Fidelitas

# Política de GESTIÓN DE RIESGOS

## Control de versiones

| | |
|---|---|
| **Código.** | FIITPO003 |
| **Versión.** | V1.0 |
| **Fecha de la versión.** | 12/9/2025 |
| **Creado por.** | Alejandro Burgol |
| **Aprobado por.** | Comité de seguridad (Félix El Idd, Jorge El Idd, Alejandro Burgol, Natalia Queija) |
| **Clasificación.** | Público |

## Historial de modificaciones

| Fecha. | Versión. | Creado por. | Descripción de la modificación. |
|---|---|---|---|
| 12/09/2025 | 1.0 | Alejandro Burgol | Documento inicial |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |

# Tabla de contenido

# 1. Objetivos y alcance

**Objeto**

Este documento describe una política y una metodología para la adopción formal de la gestión de riesgos en FIDELITAS SA. Esto implica un proceso de identificación, evaluación, ponderación de impacto, mitigación y monitoreo de los riesgos, con el objetivo de mejorar la toma de decisiones.

**Alcance**

La política debe ser aplicada por toda la empresa.

# 2. Documentos de referencia

- Manual de SGSI.
- Política de SGSI.
- Metodología de Gestión de Riesgos.
- ISO/IEC ISO 27001:2022.
- ISO/IEC ISO 27018:2019
- ISO/IEC ISO 27005:2022
- Matriz de Gestión de Riesgos.

# 3. Vigencia del documento

Este documento es válido desde su fecha de aprobación.

El propietario del documento es el CTO, que debe verificar y actualizar, de ser necesario al menos una vez al año.

# 4. Roles y responsabilidades

A continuación, las responsabilidades definidas según su rol:

- **Comité de Seguridad:** Desarrolla, implementa y mantiene las políticas y procedimientos de gestión de riesgos. Revisa periódicamente los informes de riesgo y toma decisiones estratégicas.
- **Alta Dirección:** Asegura que las responsabilidades y la rendición de cuentas en la gestión de riesgos sean asignadas y comunicadas a toda la organización. Asigna recursos necesarios para la gestión de riesgos.
- **Propietario de los riesgos:** Identificar evaluar riesgos en sus áreas. Implementar y monitorear los controles aprobados.
- **CTO:** Gestiona integralmente el cumplimiento de esta política.
- **Áreas de las organización:** Aplican las medidas de control y mitigación de riesgos en sus áreas de responsabilidad.

# 5. Lineamientos de política

## 5.1. Definiciones

**Riesgo:** Se define como la incertidumbre resultante de la posible ocurrencia de un evento que puede impactar en forma negativa al cumplimiento de los objetivos de FIDELITAS S.A.

**Gestión de Riesgos:** Proceso continuo conformado por un conjunto de herramientas y acciones que permite, de forma sistemática, identificar, evaluar y tomar acción de manera racional sobre un los eventos que pueden afectar a la organización y que representan una amenaza para el cumplimiento de los objetivos actuales o futuros

**Proceso:** Actividades habituales gestionadas por la administración.

**Riesgo Inherente**: Toda actividad, solo por el hecho de ser realizada, en sí tiene asociado un riesgo implícito (es decir, antes de aplicar controles). Es también llamado riesgo puro.

**Riesgo Residual:** Es aquel riesgo que subsiste, después de haber implementado controles.

### 5.2. Declaración

FIDELITAS SA ha decidido implementar una política que permita reconocer de forma sistemática los eventos internos o externos a ella que pueden representar riesgos para el logro de los objetivos del negocio.

Lo anterior requiere la implementación de herramientas para evaluarlos de manera consistente, determinar sus consecuencias y poder desarrollar acciones de tratamiento que permitan mantenerlos en un nivel aceptable.

Es política de FIDELITAS SA:

- Establecer, formalizar y poner en práctica una metodología integral para la gestión del riesgo que contempla las siguientes actividades:
    - El alcance del proceso de gestión de riesgos y su necesidad de adaptación al contexto más actual de FIDELITAS SA.
    - La implementación de métodos para la identificación y evaluación de los riesgos de seguridad de la información será basado en ISO 27005.
    - El análisis y decisión de los planes de tratamiento de riesgo.
    - La definición del umbral de tolerancia y los criterios de aceptación de los riesgos.
    - La evaluación y aceptación del nivel de riesgo residual.
- Contar con la aprobación explícita de los planes de tratamiento de los riesgos.
- Determinar la decisión ante el riesgo que contempla las siguientes opciones:
    - Aceptar
    - Mitigar
    - Transferir
    - Eliminar
- Realizar evaluaciones periódicas de los procedimientos en uso para el control de los riesgos.
- Mantener informadas a las partes involucradas sobre el estado y el perfil de riesgos de la organización.
- Establecer una Matriz de Gestión de Riesgos que permita la realización de las actividades emanadas de la presente política sobre los riesgos. Esta Matriz deberá contemplar por lo menos:
    - Proceso asociado
    - Tipo de activo
    - Nombre o ID del activo
    - ID de riesgo
    - Amenaza
    - Vulnerabilidad
    - Descripción del riesgo
    - Dueño del riesgo
    - Probabilidad
    - Impacto
    - Nivel de riesgo (Riesgo inherente)

- Decisión/Opción de tratamiento
- Acción Recomendada/Justificación de Aceptación
- Plan de tratamiento
- Responsable de seguimiento
- Estado del riesgo
- Fecha de cierre
- Probabilidad residual
- Impacto residual
- Nivel de riesgo Residual
- Acciones recomendadas
- Responsable de seguimiento
- Fecha de seguimiento
- Evidencia
- Comentarios de seguimiento
- Fecha de próximo seguimiento
- Comentarios de comunicación

