UNIVERSIDAD NACIONAL DE ROSARIO
FACULTAD DE CIENCIAS ECONÓMICAS Y ESTADÍSTICAS

CARRERA DE POSGRADO
ESPECIALIZACIÓN EN GESTIÓN ESTRATÉGICA DE LA TECNOLOGÍA INFORMÁTICA

Tema: *Análisis de Brecha de Seguridad de la Información en una Empresa de Desarrollo de Software de Gestión Ubicada en España*

Autora: Lic. Ilse Maria Itati Tomasini

Director: Mg. Esp. Marcelo García

2026

Resumen Ejecutivo

La información y los activos digitales de una organización representan un recurso crítico que ante un incidente de seguridad de la información pueden verse afectados en su confidencialidad, integridad o disponibilidad, ocasionando pérdidas operativas, sanciones legales y daños reputacionales. En este contexto, la implementación de un Sistema de Gestión de Seguridad de la Información (SGSI) bajo los lineamientos de la norma ISO/IEC 27001 se convierte en un componente estratégico para garantizar la continuidad del negocio, reducir el riesgo comercial y generar confianza en clientes y partes interesadas.

El presente trabajo tiene como objetivo analizar la madurez actual en materia de seguridad de la información de una empresa de *software* ubicada en Madrid, España, especializada en el desarrollo e implementación de soluciones ERP. A partir de un estudio descriptivo y explicativo que incluye revisión documental, encuestas al personal y entrevistas con la Dirección, se examina el estado real de sus prácticas de seguridad, identificando brechas frente a los requisitos exigidos por ISO/IEC 27001.

El análisis evidenció que la organización no cuenta aún con un SGSI formal, ni con políticas centralizadas, roles definidos de seguridad o procedimientos estandarizados. La gestión de riesgos se desarrolla de manera reactiva e intuitiva, y la capacitación en seguridad es escasa y voluntaria. Si bien algunas áreas aplican buenas prácticas técnicas, principalmente la anonimización de bases de datos, el panorama general muestra una falta de concientización transversal y una ausencia de gobernanza en torno a la seguridad. Esta situación expone a la empresa a riesgos relevantes tanto operativos como regulatorios, especialmente considerando el marco del GDPR.

Para comprender el alcance de la brecha, realizamos un análisis comparativo punto por punto contra los siete capítulos principales de la ISO/IEC 27001, incluyendo contexto organizacional, liderazgo, planificación, soporte, operación, evaluación del desempeño y mejora continua. Asimismo, llevamos a cabo un análisis FODA que permitió identificar fortalezas, debilidades y oportunidades claras para la construcción de una cultura de seguridad sostenible. A partir de estos hallazgos, desarrollamos un plan de acción detallado que prioriza la definición del alcance del SGSI, la elaboración de políticas, la creación de una metodología de análisis y tratamiento de riesgos, la estandarización de procedimientos, la formalización de roles y responsabilidades, y la implementación de un programa anual de capacitación obligatoria.

Finalmente, proponemos un *roadmap* que permitiría reducir significativamente la brecha actual en un período menor a un año, sin que la certificación inmediata sea el objetivo, sino la mejora sustancial del nivel de seguridad corporativa.

Palabras Clave: Seguridad de la Información, ISO/IEC 27001, Sistema de Gestión de Seguridad de la Información (SGSI), Gestión de Riesgos, Análisis GAP.

Índice

1. Marco Teórico

1.1 Introducción

El objetivo de este capítulo es entender y definir la dimensión teórica, los conceptos de gestión estratégica de la seguridad de la información, para poder gestionar y proteger de manera correcta los activos de la empresa involucrados en esta área.

Después de haber relevado la bibliografía y habiendo hecho un análisis de los marcos de cumplimientos afines, desarrollaremos un cuerpo teórico con los principales conceptos en relación a la SGSI[1].

1.2 Seguridad de la Información

La seguridad de la información (SI) está dedicada a proteger los activos de información contra los accesos no autorizados, las modificaciones o destrucciones, garantizando sus tres propiedades: confidencialidad, integridad y disponibilidad. (International Organization for Standardization (ISO) - International Electrotechnical Commission (IEC) 2022)

- Confidencialidad: es la propiedad de la información, por la que se garantiza que está accesible únicamente a personal autorizado a acceder a dicha información (Incibe 2020). No debemos confundirla con la "privacidad", relacionada con la protección asociada a la identidad de los usuarios y sus actividades.
- Integridad: es la propiedad de la información por la que se garantiza la exactitud de los datos transportados o almacenados, asegurando que no se ha producido su alteración, pérdida o destrucción, ya sea de forma accidental o intencionada por

[1] Sistema de gestión de seguridad de la información

errores de *software*[2] o *hardware*[3] o por condiciones medioambientales. (Incibe 2020)

- Disponibilidad: Se trata de la capacidad de un servicio, un sistema o una información, a ser accesible y utilizable por los usuarios o procesos autorizados cuando éstos lo requieran. (Incibe 2020)

En un contexto globalizado, donde el 95% de las brechas de seguridad de la información se deben a errores humanos o controles insuficientes, la SI es crítica para evitar pérdidas financieras, daños reputacionales y sanciones legales. (Report 2023)

La seguridad de los sistemas de información puede verse comprometida de muchas maneras. La protección de los sistemas por medios técnicos (cortafuegos, sistemas de detección de intrusos, etc.) es necesaria, pero no suficiente por sí misma.

