el efecto que produce el riesgo)
- Fuente de riesgo: Elemento que por sí solo o en combinación tiene el potencial intrínseco para dar lugar a riesgo
- El tratamiento del riesgo: es el proceso para modificar el riesgo. El tratamiento del riesgo puede incluir*:*
    - **Evitar** o eliminar el riesgo: por ejemplo, sustituyendo el activo por otro que no se vea afectado por la amenaza o eliminando la actividad que lo produce.
    - **Reducirlo o mitigarlo:** tomando las medidas oportunas para que el nivel de riesgo se sitúe por debajo del umbral. Para conseguirlo se puede:
        - o reducir la probabilidad o frecuencia de ocurrencia: tomando, por ejemplo, medidas preventivas
        - o reducir el impacto de la amenaza o acotar el impacto, estableciendo por ejemplo controles y revisando el funcionamiento de las medidas preventivas.
    - **Transferirlo, compartirlo o asignarlo a terceros:** en ocasiones la empresa no tiene la capacidad de tratamiento y precisa la contratación de un tercero con capacidad para reducir y gestionar el riesgo dejándolo por debajo del umbral.

- **Aceptarlo:** se asume el riesgo, bien porque está debajo del umbral aceptable de riesgo bien en situaciones en las que los costes de su tratamiento son elevados y aun siendo riesgos de impacto alto su probabilidad de ocurrencia es baja o porque aun a pesar del riesgo la empresa no quiere dejar de aprovechar la oportunidad que para su negocio supone esa actividad arriesgada.

- **Activo**: cualquier recurso de la empresa necesario para desempeñar las actividades diarias y cuya no disponibilidad o deterioro supone un agravio o coste. La naturaleza de los activos dependerá de la empresa, pero su protección es el fin último de la gestión de riesgos. La valoración de los activos es importante para la evaluación de la magnitud del riesgo. En definitiva, un activo es una fuente de riesgo siendo el elemento que sólo o con otros puede originar un riesgo.
- **Amenaza**: circunstancia o suceso desfavorable que puede ocurrir y que cuando sucede tiene consecuencias negativas sobre los activos provocando su indisponibilidad, funcionamiento incorrecto o pérdida de valor.
- **Vulnerabilidad**: debilidad que presentan los activos y que facilita la materialización de las amenazas.
- **Impacto o consecuencia** de la materialización de una amenaza sobre un activo aprovechando una vulnerabilidad.
- **Probabilidad/ Frecuencia**: es la posibilidad de ocurrencia de un hecho, suceso o acontecimiento. La frecuencia de ocurrencia implícita se corresponde con la amenaza. Para estimar la frecuencia podemos basarnos en datos empíricos (datos objetivos) del histórico de la empresa, o en opiniones de expertos o del empresario (datos subjetivos).

5.- Realización

5.1 Proceso de Gestión de Riesgo



5.2 Responsabilidades

La identificación de peligros y la evaluación de riesgos son responsabilidad de:

- Dirección
- Oficial SGSI

5.3 Gestión de los riesgos

5.3.1 Elementos de entrada

Se consideran para la gestión de riesgos los siguientes elementos:

- Análisis de contexto (punto 4.1 del Manual de Gestión)
- Partes interesadas (punto 4.2 del Manual de Gestión y consideradas al realizar el análisis de contexto)
- Procesos de negocio
- Riesgos de SI (activos, personas)

5.3.2 Valoración del riesgo

La valoración del riesgo consiste en:

- identificar los peligros y
- analizar y evaluar los riesgos asociados a la exposición a dichos peligros

La identificación figura en la planilla de Gestión de Riesgos, tomando en cuenta lo establecido en 5.3.1.

La evaluación se realiza en base a los siguientes criterios:

- Impacto. Se analizan los siguientes atributos: impacto legal, imagen y pérdida de confianza, interés por el activo y exposición. Se cuantifican en una escala continua de 1 a 5. Estos criterios figuran detallados en la planilla de Gestión de Riesgos
- Clasificación. Se analizan los atributos de confidencialidad, disponibilidad e integridad. Se cuantifican en una escala discreta (1,3,5 o 1,3). Estos criterios figuran detallados en la planilla de Gestión de Riesgos
- Frecuencia. En función de no disponer registros históricos sobre los elementos de riesgo evaluado, se asume una frecuencia con base en los siguientes criterios:
    - 0.05: sucede en forma permanente
    - 0.04: no sucedió en el último mes
    - 0.03: no sucedió en el último año
    - 0.02: no sucedió en los últimos cinco años
    - 0.01: no sucedió nunca

Este valor es actualizado con la revisión anual de los riesgos tomando en cuenta la gestión de incidentes, auditorías internas, auditorías externas, etc.

- Se fija una cota mínima: 6 puntos.

5.3.3 Tratamiento del riesgo

Se compara el valor resultante de la valoración del riesgo contra la cota mínima. En función de tal comparación se decide el tratamiento del riesgo que puede incluir las decisiones de:

- Evitar o eliminar el riesgo: se establece cómo en el campo *forma de gestión del riesgo*
- Reducirlo o mitigarlo: se establece cómo en el campo *forma de gestión del riesgo*
- Transferirlo, compartirlo o asignarlo a terceros: se establece cómo en el campo *forma de gestión del riesgo*
- Aceptarlo: se establece la aceptación solamente.

5.3.4 Comunicación del riesgo:

La ***comunicación del riesgo*** consiste en el intercambio de información sobre el riesgo y su gestión entre quienes toman las decisiones y otras partes que están involucradas en la gestión del riesgo.

5.3.5 Revisión del riesgo:

La gestión del riesgo es un proceso continuo del Sistema tomando en cuenta las situaciones cambiantes que afectan al riesgo. El Oficial del SGSI es el responsable también de realizar su revisión que se establece con período anual.

Los resultados del proceso de gestión del riesgo deben revisarse teniendo en cuenta nuevos conocimientos y la experiencia. La revisión del riesgo podría incluir una reconsideración de las decisiones adoptadas para la aceptación del riesgo.

5.3.6 Evaluación de la eficacia

Las medidas tomadas para gestión del riesgo deben ser analizadas para verificar que son eficaces y mantienen el riesgo controlado. En los casos que corresponda, se indica cuáles fueron las medidas para comprobar su eficacia (desafiar el control, realizar una auditoría, verificar in situ en forma aleatoria, etc.)

5.3.7 Etiquetado

El registro de evaluación de riesgos incluye el etiquetado del activo información.

6. Registros

Gestión de riesgos.