Fidelitas

Descriptivo de roles y responsabilidades

Control de versiones

Código.	FIRHDO004
Versión.	1.2
Fecha de la versión.	12/09/2025
Creado por.	Natalia Queija
Aprobado por.	Comité de Seguridad
Clasificación.	Interno

Historial de modificaciones

Fecha.	Versión.	Creado por.	Descripción de la modificación.
12/09/2025	1.2	Natalia Queija	Se agregan roles genéricos de usuarios del sistema y dueños de activos
12/08/2025	1.0	Natalia Queija	Creación inicial del documento

Tabla de contenido

1. Objetivo **4**
2. Alcance **4**
3. Descriptivos **4**
3.1 CEO 4
3.2 CTO - Departamento de Infraestructura y Seguridad 6
3.3 CFO – Departamento de finanzas 8
3.4 COO - Departamento de operaciones 11
3.5 Head of Software Development 12
3.6 Software Developer 13
3.7 Usuarios del sistema 14
3.8 Dueño de Activos 15

1. Objetivo

Este documento tiene como objetivo definir los roles y responsabilidades que se deben desempeñar dentro de Fidelitas SA, así como las características y requerimientos a cubrir para cada cargo.

2. Alcance

Este descriptivo alcanza a todos aquellos puestos que desempeñan cargos relacionados a la seguridad de la información o que tienen responsabilidades relacionadas a ella. Así como también a los roles alcanzados por el SGSI de la organización.

3. Descriptivos

3.1 CEO

Objetivos del puesto

Es el máximo ejecutivo de Fidelitas y su objetivo es proponer, ejecutar y dirigir las estrategias para alcanzar los objetivos corporativos de manera sustentable y empleando óptimamente los recursos.

Responsabilidades

- Desarrolla e implementa estrategias necesarias para cumplir los objetivos corporativos.
- Toma decisiones relativas a las inversiones, sujetas a un uso óptimo del presupuesto.
- Ayuda a que exista una correcta coordinación y comunicación entre las distintas áreas de la empresa.
- Analiza deficiencias en las distintas áreas para proponer planes de mejora o cambios de estructura cuando sea necesario.
- Gestiona la organización y a todos los colaboradores, comunicando la misión y visión corporativa, motiva a los equipos y crea lazos de compromiso, siendo referente de la cultura y valores de la empresa.
- Comunica al directorio sobre los objetivos y logros de la empresa.
- Trabaja en constante colaboración con los c-levels con el fin de alinear la estrategia empresarial para lograr las metas de cada área y mantiene una visión actualizada del negocio.

- Mantiene la sostenibilidad del negocio a largo plazo y se encarga de la relación con potenciales inversionistas.
- Interactúa con potenciales clientes importantes, en caso de ser requerido y facilita la solución de conflictos con clientes actuales.
- Participa en el comité seguridad de la información.
- Informa sobre el desempeño del SGSI.
- Lleva a cabo procesos específicos de seguridad de la información
- Miembro del Comité de Seguridad.

Experiencia técnica requerida

- Título universitário en Administración de empresas, Finanzas, Sistemas o similar.
- Experiencia en puestos directivos o gestión de grandes equipos.
- Conocimientos generales de marketing, ventas, manejo de proyectos y satisfacción al cliente.
- Capacidad para encontrar, relacionar y estructurar información proveniente de diversas fuentes para integrar ideas y conocimientos.
- Capacidad de trabajar en situaciones de falta de información y/o con restricciones temporales y/o de recursos.
- Deseable conocimientos de programación o desarrollo de software.

Competencias específicas

- Liderazgo y dirección de equipos de trabajo.
- Visión estratégica.
- Comunicación eficaz.
- Eficacia en la toma de decisiones.
- Innovación, iniciativa y capacidad resolutiva.
- Razonamiento crítico, lógico y matemático.

Aprobación del perfil

Este rol es aprobado por los accionistas.