Desde los empleados dentro de la organización hasta los clientes fuera de ella, las personas son engranajes vitales en la rueda de la seguridad de la información, que descansa sobre muchos pilares diferentes.

Cuando grandes cantidades de datos se almacenan en formato electrónico, son vulnerables a muchos tipos de amenazas. A través de las redes de comunicaciones, los sistemas de información de distintos lugares están interconectados.

Es posible acceder a los datos que circulan por las redes, robar datos valiosos durante la transmisión o alterar los datos sin autorización. Los intrusos pueden lanzar ataques de denegación de servicio o *software* malicioso para interrumpir el funcionamiento de los sitios *web*. Quienes son capaces de penetrar en los sistemas corporativos pueden robar, destruir, o alterar datos corporativos almacenados en bases de datos o archivos.

[2] Software: parte lógica de un sistema informático
[3] Hardware: parte física de un sistema informático

Los sistemas funcionan mal si los equipos informáticos se averían, no están configurados correctamente o resultan dañados por un uso indebido o actos delictivos. Los errores de programación, la instalación incorrecta o los cambios no autorizados provocan fallos en el *software* informático. Los cortes de electricidad, inundaciones, incendios u otras catástrofes naturales también pueden perturbar los sistemas informáticos.

Sin una sólida protección, los activos de información podrían perderse, destruirse o caer en las manos equivocadas, revelando importantes secretos comerciales o información que vulnere la intimidad personal.

La portabilidad hace que los *smartphones* y las *tablets* sean fáciles de perder o de robar. Los teléfonos inteligentes comparten las mismas debilidades de seguridad de la información que otros dispositivos de Internet y son vulnerables al *software* malicioso y a la penetración de extraños.

Los *smartphones* que utilizan los empleados de las empresas suelen contener datos confidenciales, como cifras de ventas, nombres de clientes, números de teléfono y direcciones de correo electrónico. Los intrusos también pueden acceder a los sistemas internos de la empresa a través de estos dispositivos. (Laudon y Laudon 2021)

En el contexto organizacional, la protección de la Seguridad de la Información requiere un enfoque sistemático y estructurado, que trascienda las prácticas técnicas aisladas. Esto se puede ver reflejado implementando un Sistema de Gestión de Seguridad de la Información, el cual permite mejorar la gestión de riesgos asociados a los activos de la información.

1.2.1 Activos de la Información

En el glosario de términos de ciberseguridad publicado por el Instituto Nacional de Ciberseguridad del Gobierno de España, se define el término Activo de Información como:

Es cualquier información o sistema relacionado con el tratamiento de la misma que tenga valor para la organización pueden ser procesos de negocio, datos, aplicaciones, equipos informáticos, personal, soportes de información, redes, equipamiento auxiliar o instalaciones. Es susceptible de ser atacado deliberada o accidentalmente con consecuencias para la organización. (Incibe 2020)

Estos activos pueden contener información confidencial sobre los individuos de la empresa como los impuestos, activos financieros, historias médicas y el desempeño laboral. Además contienen información sobre las operaciones corporativas, incluidos los secretos comerciales, desarrollo de nuevos productos, planes y estrategias de marketing. Todos estos activos tienen un valor muy importante y las consecuencias pueden ser devastadoras si se pierden, se modifican o si caen en manos equivocadas. (Laudon y Laudon 2021)

El valor que se le da a los activos, depende de las características del negocio y de las necesidades concretas. Esta valoración va a definir los tipos de controles y las pruebas necesarias para garantizar la seguridad de la información.

En base a todo lo anterior podemos decir que un activo es todo lo que tiene valor para una organización que pueda generar flujos de fondos o equivalentes, necesarias para el funcionamiento normal de los negocios. Es decir, toda la información, o sistema relacionado que su tratamiento posea valor para la organización, por lo que es posible esperar que sea susceptible de ataques intencionales o accidentales, generando consecuencias económicas, legales o reputacionales para la organización.

1.2.2 Vulnerabilidades

Debilidad o fallo de un sistema que puede ser aprovechado con fines maliciosos (normalmente mediante un programa que se denomina *exploit*[4]). Cuando se descubre el desarrollador del *software* o *hardware* lo solucionará publicando una actualización de seguridad del producto. (Incibe 2020)

Los datos digitales son vulnerables a la destrucción, el uso indebido, errores, fraudes y fallos de *hardware* o *software*. Internet es un sistema abierto y hace que los sistemas internos de las organizaciones sean más vulnerables a los ataques externos. (Laudon y Laudon 2021) Cada componente de la arquitectura de una aplicación web presenta vulnerabilidades de seguridad.

Las vulnerabilidades son características de los recursos de información que pueden ser explotadas por una amenaza para causar daño. Los siguientes son ejemplos de vulnerabilidades:

- Falta de conocimiento del usuario
- Falta de funcionalidad de la seguridad
- Educación/concientización del usuario inadecuadas
- Tecnología no probada
- Transmisión de comunicaciones no protegidas

Para que una vulnerabilidad sea reconocida, debe existir una amenaza humana o ambiental para que explote la vulnerabilidad. (ISACA s.f.)

[4] Exploit: método para explotar una falla de seguridad.

