Declaración de apetito de riesgo.





SEGURIDAD DE LA

INFORMACIÓN

Declaración de apetito de riesgo

|  |  |  |  |
| --- | --- | --- | --- |
| **Versión** | 1.0 | **Categoría** | Declaración |
| **Última actualización** | 30/07/2023 | **Estado** | Aprobado |
| **Aprobado por** | [cargo][nombre][firma] |

# Objetivo

La declaración de apetito de riesgo marca las pautas para la gestión del riesgo en los distintos niveles dentro de la organización. Esta declaración refuerza la capacidad de la Dirección de adoptar decisiones fundamentadas y eficaces al

tiempo que se mantiene la exposición al riesgo dentro de límites aceptables y definidos.

# Referencias normativas

Acá se especifican leyes, reglamentaciones y/o procedimientos internos que apoyen las decisiones especificadas.

# Responsabilidades

**RSI - Responsable de seguridad de la información** debe velar por el cumplimiento de la definición de Apetito de riesgo en cada iteración del proceso de gestión de riesgos.

**Equipo de gestión de riesgos** debe ejecutar el proceso de gestión de riesgos teniendo en cuenta las definiciones de este documento, y si detecta desviaciones analizar la necesidad de actualizar las definiciones e informar al RSI.

**Dirección** establece y aprueba el apetito de riesgo, y realiza una revisión al menos anualmente, o cuando el RSI detecte que se necesita actualizar la definición. La dirección es responsable de establecer y ejecutar las comunicaciones pertinentes.

# Componentes

## Apetito de riesgo.

Para definir el apetito de riesgo se evalúan todos los posibles riesgos que la organización afronta y puede soportar estableciendo los límites de aceptación y los

correspondientes controles necesarios.

### Criterios

**Estimación de Probabilidad**

1-Muy Bajo: puede ocurrir solo en circunstancias excepcionales.

2-Bajo: es un suceso raro e infrecuente, aunque no improbable.

3-Medio: es posible que ocurra una vez al año.

4-Alto: es posible que ocurra varias veces en el año.

5-Muy Alto: es posible que ocurra en periodos menores a 1 año.

**Estimación del impacto**

1-Muy Bajo: No se registra adulteración, pérdida, consulta o tratamiento no autorizado, así como desviaciones de información. No hay costos económicos y las operaciones no se ven afectadas. No se registran comentarios adversos que afecten la reputación de la organización.

2-Bajo: Se registra una consulta o tratamiento no autorizado. Costos económicos extras menores. Las operaciones de negocio no son afectadas significativamente, la interrupción no es percibida por las áreas usuarias. Hay algún comentario adverso externo sin llegar a los medios de comunicación o redes sociales.

3-Moderado: Se registra adulteración, pérdida, consulta o tratamiento no autorizado, o desviaciones de información sin consecuencias significativas. Afecta las operaciones del negocio en hasta un día ocasionando retrabajos que afectan al área de TI. Puede existir un impacto económico importante. Hay comentarios adversos a la organización en los medios o redes sociales.

4-Alto: Se registra adulteración, pérdida, consulta o tratamiento no autorizado, o desviaciones de información con consecuencias significativas. Afecta las operaciones del negocio en más de un día ocasionando retrabajos, la necesidad de contratar servicios adicionales y/o pérdidas económicas. Hay comentarios adversos a la organización en los medios o redes sociales durante más de 1 semana.

5-Muy Alto: Se registra adulteración, pérdida, consulta o tratamiento no autorizado, o desviaciones de información sensible o confidencial. Afecta las operaciones del negocio, tendiendo a forzar su cierre o reformulación. Tiene un impacto económico significativo. Se daña la reputación de la organización.

**Mapa de calor: impacto x probabilidad.**

**[Los colores utilizados en los criterios son a modo de ejemplo, deben ser establecidos de acuerdo al apetito de riesgo de la organización.**

**En el ejemplo, el apetito está en los valores entre 1 y 4. Entre 5 y 9 tenemos la tolerancia.]**

|  |  |
| --- | --- |
|  | **Impacto** |
| **Probabilidad** | **1** | **2** | **3** | **4** | **5** |
| **5** | 5 | 10 | 15 | 20 | 25 |
| **4** | 4 | 8 | 12 | 16 | 20 |
| **3** | 3 | 6 | 9 | 12 | 15 |
| **2** | 2 | 4 | 6 | 8 | 10 |
| **1** | 1 | 2 | 3 | 4 | 5 |

Valor entre 1 y 4: Riesgo tolerable.

Valor entre 5 y 9: Riesgo tolerable, pero merece atención.

Valor entre 10 y 25: Riesgo no tolerable, son necesarias acciones.

**Niveles de riesgo y tratamiento.**

|  |  |  |
| --- | --- | --- |
| **Nivel** | **Descripción** | **Tratamiento** |
| Bajo | Tienen un bajo efecto negativo en la organización, por lo que son considerados aceptables. Pueden tomarse acciones pero su prioridad para el tratamiento es baja. | Aceptar y mantener observación. |
| Alto | Pueden tener serios efectos negativos en la organización por lo que estos riesgos deberían ser reducidos o tratados de alguna forma para ser más aceptables. | Aplicar controles sólo si se considera necesario y mantener bajo observación. |
| Crítico | Tienen efectos muy negativos en la organización ydeberían ser reducidos o tratados de alguna forma en todas las circunstancias. | Aplicar controles para mitigar o considerar eliminar el activo que provoca el riesgo. |

## Capacidad para asumir riesgos.

La capacidad para asumir riesgos hace referencia a la capacidad de la organización, en términos de recursos, para permitirse asumir un determinado riesgo en un momento concreto, aunque este riesgo sea de un nivel que indique aplicar algún tratamiento.

Se analizará cada situación particular en función del objetivo estratégico que afecte, y la Dirección será la responsable de aprobar que se asuma un riesgo particular.

## Tolerancia al riesgo.

Se define la desviación respecto al nivel de riesgo aceptado por la organización. De acuerdo a la definición de niveles de riesgo y el tratamiento para cada nivel, la tolerancia se encuentra dentro de los riesgos de nivel significativos. Éstos pueden ser aceptados hasta la próxima revisión, y sólo si pasan a nivel Alto serán aplicados controles.

# **Comunicación**.

La declaración de apetito de riesgo de la organización debe comunicarse a todos los niveles de la organización para garantizar que el conjunto de directivos y personal actúen teniendo presente la gestión del riesgo, y para que los encargados de la supervisión y el seguimiento tengan claro si los riesgos se están gestionando conforme al apetito de riesgo aprobado.

# Cumplimiento

Ante la verificación del incumplimiento de lo estipulado en este documento, la Dirección de la organización podrá tomar las medidas que se considere pertinentes, a efectos de darle el debido cumplimiento.

**Historial de revisiones**

|  |  |  |
| --- | --- | --- |
| **Fecha de revisión** | **Responsable** | **Resumen de cambios** |
|  |  |  |