3.2 CTO - Departamento de Infraestructura y Seguridad

Objetivos del puesto

El objetivo del cargo es liderar y desarrollar la estrategia tecnológica de la organización, asegurando que la infraestructura, los sistemas y los servicios operen de manera eficiente, segura y escalable. Debe garantizar que las soluciones tecnológicas respalden las operaciones diarias y contribuyan al cumplimiento de los objetivos estratégicos de la empresa. Asimismo, es responsable de diseñar, implementar y supervisar el plan integral de seguridad de la información, promoviendo la protección de los activos y la privacidad de los datos. Le corresponde también velar por el cumplimiento normativo, la gestión de riesgos y la aplicación de controles adecuados, fortaleciendo la resiliencia de la organización frente a amenazas tecnológicas.

Responsabilidades

-> Estrategia y liderazgo

- Planificar la estrategia del área de Tecnología en conjunto con el CEO, alineánla a la estrategia comercial y empresarial.
- Definir e implementar planes para acelerar los resultados y la eficiencia del área, asegurando el cumplimiento de objetivos a corto, mediano y largo plazo.
- Coordinar y gestionar equipos de trabajo, fomentando la colaboración interáreas y generando valor agregado al negocio.
- Definir perfiles profesionales y puestos de trabajo en conjunto con Recursos Humanos, contribuyendo al crecimiento y desarrollo del equipo.
- Impulsar la cultura de seguridad, de alto rendimiento y de mejora continua, estableciendo estándares de trabajo claros.
- Gestionar el presupuesto del área y de infraestructura, optimizando recursos y controlando gastos.

-> Gestión de infraestructura tecnológica

- Planificar, diseñar, implementar y mantener la infraestructura de TI (redes, servidores, almacenamiento, sistemas operativos).
- Supervisar su rendimiento, disponibilidad y seguridad, implementando medidas de protección frente a amenazas y vulnerabilidades.
- Coordinar y ejecutar proyectos de infraestructura, desde la planificación hasta el despliegue.
- Documentar la infraestructura y procesos asociados, manteniendo registros actualizados.
- Evaluar, seleccionar e implementar nuevas tecnologías, incluyendo pruebas y análisis de viabilidad.

- Liderar y desarrollar al equipo de infraestructura, asignando tareas, dando retroalimentación y promoviendo el crecimiento profesional.

-> Seguridad de la información y cumplimiento normativo

- Definir, implementar y mejorar la misión, estrategia y programa de seguridad de la información de la empresa, garantizando su eficacia y mejora continua.
- Administrar y actualizar políticas, normas y procedimientos de seguridad de la información.
- Identificar, evaluar y analizar riesgos de seguridad de la información considerando amenazas, vulnerabilidades e impactos potenciales.
- Desarrollar e implementar estrategias de tratamiento de riesgos (mitigación, transferencia, aceptación o evitación), y dar seguimiento a su ejecución.
- Revisar y mejorar metodologías, procesos y procedimientos de evaluación de riesgos y cumplimiento.
- Realizar evaluaciones periódicas de cumplimiento de políticas, normas y controles internos, incluyendo preparación para auditorías externas (ISO 27001, entre otras).
- Elaborar, actualizar y probar el Plan de Recuperación ante Desastres (DRP), definiendo objetivos de RTO y RPO.
- Definir y supervisar arquitecturas seguras y el endurecimiento de aplicaciones SaaS en nubes públicas.
- Planificar y hacer seguimiento de pruebas de control de seguridad ejecutadas por colaboradores o terceros.
- Estructurar y coordinar equipos/células de respuesta a incidentes de ciberseguridad y de análisis de vulnerabilidades.
- Promover la concienciación y capacitación en seguridad de la información en toda la organización.
- Apoyar la revisión de procesos para garantizar que cumplen con obligaciones regulatorias e internas vigentes.

-> Gobernanza y comunicación

- Generar y analizar reportes sobre riesgos, desempeño del SGSI y estado de seguridad de la información, presentándolos periódicamente a la Dirección.
- Participar activamente en el comité de seguridad de la información.
- Apoyar la evaluación, implementación y mejora de iniciativas de mitigación de riesgos y controles de seguridad.
- Actuar como Delegado de Protección de Datos, asegurando el cumplimiento de la normativa aplicable y atendiendo requerimientos en esta materia.