1.2.3 Amenazas

Circunstancia desfavorable que puede ocurrir y que cuando sucede tiene consecuencias negativas sobre los activos provocando su indisponibilidad, funcionamiento incorrecto o pérdida de valor. Una amenaza puede tener causas naturales, ser accidental o intencionada. Si esta circunstancia desfavorable acontece a la vez que existe una vulnerabilidad o debilidad de los sistemas o aprovechando su existencia, puede derivar en un incidente de seguridad. (Incibe 2020)

Cuando se almacenan grandes cantidades de información de manera digital y con la dependencia casi total de estos para las actividades operativas y funcionales, las empresas enfrentan numerosas amenazas internas y externas. La vulnerabilidad de la información es reconocida porque existen amenazas humanas o ambientales que las pueden explotar. Los actores de amenazas humanas típicos son: novatos, *hackers*[5], delincuentes, terroristas, sublevaciones o disturbios civiles, inestabilidad política y transiciones. Las amenazas ambientales típicas incluyen las inundaciones, los rayos, tornados, huracanes, terremotos e incendios. (ISACA s.f.)

1.2.4 Riesgos

Según La Real Academia Española, riesgo es la contingencia o proximidad de un daño. Cada una de las contingencias que pueden ser objeto de un contrato seguro.

En el ámbito de la seguridad de la información un riesgo es la posibilidad de que una amenaza explote una vulnerabilidad existente, perjudicando los activos de la información mediante accesos no autorizados modificación, interrupción o destrucción de información o

[5] Hackers: Persona con grandes conocimientos en el manejo de las tecnologías de la información que investiga un sistema informático para reportar fallos de seguridad y desarrollar técnicas que previenen accesos no autorizados. (Incibe 2020)

sistemas de información, lo que puede afectar las operaciones, la reputación o los activos de una organización.

Según el Incibe, es la posibilidad de que una amenaza o vulnerabilidad se convierta en un daño real para la empresa, que resulte en una pérdida o robo de información o en una detención de su actividad como consecuencia del daño ocasionado. El riesgo puede ser mitigado mediante políticas de seguridad de la información y continuidad del negocio que suelen prever posibles ataques y proponen soluciones de actuación ante situaciones cuyo riesgo pueda ser elevado. (Incibe 2020)

1.3 Gobernanza de Seguridad de la Información y Marcos de Cumplimientos

Gobernanza: gestión de las políticas, procesos y decisiones de la empresa. La gobernanza empresarial abarca toda la empresa, con diferentes funciones, cada una de las cuales desempeña un papel en la gestión del riesgo para la empresa.

Debido a su papel destacado en los procesos de gobierno de TI, la gobernanza de la seguridad de la información ha aumentado a uno de los niveles más altos de actividad centrada con impulsores de valor específicos: confidencialidad, integridad, disponibilidad de información, continuidad de servicios y protección de activos de información. (ISACA s.f.)

La seguridad y la gobernanza de la información centralizan la responsabilidad y la planificación en una organización para que siempre haya varias prioridades superpuestas. Estas prioridades son la asignación de recursos, incluyendo financiamiento para tecnología, personal, materiales de capacitación y posiciones ejecutivas relacionadas con el cumplimiento y la seguridad de la información; el cumplimiento, ya sea con estándares de la industria o marcos opcionales según lo determinado por las necesidades organizacionales; la responsabilidad centrada en una jerarquía de gestión que pueda formalizar la toma de decisiones y el desarrollo

de procesos; la implementación de medidas de seguridad de la información avanzadas como gestión de riesgos, prevención proactiva y herramientas como escáneres de vulnerabilidades, pruebas de penetración o Inteligencia Artificial (IA).

La gobernanza y la gestión estratégica de la seguridad de la información son enfoques fundamentales para proteger los activos de información de la empresa, garantizar el cumplimiento normativo y alinearse con los objetivos empresariales.

Combina el liderazgo, la planificación estratégica, la implementación de políticas y el monitoreo constante.

1.3.1 Sistemas de Gestión

Se entiende por Sistema de Gestión la estructura organizada, la planificación de las actividades, las responsabilidades, las prácticas, los procedimientos, los procesos y los recursos para desarrollar, implantar, llevar a cabo, revisar y mantener al día la política de una empresa. En otras palabras, es un método sistemático de control de las actividades, procesos y asuntos relevantes para una organización, que posibilita alcanzar los objetivos previstos y obtener el resultado deseado, a través de la participación e implicación de todos los miembros de la organización, garantizando la satisfacción del cliente, de la sociedad en general y de cualquier parte interesada. (García 2006)

Entre los elementos que conforman un sistema de gestión están los recursos, ya sean las personas, la infraestructura, los equipos, el conocimiento, etc, los métodos de trabajo, la estructura organizativa, las funciones y responsabilidades, los productos y servicios a desarrollar y la documentación asociada. Todos estos elementos interrelacionados crean una estructua que posibilita el desarrollo de un objetivo estratégico determinado.

1.3.1.1 Beneficios a Implementar una Gestión de Gobernanza en la Empresa

Sin importar el objetivo, el sistema de gestión es proporcionar garantías del cumplimiento de políticas, especificaciones y normativas; favorecer la mejora continua; permitir demostrar ante otras instituciones el cumplimiento de los requisitos, mediante la documentación y los registros adecuados.

Organizar los esfuerzos de seguridad de la información y cumplimiento bajo una sola estrategia traerá varios beneficios significativos a una organización más allá de luchas con la seguridad *ad hoc*[6].

