Fidelitas

Política de Tecnología y Operaciones

Control de versiones

Código.	FIITPO001
Versión.	1.0
Fecha de la versión.	28/07/2025
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.

Tabla de contenido

1. Objetivos y alcance

El objetivo de este documento es el de establecer los lineamientos de seguridad de los principales procesos de tecnología de la información aplicados dentro de Fidelitas SA para asegurar la disponibilidad y continuidad del negocio, y la asignación adecuada de los recursos y plataformas tecnológicas para un correcto aprovisionamiento y mantenimiento.

Esta política es aplicable a todos los colaboradores internos y externos con acceso a elementos tecnológicos, y a los proyectos que utilicen cualquier tipo de recurso tecnológico dispuesto por la organización.

2. Documentos de referencia

- Manual de SGSI
- Política de Seguridad de la Información
- OWASP (https://owasp.org.)
- ISO/IEC ISO 27001:2022

3. Vigencia del documento

Este documento es válido desde su fecha de aprobación.

El propietario del documento es 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:

- El área de Infraestructura y Seguridad será responsable de seguir las prácticas aquí descritas y cumplir con esta política.
- El CTO supervisará la implementación y el cumplimiento de la política de tecnología y operaciones.
- El CEO, CTO y COO son los responsables principales en aspectos de seguridad de la información y tecnología en todos los aspectos de la organización.

5. Lineamientos de política

5.1. Gestión de Cambios

La gestión de los cambios tiene como objetivo mejorar los procesos o sistemas de Fidelitas SA, evaluando los posibles riesgos de seguridad asociados y con ello, tomar las mejores decisiones. Así como también llevar el registro y seguimiento oportuno de ellos.

Fidelitas SA contempla, pero no se limita, a los siguientes tipos de cambios:

- Cambios comerciales
- Cambios en infraestructura o instalaciones
- Cambios organizacionales
- Cambios en sistemas de procesamiento de información
- Cambios productivos

La organización determina que para cualquier tipo de cambio debe existir una autorización formal y una evaluación de riesgos previa a su ejecución. Además, se mantiene un registro de todos los cambios realizados.

5.2. Gestión de cambios productivos

Para la implementación de mejoras o nuevas funcionalidades a las plataformas o sistemas de la organización, Fidelitas SA establece un Procedimiento de Gestión de Cambios Productivos donde se definen los pasos a seguir y las herramientas a utilizar, el cual contempla:

- El proceso de autorización formal previo a la instalación de cualquier modificación a los sistemas de la Fidelitas SA.
- La verificación del cumplimiento de todos los requisitos de seguridad y especificaciones definidos para el desarrollo.
- La definición de un procedimiento de rollback, o “vuelta atrás”, para dejar sin efecto los cambios aplicados o para recuperar la última versión autorizada del sistema, en caso de presentar problemas durante o posterior a la instalación.
- El registro de dichos cambios, modificaciones, nuevas funcionalidades o instalaciones efectuadas en el ambiente productivo, documentando toda la información pertinente (véase la sección 3.1 Gestión de los cambios).

Todos los cambios productivos deben encontrarse vinculados a un requerimiento formal y justificado, el cual debe ser analizado y autorizado por el COO, el HSD y el CTO en forma conjunta, así como también se le deben aplicar el plan de pruebas pertinente, todo esto previo a su ejecución.

Estos requerimientos pueden originarse por diferentes causas, como, por ejemplo:

- Para corregir errores identificados por el equipo interno, clientes, proveedores o por notificación de algún incidente;
- Por la adquisición de nuevos servicios;
- Por cambios estratégicos de la organización;
- Por actualizaciones de software;
- Por cambios regulatorios;
- Por implementación de mejoras que agreguen valor al producto o servicio, etcétera.

Por lo que es parte importante del procedimiento conocer el origen y la necesidad del cambio para tomar las decisiones más adecuadas.

La ejecución de los cambios se realiza con base en la Metodología de Ciclo de Vida de Desarrollo definida por la Fidelitas SA, la cual determina todas las actividades necesarias para la planificación, evaluación y seguimiento de los cambios y las herramientas involucradas.