Experiencia técnica requerida

- Título universitario en Ingeniería en Computación, Ingeniería en Sistemas, Ingeniería en Informática o carrera afín.
- Deseable: estudios de posgrado y/o certificaciones en seguridad de la información (ISO 27001, NIST) o infraestructura (ej. CCNA, CCNP).

- Experiencia en la gestión de proyectos y equipos tecnológicos.
- Experiencia en desarrollo de software y conocimiento de metodologías de gestión de proyectos.
- Experiencia en la administración de infraestructura de TI (redes, servidores, almacenamiento, virtualización, sistemas operativos Windows y Linux).
- Experiencia en la implementación y gestión de soluciones de seguridad (firewalls, WAF, IDS/IPS, SIEM, análisis de vulnerabilidades, PenTests).
- Experiencia en gestión de infraestructura en la nube (AWS, Azure o GCP).
- Amplio conocimiento de arquitecturas y topologías de infraestructura, comunicación y desarrollo de software.
- Conocimiento de estándares y normas de seguridad de la información (ISO/IEC 27001, ISO/IEC 27002, NIST).
- Manejo de herramientas de monitoreo y gestión de infraestructura.
- Conocimiento de soluciones y mejores prácticas de seguridad de la información y gestión de riesgos.

Competencias específicas

- Capacidad analítica, proactividad y orientación a resultados.
- Liderazgo y habilidad para coordinar equipos multidisciplinarios.
- Visión estratégica y capacidad de alinear tecnología con objetivos de negocio.
- Comunicación eficaz con equipos técnicos y no técnicos.
- Resolución de problemas complejos de infraestructura.
- Capacidad de planificación y organización de proyectos.
- Pensamiento analítico y capacidad para evaluar riesgos y tomar decisiones.
- Proactividad e iniciativa en la identificación y solución de problemas.

Aprobación del perfil

Este rol es aprobado por el CEO.

3.3 CFO – Departamento de finanzas

Objetivos del puesto

Es el encargado de establecer y mantener un marco excelente de controles internos, cumplimiento de regulaciones legales locales y extranjeras y prevención de fraude. Liderando de forma adecuada y responsable el departamento de administración y finanzas, actuando de forma proactiva para la mejora continua de los procesos propios del área.
Además, es el encargado de desarrollar e implementar estrategias e iniciativas de HR alineadas con la estrategia comercial general de la empresa, además de contribuir al desarrollo de metas y objetivos.

Responsabilidades

-> Gestión financiera y administrativa

- Controlar y gestionar activos, recursos y gastos generales (oficina, insumos, materiales, arriendos, etc.).
- Supervisar las funciones de tesorería, cobranzas y adquisiciones, incluyendo contrataciones de bienes, servicios, asesorías y consultorías.
- Relacionarse con entidades bancarias y gestionar la apertura y administración de cuentas.
- Definir y aplicar políticas de liquidez, inversión y cobertura financiera.
- Proveer información financiera y contable confiable y oportuna, asegurando el cumplimiento de la regulación vigente.
- Elaborar y supervisar el presupuesto general de la compañía.
- Establecer políticas, procedimientos y controles internos relacionados con su gestión.
- Promover e implementar mecanismos de control sobre los procesos con clientes internos y externos.
- Establecer y analizar indicadores de gestión, definiendo estrategias de mejora alineadas a las mejores prácticas de la industria.

-> Gestión de Recursos Humanos

- Desarrollar e implementar políticas, procedimientos y procesos de Recursos Humanos.
- Planificar, controlar y ejecutar acciones de personal (promociones, traslados, vacaciones, liquidaciones, incapacidades, terminaciones, etc.).
- Mantener y actualizar descripciones de puestos y perfiles de acuerdo con la estructura organizacional.
- Administrar el sistema de compensación y beneficios (escalas salariales, aumentos, beneficios), asegurando competitividad con el mercado.
- Brindar asesoría a la Gerencia General y Directores en temas de relaciones laborales, acciones disciplinarias y mejores prácticas de RRHH.
- Representar a la empresa ante autoridades laborales y asegurar el cumplimiento de las disposiciones legales en materia laboral, tanto a nivel nacional como en países donde la compañía opere.
- Apoyar y orientar al personal en la identificación, prevención y resolución de conflictos laborales para favorecer un buen clima de trabajo y el desempeño efectivo.