Entre los beneficios podemos mencionar la seguridad de la información más efectiva. Una política de gobernanza de seguridad integral y bien definida puede unir los objetivos empresariales y de seguridad de una manera que los enfoques de seguridad desorganizados simplemente no pueden igualar. Los marcos pueden ayudar aún más a las organizaciones a comenzar con enfoques integrales de seguridad que les ayudarán a alcanzar sus objetivos.

La aplicación uniforme de los requisitos de cumplimientos es una parte crítica de hacer negocio en la mayoría de las industrias. La adherencia a las regulaciones es una realidad de todo o nada: si una parte de un sistema no cumple, entonces toda la organización está abierta a sanciones o posibles brechas. Las políticas de gobernanza de seguridad de la información pueden agilizar las prácticas de cumplimiento en sistemas técnicos, administrativos y físicos.

Por último, una vez que los requisitos de seguridad de la información y cumplimiento se movilizan en políticas, se vuelve bastante fácil definir las plataformas adecuadas que la organización debe usar para operaciones empresariales como la gestión de relaciones con clientes, transferencia segura de archivos, gestión de documentos y correo electrónico seguro.

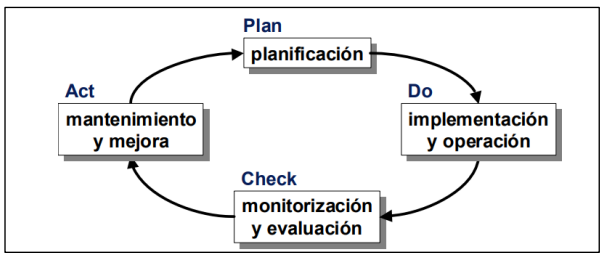
[6] Ad hoc: creado para un fin específico.

1.3.1.2 Sistemas de Gestión de Seguridad de la Información (SGSI)

Un Sistema de Gestión de la Información (SGSI) es un conjunto de políticas de seguridad de la información que siguen la norma ISO/IEC 27001. Un SGSI es para una organización el diseño, implantación, mantenimiento de un conjunto de procesos para gestionar eficientemente la accesibilidad de la información, buscando asegurar la confidencialidad, integridad y disponibilidad de los activos de información minimizando a la vez los riesgos de seguridad de la información. (Incibe 2020)

Se define "sistema de gestión" como lo que la Organización hace para gestionar sus procesos o actividades, de forma que los productos que fabrica o los servicios que presta satisfagan los objetivos que la propia organización que ha marcado.

Dentro del sistema de gestión de una Organización, se entiende por SGSI la parte relacionada con la seguridad de la información. Es habitual entender que los sistemas de gestión deben ajustarse al llamado ciclo de *Deming* (PDCA), habitual en sistemas de gestión de la calidad: *Plan*, se establecen objetivos y se preparan planes para alcanzarlos. Esto incluye analizar la situación de la Organización. Dónde estamos y dónde queremos estar. *Do*, se ejecutan los planes. *Check*, se evalúan los resultados obtenidos para determinar en qué medida se han alcanzado los objetivos propuestos. *Act*, a fin de estar cada día mejor (mejora continua), se actualizan los planes y su implantación.



1 Ciclo PDCA. Fuente: MARGERIT v3.0 página 114

El objetivo del plan debe incluir principalmente tener el riesgo bajo control. Debe incluir una política de seguridad de la información y un análisis de riesgos que modele el valor del sistema y la exposición a amenazas. Básicamente el plan de seguridad de la información debe ser para la gestión de riesgos.

La ejecución del plan debe abarcar los aspectos técnicos y de organización. El centro deben ser las personas que se hacen cargo del sistema o están relacionadas. El éxito se contempla por la operativa diaria sin sorpresas.

La monitorización de la operación del sistema esta fundado en que no se puede tener confianza ciega en las medidas tomadas. Hay que evaluar constantemente que se responda a lo esperado con la eficacia deseada. Hay que medir lo que ocurre como lo que quizás ocurriría si no se hubiera tomado medidas. Además, hay que estar constantemente al tanto de las novedades que surjan de las modificaciones del sistema de información como de las nuevas amenzas.

La reacción es saber actuar en base a la experiencia propia y de sistemas similares, repitiendo el ciclo PDCA.

La evaluación de un sistema de gestión de seguridad de la información parte de las actuaciones de la organización en cuanto a la seguridad y mide la eficacia de los controles implantados para alcanzar los objetivos propuestos.

Por último, mencionar que un sistema de gestión maduro debe estar documentado en todos sus aspectos. Las actividades que se realizan siguiendo normas y procedimientos no deben estar solamente en la cabeza de las personas. Cuando este todo por escrito es que podemos hablar de un sistema de gestión que puede ser objeto de una certificación. (Dirección General de Modernización Administrativa, Procedimientos e Impulso de la Administración Electrónica 2012)

1.4 Compliance

El *compliance*[7], o cumplimiento normativo, es un conjunto de prácticas, normas y procesos que una organización implementa para asegurar que sus actividades se ajusten a las leyes, regulaciones, normas y estándares éticos aplicables a su sector y contexto. Puede ser obligatorio o voluntario. Satisfacción de unos requisitos. Declaración de que se ajusta y es conforme a la normativa correspondiente.

La importancia del compliance corporativo como herramienta fundamental para garantizar el éxito en las empresas a largo plazo, independientemente del sector o del tamaño de la misma.