5.3. Gestión de la capacidad

La gestión de la capacidad tiene como objetivo asegurar la disponibilidad de los recursos tecnológicos que soportan la operación correcta del negocio. Para esto, Fidelitas SA define los siguientes lineamientos:

- Se configuran alarmas para recibir una notificación si se presenta algún problema con la capacidad
- La organización realiza un análisis de manera periódica cada 3 (tres) meses para validar que se cuenta con la capacidad necesaria para seguir operando.

Para implementar una gestión adecuada de la capacidad, se deben satisfacer los requisitos de procesamiento y mantener un alto rendimiento de las plataformas y sistemas. Por ello, el análisis debe basarse, por lo menos en lo siguiente:

- Los volúmenes transaccionales estimados.
- Los nuevos proyectos que podrían implementarse.
- La capacidad actual de las plataformas o sistemas.

Los planes de acción que se generen con base en los resultados del análisis de capacidad deben ser revisados y aprobados por el CTO.

5.4. Gestión de los parches de seguridad

La gestión de los parches tiene como objetivo asegurar la correcta instalación de las actualizaciones en los sistemas y la resolución de posibles vulnerabilidades.

Los lineamientos sobre la gestión de vulnerabilidades técnicas se encuentran dentro de la Política de Seguridad de la Información, y su implementación se realiza conforme al Procedimiento de Gestión de Vulnerabilidades definidos por la Fidelitas SA.

Fidelitas SA define los siguientes lineamientos para llevar una adecuada gestión de los parches de seguridad:

- Todo software utilizado por la organización debe actualizarse regularmente.
- Se prueban los nuevos parches en un entorno de pruebas para asegurar que son funcionales y no representan un riesgo para los sistemas de la organización.
- Se consultan listas de vulnerabilidades más comunes, las cuales resumen las mismas a lo largo del proceso de gestión de parches, especialmente si hay algún problema en relación con el despliegue después del entorno de prueba.

5.5. Adquisición y mantenimiento de equipos y sistemas

La adquisición de equipamiento tecnológico ya sea hardware o software, debe ser administrada correctamente y estar alineada a los requisitos de seguridad de la información definidos por Fidelitas SA. Y para esto, Fidelitas SA define los siguientes lineamientos:

- Cualquier componente de la infraestructura, equipo o sistema tecnológico, se implementa y configura siguiendo los lineamientos de las políticas aplicables definidas por la Fidelitas SA;
- Se realiza un mantenimiento oportuno de los equipos y sistemas, velando siempre por la calidad, la seguridad de estos y de la información que contienen;
- Toda adquisición de equipos o sistemas debe ser previamente autorizada por el CTO y también por la alta dirección, si aplica.

Félix H. El Idd	Jorge El Idd	Natalia Queija	Alejandro Burgol
Félix H. El Idd	Jorge El Idd	Natalia Queija	Alejandro Burgol

Registro de auditoría

Detalles

NOMBRE DEL ARCHIVO	Fidelitas - Política de Tecnología y Operaciones.pdf - 20/8/25, 17:10
ESTADO	Firmado
MARCA DE TIEMPO DEL ESTADO	2025/08/20 21:27:19 UTC

Actividad

ENVIADA	natalia.queija@fidelitas.com.ar **ha enviado** una solicitud de firma a: • Alejandro Burgol (alejandro.burgol@fidelitas.com.ar) • Félix H. El Idd (felix@fidelitas.com.ar) • Natalia Queija (natalia.queija@fidelitas.com.ar) • Jorge El Idd (jorge.elidd@fidelitas.com.ar)	2025/08/20 20:10:34 UTC
FIRMADO	**Firmado** por Félix H. El Idd (felix@fidelitas.com.ar)	2025/08/20 21:27:19 UTC
FIRMADO	**Firmado** por Natalia Queija (natalia.queija@fidelitas.com.ar)	2025/08/20 20:19:33 UTC
FIRMADO	**Firmado** por Alejandro Burgol (alejandro.burgol@fidelitas.com.ar)	2025/08/20 20:18:44 UTC
FIRMADO	**Firmado** por Jorge El Idd (jorge.elidd@fidelitas.com.ar)	2025/08/20 20:31:23 UTC
COMPLETADO	Todos los firmantes han firmado este documento y ya se ha **completado**	2025/08/20 21:27:19 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.