-> Cumplimiento y comités

- Asegurar el cumplimiento de disposiciones legales, fiscales, financieras y laborales aplicables.
- Ser miembro del Comité de Seguridad de la Información, aportando desde la perspectiva financiera y administrativa.

Experiencia técnica requerida

- Título universitario en Contaduría, Ingeniería Comercial, Ingeniería Civil Industrial o carrera afín.
- Deseable: MBA o estudios de posgrado en administración financiera o gestión de personas.
- Mínimo 5 años de experiencia en cargos similares de gestión financiera y administrativa.
- Experiencia en control presupuestario, finanzas y contabilidad, con sólidos conocimientos en normativa legal y auditoría.
- Experiencia en la gestión integral de Recursos Humanos: contratación nacional e internacional, gestión de personal, desarrollo organizacional, cálculo de remuneraciones y cotizaciones previsionales.
- Conocimiento profundo de normativa legal vigente en materia financiera, contable y laboral.
- Conocimiento en procesos de administración de compensaciones, beneficios y desarrollo organizacional.
- Deseable: certificaciones en liquidación y cálculo de remuneraciones y en dirección estratégica de personas.
- Deseable: dominio de inglés.

Competencias específicas

- Liderazgo.
- Empatía.
- Trabajo con equipos multidisciplinarios.
- Buen nivel de comunicación.

- Una excelente capacidad de organización.
- Debe poder trabajar de forma autónoma y mantener la calma bajo presión.
- Experiencia demostrable con métricas de Recursos Humanos.
- Capacidad para diseñar estrategias junto con habilidades de liderazgo.
- Cuenta con excelentes habilidades de escucha activa, negociación y presentación.
- Competencia para construir y gestionar eficazmente las relaciones interpersonales en todos los niveles de la empresa.
- Conocimiento profundo de la legislación laboral y mejores prácticas de Recursos Humanos.
- Conocimiento global para el cálculo de remuneraciones.

Aprobación del perfil

Este rol es aprobado por el CEO

3.4 COO - Departamento de operaciones

Objetivos del puesto

Supervisar las operaciones diarias de la empresa, garantizando que los procesos críticos del negocio se ejecuten eficientemente y en conformidad con los lineamientos estratégicos. Asegurar que las operaciones estén alineadas con los objetivos del Sistema de Gestión de Seguridad de la Información (SGSI), promoviendo una cultura organizacional orientada a la seguridad de la información.

Responsabilidades

- Asegurar la implementación de políticas, procedimientos y controles operativos alineados con el SGSI.
- Garantizar la continuidad operativa en situaciones de crisis o incidentes relacionados con la seguridad de la información.
- Supervisar que los procesos operativos cumplan con los requisitos legales, normativos y contractuales vinculados a la seguridad de la información.
- Promover la capacitación y concientización en seguridad de la información dentro de las áreas operativas.
- Velar por la adecuada asignación de recursos para el cumplimiento de objetivos del SGSI.
- Participar en la identificación, análisis y tratamiento de riesgos operativos vinculados a la seguridad de la información.
- Alinear la estrategia operativa con los requerimientos definidos por el Comité de Seguridad de la Información o autoridad equivalente.

Experiencia técnica requerida

- Conocimiento en gestión de procesos, continuidad del negocio y gestión de riesgos operacionales.
- Familiaridad con normas como ISO/IEC 27001, ISO 27018 y otras relacionadas a la seguridad de la información y protección de datos.
- Deseable experiencia previa en participación o implementación de un SGSI.

Competencias específicas

- Buen nivel de comunicación.
- Visión estratégica con foco en la eficiencia operativa y la seguridad.
- Liderazgo y habilidades para gestionar equipos interdisciplinarios.
- Capacidad para la toma de decisiones basadas en riesgos.
- Alta orientación a resultados y cumplimiento de objetivos.
- Compromiso con la mejora continua y la cultura de seguridad de la información.