El compliance reduce riesgos de sanciones, multas, procesos judiciales y pérdida de la reputación, asegurando la estabilidad de la empresa. Transmite confianza a los *stakeholders*[8] demostrando ética y transparencia. Mejora la percepción de la empresa como responsable dentro del mercado y motiva a los empleados a actuar con integridad y responsabilidad en su trabajo diario. Por último, evita errores y costos derivados de los incumplimientos de las normas. (Repsol 2024)

1.4.1 Diferencia entre el Cumplimiento Legal y el Normativo

La principal diferencia entre el cumplimiento legal y normativo tiene que ver con el origen y la obligatoriedad.

Lo legal implica acatar las leyes y regulaciones establecidas por un tercero, ya sea el gobierno o una autoridad competente. Dentro de los ejemplos más conocidos tenemos las leyes laborales, la ley de protección de datos y las regulaciones ambientales.

---

[7] Palabra en inglés. Significa cumplimiento
[8] Clientes, proveedores, empleados e inversores

En cambio, el cumplimiento normativo abarca las leyes y las normas internas de una organización, los códigos de ética, las buenas prácticas, las cuales pueden ser obligatorias o recomendadas. En este caso el ejemplo principal sería las normas ISO, las políticas de la empresa y los códigos de conducta.

1.4.2 Normativas que Afectan a la Compañía

Hay ciertas normativas naciones e internacionales que son relevantes en el caso del análisis y gestión de riesgos, bien por exigirlo, por sustentarlo o por ser de utilidad en el Proceso de Gestión de Riesgos.

En nuestro caso particular y a lo que nos compete desarrollaremos la normativa GDPR en España que se refiere al Reglamento General de Protección de Datos y el estándar internacional que establece los requisitos para un Sistema de Gestión de Seguridad de la Información (SGSI), la norma ISO/IEC 27001.

1.4.2.1 GDPR

A principios del año 2018 se estableció el Reglamento General de Protección de Datos de la Unión Europea para mejorar la protección de datos personales.

Impacta directamente en el almacenamiento, procesamiento, acceso, transferencia y divulgación de los registros de datos de un individuo y afecta a cualquier organización a nivel mundial que procese datos personales de personas de la Unión Europea.

Es un reglamento que tiene la intención de reforzar y unificar la protección de datos para todos los individuos dentro de la Unión Europea. Sustituye a la Directiva de protección de datos (Directiva 95/46 / CE) de 1995

1.4.2.2 ISO/IEC 27001

La seguridad de la información se ha convertido en un pilar estratégico para las organizaciones en la era digital, donde amenazas como ciberataques, fugas de datos y vulnerabilidades tecnológicas exigen marcos de gestión robustos. La norma ISO/IEC 27001, estándar internacional para Sistemas de Gestión de Seguridad de la Información (SGSI), proporciona un enfoque sistemático para proteger los activos críticos bajo los principios de confidencialidad, integridad y disponibilidad. Sin embargo, muchas empresas enfrentan brechas significativas entre sus prácticas actuales y los requisitos de esta norma. Este marco teórico explora los fundamentos de la seguridad de la información, la estructura de la ISO/IEC 27001 y las metodologías para identificar dichas brechas, sentando las bases para analizar el caso de la empresa.

2. Empresa Objeto de Estudio

2.1 Introducción

Teniendo en cuenta la información relevada de la empresa que es objeto de análisis, describiremos en el capítulo sus características principales para comprender su funcionamiento detalladamente y el contexto en el que se encuentra su sistema de gestión de seguridad de la información. Esto nos permitirá establecer una base para identificar fortalezas, debilidades y brechas en relación con las normativas y marcos de cumplimiento vigente. El estudio es de carácter descriptivo y explicativo.

2.2 Presentación de la Empresa

La empresa se encuentra en la ciudad de Madrid, en el centro del país. Es una empresa innovadora especializada en el desarrollo e implementación de soluciones de software de gestión empresarial. Tiene cientos de clientes esparcidos por toda España. Ofrece como solución un ERP dividido en paquetes funcionales para adaptarse a las necesidades de los clientes. Con más de quince años de experiencia y clara vocación de optimizadores de procesos, atienden aquellos factores que hacen peligrar la rentabilidad de las empresas.

Con un tamaño de más de 70 empleados especializados y más de 100 clientes.

Los segmentos objeto de la compañía son las empresas de distribución B2B, *retail* B2C, *e-commerce* y financiero y almacenes logísticos. La mayoría de sus clientes son ampliamente reconocidos y pertenecen al rubro de la moda en sus diferentes áreas, desde ropa interior, deportiva, calzados, gafas, y accesorios. También están dentro del mundo de los deportes con clientes que venden suplementos alimenticios, y artículos deportivos. Además cuentan con

clientes que venden productos alimenticios para mascotas entre muchos otros rubros. (Empresa, Sitio Oficial de la empresa 2025)

2.3 Capital Humano y Organización

La empresa organiza el trabajo en tres tipos de equipos: área funcional (AF), control de proyectos y círculos.

Las áreas funcionales formadas por desarrolladores y consultores, especializadas en distintos ámbitos del ERP. Son seis áreas funcionales actualmente: conectores, transportistas y operadores logísticos, pedidos, almacén, financiero y TPV.