## Criterios de aceptación y niveles de riesgos

***Niveles de Riesgo y aprobación***

**Crítico:**

- **Definición:** Riesgos que amenazan la viabilidad de la organización, su continuidad operativa, o su reputación, y que requieren de una respuesta inmediata.
- **Acciones Requeridas:**
  - Movilización inmediata de recursos para mitigar el riesgo.
  - Implementación de un plan de contingencia o tratamiento.
  - No admite aprobación directa, solo en el caso que el costo de implementar y subsanar sea mayor al beneficio.
  - Comunicación constante a la Alta Dirección y accionistas clave.
- ***Ejemplos:*** *Desastre natural que inutiliza las instalaciones principales, ciberataque masivo que compromete datos críticos, crisis de reputación que afecta gravemente la imagen de FIDELITAS SA.*

**Alto:**

- **Definición:** Riesgos que, de materializarse, podrían afectar significativamente las operaciones, la rentabilidad, o la reputación de la organización, y que requieren de una respuesta rápida y decisiva.
- **Acciones Requeridas:**
  - Desarrollo e implementación de un plan de acción detallado dentro de los 30 días siguientes a la identificación del riesgo.
  - No admite aprobación directa, solo en el caso que el costo de implementar y subsanar sea mayor al beneficio.

    - Monitoreo constante y ajuste del plan de acción según sea necesario.
    - Comunicación regular al Comité de Gestión de Riesgos y a las partes interesadas relevantes.
- ***Ejemplos:*** *Incumplimiento normativo significativo, pérdida de un cliente clave, fallo importante en un sistema crítico.*

**Medio:**

- **Definición:** Riesgos que, de materializarse, podrían causar interrupciones operativas, pérdidas financieras, o daños a la reputación, pero que pueden ser gestionados con acciones planificadas y controladas.
- **Acciones Requeridas:**
    - Desarrollo e implementación de un plan de acción detallado dentro de los 90 días siguientes a la identificación del riesgo.
    - Puede admitir aprobación directa, la decisión quedará a criterio del responsable del riesgo. Se debe presentar la Aceptación de Riesgo Residual en el Informe de Gestión de Riesgos.
    - Monitoreo periódico y ajuste del plan de acción según sea necesario.
    - Comunicación regular al Propietario del Riesgo y a las partes interesadas relevantes.
- ***Ejemplos:*** *Interrupción temporal de la cadena de suministro, litigio menor, problema de calidad de un producto.*

**Bajo:**

- **Definición:** Riesgos que, de materializarse, tendrían un impacto limitado en las operaciones, las finanzas, o la reputación de la organización.
- **Acciones Requeridas:**
    - Asumir el riesgo y presentar la Aceptación de Riesgo Residual en el Informe de Gestión de Riesgos.
- **Ejemplos:** Quejas menores de clientes, pequeños retrasos en proyectos, desgaste normal de equipos.

***Responsables de aprobación***

- **Riesgos Medios y Bajos:** Los Propietarios de Riesgo, que son los responsables directos de las áreas o procesos donde se originan los riesgos, tienen la autoridad para aprobar y gestionar los planes de acción para riesgos medios y bajos.

### 5.3. Registros de los riesgos

La gestión completa de los riesgos debe ser documentada en:

- Matriz de Riesgos.
- Informe de Gestión de Riesgos.
- Declaración de apetito y umbrales de tolerancia.

| | | | |
|---|---|---|---|
| Félix El Idd | Jorge El Idd | Alejandro Burgol | Natalia Queija |
| Félix El Idd | Jorge El Idd | Alejandro Burgol | Natalia Queija |

# Registro de auditoría

## Detalles

| | |
|---|---|
| NOMBRE DEL ARCHIVO | Fidelitas - Política de Gestión de Riesgos.pdf - 16/9/25, 13:09 |
| ESTADO | Firmado |
| MARCA DE TIEMPO DEL ESTADO | 2025/09/16<br>17:44:31 UTC |

## Actividad

| | | |
|---|---|---|
| ENVIADA | natalia.queija@fidelitas.com.ar **ha enviado** una solicitud de firma a:<br>• Félix El Idd (felix@fidelitas.com.ar)<br>• Jorge El Idd (jorge.elidd@fidelitas.com.ar)<br>• Natalia Queija (natalia.queija@fidelitas.com.ar)<br>• Alejandro Burgol (alejandro.burgol@fidelitas.com.ar) | 2025/09/16<br>16:09:27 UTC |
| FIRMADO | **Firmado** por Félix El Idd (felix@fidelitas.com.ar) | 2025/09/16<br>16:34:30 UTC |
| FIRMADO | **Firmado** por Alejandro Burgol (alejandro.burgol@fidelitas.com.ar) | 2025/09/16<br>17:27:32 UTC |
| FIRMADO | **Firmado** por Natalia Queija (natalia.queija@fidelitas.com.ar) | 2025/09/16<br>17:44:31 UTC |
| FIRMADO | **Firmado** por Jorge El Idd (jorge.elidd@fidelitas.com.ar) | 2025/09/16<br>17:09:21 UTC |
| COMPLETADO | Todos los firmantes han firmado este documento y ya se ha **completado** | 2025/09/16<br>17:44:31 UTC |

La dirección de correo indicada arriba para cada firmante puede estar asociada a una cuenta de Google. Puede ser la dirección de correo electrónico principal asociada a la cuenta o una secundaria.