Aprobación del perfil

Este rol es aprobado por el CEO

3.5 Head of Software Development

Objetivos del puesto

Dirigir y coordinar los equipos de desarrollo de software, asegurando la entrega de soluciones tecnológicas alineadas con los objetivos del negocio y los estándares de calidad y seguridad definidos por la organización. Integrar prácticas seguras de desarrollo en todas las etapas del ciclo de vida del software, en cumplimiento con el SGSI.

Responsabilidades

- Supervisar el desarrollo e implementación de soluciones tecnológicas seguras.
- Garantizar la aplicación de prácticas de desarrollo seguro (secure coding) y revisión de código en todo el equipo.
- Coordinar con el Responsable de Seguridad de la Información la identificación y mitigación de vulnerabilidades en productos desarrollados.
- Asegurar que los desarrollos cumplan con normativas y políticas internas de seguridad de la información.
- Participar en la definición de requisitos de seguridad desde las etapas de análisis y diseño.
- Impulsar la capacitación continua del equipo en prácticas seguras de desarrollo.

Experiencia técnica requerida

- Título universitario o estudiante en Ingeniería en Sistemas, Ingeniería en Computación, Ingeniería de Software o carrera afín.
- Deseable: estudios de posgrado o certificaciones en gestión de proyectos ágiles, arquitectura de software o seguridad de aplicaciones.
- Sólido conocimiento en arquitectura de software, metodologías ágiles y control de versiones.
- Experiencia práctica en implementación de controles de seguridad en entornos de desarrollo.
- Experiencia en herramientas de análisis estático/dinámico de código, gestión de dependencias y CI/CD con foco en seguridad.

Competencias específicas

- Liderazgo técnico y habilidades de gestión de equipos multidisciplinarios.
- Mentalidad orientada a la calidad, eficiencia y seguridad.

- Capacidad para identificar riesgos técnicos y de seguridad en los desarrollos.
- Comunicación efectiva con áreas técnicas y no técnicas.
- Foco en la innovación responsable y mejora continua de procesos de desarrollo.

Aprobación del perfil

Este rol es aprobado por el CEO y COO

3.6 Software Developer

Objetivos del puesto

Desarrollar, mantener y optimizar aplicaciones y servicios de software que respondan a los requerimientos funcionales y no funcionales definidos, asegurando el cumplimiento de estándares de calidad y seguridad establecidos por la organización. Participar activamente en la implementación de prácticas de desarrollo seguro, en línea con los lineamientos del SGSI.

Responsabilidades

- Desarrollar soluciones de software que cumplan con los requerimientos técnicos, funcionales y de seguridad establecidos.
- Aplicar buenas prácticas de desarrollo seguro (secure coding) en todo el ciclo de vida del software.
- Colaborar en la identificación, reporte y corrección de vulnerabilidades detectadas en el código.
- Participar en revisiones de código, pruebas de seguridad y validaciones técnicas.
- Seguir los procedimientos definidos por el área de desarrollo y las políticas del SGSI.
- Mantenerse actualizado sobre amenazas comunes de seguridad (ej. OWASP Top 10) y aplicar medidas preventivas.
- Documentar adecuadamente el código y los cambios realizados, incluyendo aspectos relacionados con la seguridad.
- Proponer mejoras continuas en las soluciones y procesos con foco en calidad y seguridad.

Experiencia técnica requerida

- Título universitario o estudiante en Ingeniería en Sistemas, Ingeniería en Computación, Ingeniería de Software o carrera afín.
- Experiencia en desarrollo de aplicaciones en uno o más lenguajes de programación (ej. PHP, Python, JavaScript, SQL Server, etc.).
- Conocimiento básico o intermedio en conceptos de desarrollo seguro.

- Experiencia trabajando con frameworks y herramientas de control de versiones (ej. Laravel, Git).
- Deseable experiencia en entornos regulados o con altos requerimientos de seguridad.