Además, a cargo de la gestión de la empresa están el fundador y director, un responsable financiero, responsables de capital humano, especialistas en marketing, una directora comercial y un técnico de sistemas. (Empresa, Organización Interna 2025)

2 Organización de la empresa en equipos. Fuente: documentación interna de la empresa

Control de proyectos formado por el Gestor Global de Proyectos (GGP), *Functional Development Manager*[9] (FDM), *Launch Manager*[10] (LM) y *Service Manager*[11] (SM), son los

[9] Functional Development Manager: Gerente de desarrollo funcional
[10] Launch Manager: Administrador del arranque
[11] Service Manager: Administrador de servicio

interlocutores entre el cliente y las áreas funcionales. Tienen como misión garantizar la correcta ejecución de todos los proyectos de la empresa, desde el arranque hasta la evolución. Su objetivo es asegurar que cada implantación sea predecible, escalable y rentable, manteniendo siempre la calidad y los plazos comprometidos. Para eso se coordina la planificación de la capacidad, gestiona riesgos transversales, supervisa la metodología y da soporte estratégico a la dirección.

Círculos formados por distintos perfiles, enfocados en canalizar y empujar distintas acciones de mejora interna. En ellos, la toma de decisiones está distribuida quedando claras las reglas explícitas y dando autoridad tanto al círculo como a la persona en el objetivo o el rol desempeñado. (Empresa, Organización Interna 2025)

Círculo *Product*[12]. Este círculo tiene como misión principal garantizar la calidad de nuestro servicio, coordinando todas las labores entorno al mismo con otros círculos relevantes.

Algunas de sus tareas pueden ser la definición, junto a las AF, de nuevos paquetes según necesidades detectadas en cliente o propuestas de manera proactiva. Coordinación, junto a las AF y al círculo de *Devops*, respecto a las diferentes elecciones técnicas y funcionales que se realicen. Intervención en pasos finales de cara a la adopción general de los módulos pertinentes. Junto con *Academy*, la planificación de contenidos, definición de alcance, revisión de material grabado, ayuda, etc.

Círculo *DevOps*[13] vela por la mejora metodológica de desarrollo, tanto a nivel tecnológico como cultural. Cubre todo el ciclo de desarrollo del *software* de manera que los procesos son mucho más ágiles y seguros y de esta manera también se garantiza un producto final de mucha más calidad y fiabilidad.

[12] Product: (Ing) producto.
[13] DevOps: Desarrollo de operaciones

Algunos puntos que puede tratar este círculo son la definición de buenas prácticas de desarrollo; la integración continua de los diferentes desarrollos que se realicen; la gestión de despliegues[14] dentro de nuestros entornos de test y de producción, idealmente de manera automática y continua. La infraestructura como código para permitir despliegues automatizados y gestionar escalados; la automatización de pruebas y la monitorización del rendimiento para mejorar el flujo y reducir impacto en clientes.

Círculo *ProjectOps* se encarga de coordinar, gestionar y ejecutar acciones relacionadas con la mejora de la metodología de implantación de Odoo en los clientes.

Su área de actuación abarca un ámbito meramente de gestión y funcional, y es el círculo de mejora y crecimiento profesional para *service managers* y consultores funcionales. Es un círculo que mejora la escalabilidad de los servicios, marcando pautas claras de implementación. Sus resultados tienen un impacto muy alto en la organización, dado que el beneficio de una buena implementación y gestión del cliente tiene resultados directos en su confianza hacia la empresa.

Círculo *Academy*[15]. Este círculo es para resolver dos problemas recurrentes. Primero, la necesidad de una formación interna continua, donde fluya la información entre todas las personas del equipo interesadas. Segundo, la necesidad de una formación a cliente, también continua, donde se puedan dar diferentes opciones para trasladar contenidos de calidad que les aporten valor.

En un principio, su área de actuación abarca sólo un ámbito funcional, dejando al círculo de *DevOps* la formación técnica. El círculo tiene un carácter continuo y está compuesto por un equipo muy experimentado que ejerce un rol mixto de ejecución y de coordinación,

[14] Despliegue: proceso de instalar, configurar y poner en funcionamiento una aplicación en un entorno.
[15] Academy: academia

dado que tiene que trabajar mano a mano con las diferentes áreas funcionales que serán las encargadas de consolidar diferente material de manera recurrente.

Círculo *Agile Framework*[16] se encarga de coordinar, gestionar y ejecutar diversas acciones relacionadas con la mejora interna de nuestra metodología, marco de trabajo y procesos. Su área de actuación abarca diferentes ámbitos funcionales y técnicos.

Sus resultados tienen un impacto muy alto en la organización, por lo que algunas decisiones tendrán que ser presentadas y/o refinadas por otras personas ajenas a su actividad continua.

Círculo de Responsables Técnicos (RT) encargados de definir las políticas de los despliegues, además de llevarlos a cabo, restaurar las bases de datos y a nivel de seguridad de la información son los encargados de dar accesos a los usuarios internos a los diferentes entornos de los clientes.

2.4 Lineamientos Estratégicos

Para comprender la misión y visión de la empresa, es fundamental conocer sus pilares estratégicos ya que son los lo diferencian de otras empresas similares y marcan las estrategias y los objetivos.

2.4.1 Pilares Estratégicos

Producto tecnológico diferencial. Han desarrollado su propio ERP, aprovechando lo mejor de Odoo, pero con la libertad de construir soluciones únicas y a medida. El propósito es

[16] Agile Framework: metodología flexible para desarrollar proyectos de forma colaborativa y adaptativa.

evolucionar continuamente, fomentar una verdadera cultura de producto y ofrecer una propuesta de valor que destaque por su enfoque en la experiencia del cliente.

Transformación operativa integral en empresas de producto físico. No solo implementan tecnología, transforman los procesos de negocio de sus clientes. Les ayudan a optimizar y mejorar su forma de trabajar, asegurándose de que cada solución entregue resultados tangibles y sostenibles.

Excelencia metodológica. Trabajan bajo una metodología sólida, tanto de cara al cliente como internamente. Con *Kanban* como base, documentan, gestionan el cambio, realizan actualizaciones constantes e involucran al cliente para garantizar una mejora continua.

Formación y transferencia de conocimiento. La meta es que cada cliente sea autónomo. Los forman, les proporcionan las competencias necesarias y diversifican los contenidos formativos para que estén siempre preparados.

Personas que crean valor. Fomentan relaciones a largo plazo basadas en la confianza y la cercanía. Cuentan con un equipo experimentado que anticipa necesidades y trabaja con una visión estratégica para fortalecer cada vínculo con nuestros clientes.

2.4.1.1 Misión

Transformar las empresas de producto físico para la excelencia operativa, combinando la experiencia de más de 15 años con tecnología ERP moderna y una metodología ágil. Empoderando a sus clientes para que dominen sus procesos, optimicen su gestión y evolucionen de manera sostenible en la era digital. (Empresa, Sitio Oficial de la empresa 2025)

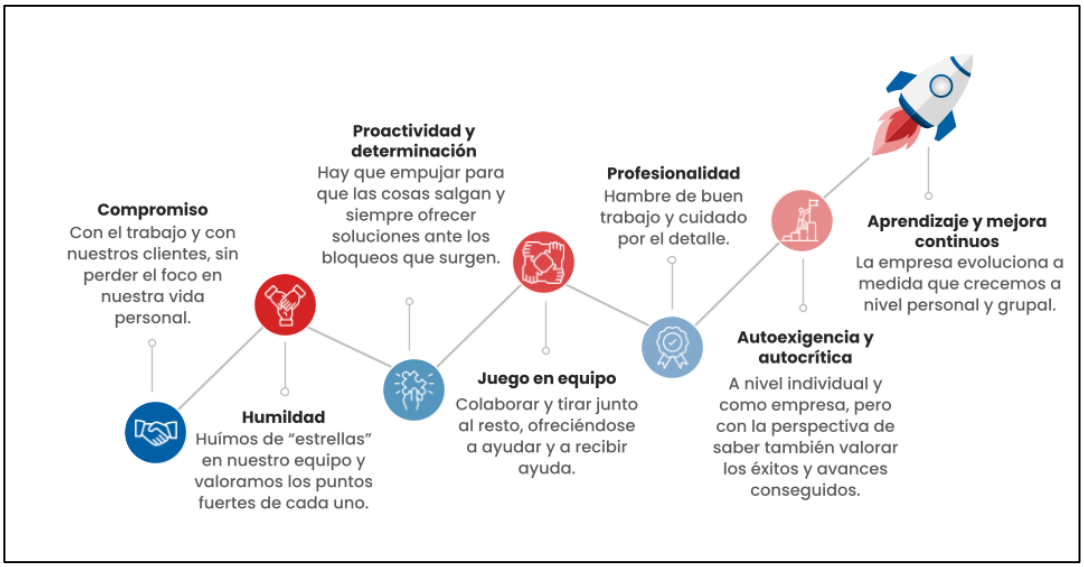
2.4.1.2 Visión

Ser el socio tecnológico estratégico líder en la transformación integral de empresas de producto físico a nivel global, reconocidos por el producto propio diferencial, la excelencia metodológica y un equipo de personas que crean valor, anticipándose a los retos y generando un impacto duradero en cada cliente. (Empresa, Sitio Oficial de la empresa 2025)

2.4.1.3 Valores

A continuación describiremos los siete valores principales con los que la empresa se identifica y que trata de fomentar a todos sus actuales y futuros colaboradores.

Comenzando por el compromiso con el trabajo y sus clientes, sin perder el foco en la vida personal de cada uno. Valorando el juego en equipo, colaborando y tirando junto al resto, ofreciéndose a ayudar y a recibir ayuda. Profesionalidad, con hambre de buen trabajo y cuidado por el detalle. Humildad, huyendo de las estrellas en los equipos y valorando los puntos fuertes de cada uno. Trabajando con proactividad y determinación para empujar para que las cosas salgan y siempre ofrezcan soluciones ante los bloqueos que surgen. Con autoexigencia y autocrítica a nivel individual y como empresa, pero con la perspectiva de saber también valorar los éxitos y avances conseguidos. La empresa evoluciona a medida que crecen a nivel personal y grupal, enfatizando el aprendizaje y la mejora continua. (Empresa, Sitio Oficial de la empresa 2025)



3 Valores de la empresa Fuente: sitio oficial de la empresa

Para cada valor existen una serie de comportamientos que se esperan de las personas del equipo día a día.

Compromiso. Involucrándose activamente en las actividades y dinámicas del equipo; aportando ideas y soluciones en reuniones; ofreciéndose a colaborar en tareas más allá del rol formal; defendiendo las decisiones de equipo o empresa; esforzándose por alinear las acciones con los objetivos estratégicos de la organización.

Humildad. Escuchando activamente sin interrumpir ni intentar de imponer las ideas propias; reconociendo los errores sin justificarse; agradeciendo y valorando el *feedback*, aunque no siempre sea como el esperado; tratando a todos con respeto, sin importar jerarquías o niveles; aceptando que no siempre se saben todas las respuestas y abriéndose a aprender de otros.