Competencias específicas

- Atención al detalle y orientación a la calidad del código.
- Capacidad de análisis y resolución de problemas.
- Compromiso con la mejora continua y con la seguridad de la información.
- Buena comunicación y disposición para el trabajo en equipo.
- Capacidad para recibir feedback técnico y adaptarse a estándares definidos.

Aprobación del perfil

Este rol es aprobado por el CTO y Head of Software Development

3.7 Usuarios del sistema

Objetivo del puesto

Utilizar los sistemas de la organización de manera responsable y segura, contribuyendo a la confidencialidad, integridad y disponibilidad de la información.

Responsabilidades

- Utilizar los sistemas de la organización de acuerdo con las políticas, normas y procedimientos establecidos.
- Proteger sus credenciales de acceso, evitando compartir contraseñas o dejar sesiones abiertas sin supervisión.
- Reportar de inmediato cualquier incidente de seguridad, anomalía o sospecha de vulnerabilidad detectada en los sistemas.
- Cumplir con las políticas de uso aceptable de la información y de los recursos tecnológicos.
- Asegurar la confidencialidad, integridad y disponibilidad de la información a la que tienen acceso en el marco de sus funciones.
- Respetar las disposiciones legales y regulatorias relacionadas con la protección de datos y el uso de la información.

Requisitos

- Conocimiento básico de los sistemas y herramientas utilizados en la organización (se provee mediante capacitación interna).
- Responsabilidad en el manejo de información sensible o confidencial.
- Compromiso con el cumplimiento de políticas de seguridad y protección de datos.

3.8 Dueño de Activos

Objetivo del puesto

Custodiar los activos de información bajo su responsabilidad, garantizando su adecuada protección, uso y disponibilidad a lo largo de su ciclo de vida.

Responsabilidades

- Identificar y clasificar los activos de información bajo su responsabilidad (ej. aplicaciones, bases de datos, documentos, infraestructura).
- Definir y autorizar los niveles de acceso a dichos activos, asegurando que solo los usuarios autorizados los utilicen.
- Garantizar que se implementen controles de seguridad adecuados para proteger los activos frente a riesgos.
- Revisar periódicamente la vigencia y pertinencia de los accesos y permisos otorgados.
- Coordinar con las áreas de TI e Infraestructura y Seguridad la implementación de medidas de protección y continuidad para los activos críticos.
- Reportar cualquier incidente o brecha que afecte a los activos bajo su custodia.
- Asegurar que el ciclo de vida de los activos (alta, modificación, baja) se gestione conforme a las políticas de la organización.

Requisitos

- Conocimiento general de los activos bajo su responsabilidad y del valor que representan para la organización.
- Comprensión básica de los riesgos asociados al uso, manejo y protección de los activos.
- Compromiso con las políticas y procedimientos de seguridad de la información.

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 - Descriptivo de roles y responsabilidades.pdf - 16/9/25, 12:51
ESTADO	Firmado
MARCA DE TIEMPO DEL ESTADO	2025/09/16 17:39:56 UTC

Actividad

ENVIADA	natalia.queija@fidelitas.com.ar **ha enviado** una solicitud de firma a: • Jorge El Idd (jorge.elidd@fidelitas.com.ar) • Félix El Idd (felix@fidelitas.com.ar) • Natalia Queija (natalia.queija@fidelitas.com.ar) • Alejandro Burgol (alejandro.burgol@fidelitas.com.ar)	2025/09/16 15:51:55 UTC
FIRMADO	**Firmado** por Natalia Queija (natalia.queija@fidelitas.com.ar)	2025/09/16 17:39:56 UTC
FIRMADO	**Firmado** por Jorge El Idd (jorge.elidd@fidelitas.com.ar)	2025/09/16 17:00:47 UTC
FIRMADO	**Firmado** por Félix El Idd (felix@fidelitas.com.ar)	2025/09/16 16:54:50 UTC
FIRMADO	**Firmado** por Alejandro Burgol (alejandro.burgol@fidelitas.com.ar)	2025/09/16 17:20:18 UTC
COMPLETADO	Todos los firmantes han firmado este documento y ya se ha **completado**	2025/09/16 17:39:56 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.