Proactividad y determinación. Insistiendo y perseverando cuando los proyectos se complican; tomando la iniciativa sin esperar indicaciones; anticipándose a los posibles

problemas y actuando para prevenirlos; asumiendo responsabilidades incluso cuando el contexto es incierto; reaccionando con agilidad y efectividad en momentos de presión.

Juego en equipo. Generar un ambiente de confianza y respeto mutuo; compartiendo recursos, conocimientos y experiencias sin necesidad de solicitarlo; apoyando a los compañeros cuando lo necesitan; facilitando acuerdos cuando surgen desacuerdos; celebrando los logros del equipo como si fueran propios.

Profesionalidad. Entregando el trabajo a tiempo, incluso bajo presión; revisando cuidadosamente lo que se entrega para garantizar la calidad; cumplir con lo prometido, incluso si requiere esfuerzo adicional; esforzándose por ser confiable y mantener la palabra dada; cuidando la imagen profesional en todos los contextos (internos y con clientes)

Autoexigencia y autocrítica. Fijándose metas retadoras, no conformándose con lo mínimo; esforzándose por mejorar lo que ya se hace bien; analizando los resultados del trabajo para detectar oportunidades de mejora; no utilizando excusas cuando algo no sale como se espera; buscando formas más eficientes y efectivas de hacer las cosas.

Aprendizaje y mejora continua. Buscando oportunidades de formación, incluso si no son obligatorias; reflexionando sobre lo aprendido y cómo aplicarlo en el día a día; manteniendo al tanto de novedades que puedan mejorar el trabajo; pidiendo *feedback* para mejorar, no solo para recibir reconocimiento; transformando los errores en aprendizajes concretos.

En este último tiempo se agregó a los siete valores uno más relacionado con el uso de la IA, fomentando la exploración de herramientas de IA para entender las posibilidades en el entorno de trabajo, aplicar herramientas de IA para automatizar o mejorar los aspectos del trabajo, esforzándose por integrar la IA en procesos habituales de forma responsable,

compartiendo con el equipo recursos, ideas o buenas prácticas sobre la IA y por último, reflexionando sobre el impacto ético, profesional y estratégico del uso de la IA.

2.4.1.4 Propuesta de Valor para los Empleados

Además la empresa tiene propuestas de valor hacia los empleados invirtiendo en ellos con formación y desarrollo profesional sin límites, manteniendo el equilibrio de la vida personal y profesional como prioridad. Con compensaciones y beneficios para valorar la dedicación.

En la empresa tienen el concepto de "barra libre" de formación, tanto interna como externa, creando planes de formación a medida. Internamente cuentan con *Academy*, su plataforma de *e-learning* para la formación de Odoo; programa de *mentoring* y comunidades de prácticas y semanas temáticas enfocadas al impulso del aprendizaje del equipo. Externamente cuentan con clases individuales de inglés, formación técnica en *Python* y *JavaScript*, cursos de habilidades (liderazgo, comunicación, gestión de proyectos, etc.), programa de *coaching* y membresía en distintas plataformas de formación. Además, como socios de la AEOdoo y contribuidores de la OCA, participan en las jornadas anuales y los OCA *Days* y facilitan la obtención de la Certificación técnica de la AEOdoo. (Empresa, Sitio Oficial de la empresa 2025)

2.4.2 Estrategias Empresariales

Cada trimestre la empresa organiza jornadas internas con un objetivo principal y varios objetivos secundarios cruciales, todos orientados a la mejora continua y la alineación estratégica de la empresa. A continuación presentaremos los objetivos principales, los

secundarios y las estrategias claves, organizadas por pilares, extraídas de las notas tomadas en la última jornada de Septiembre 2025.

2.4.2.1 Objetivo Principal de las Jornadas: Alinear y Revisar la Estrategia Integral

El propósito central es asegurar que todo el equipo, desde la dirección hasta los círculos operativos, estén completamente alineados con la estrategia general de la empresa, los pilares definidos y los retos del año. Estas jornadas permiten revisar el progreso del trimestre anterior, identificar desviaciones y ajustar el rumbo para el siguiente periodo.

2.4.2.2 Objetivos Secundarios Claves de las Jornadas

Revisión de logros y desafíos. Se celebran los éxitos y se analizan los objetivos no alcanzados del trimestre, permitiendo aprender de las experiencias menos exitosas e imitando las logradas.

Transparencia y visibilidad general. Las jornadas ofrecen una visión global del estado de la empresa. Se ven estadísticas generales como cifras de facturación, número de profesionales empleados, antigüedad, demografía, etc.

Se comparten los informes de los círculos de Dirección y los Operativos. Cada área presenta sus objetivos, logros, novedades, *KPIs* y retos para el próximo trimestre, proporcionando visibilidad a todos los equipos sobre el trabajo de los demás.

Definición y ajuste de retos trimestrales. Se establecen o reajustan los retos y objetivos específicos para cada área de cara al siguiente trimestre, asegurando que estén alineados con la estrategia global.

Fomento de la cultura de producto y metodología. Se refuerza la "mentalidad de producto" sobre la "mentalidad de consultoría a medida", impulsando la evolución del ERP y la implementación efectiva de la metodología *Agile Pack*.

Desarrollo y empoderamiento de los equipos a través de la presentación de temas de Capital Humano, formación y la discusión de roles (SM/SMA). Se busca potenciar el talento, el crecimiento profesional y el liderazgo, fortaleciendo la cultura de colaboración.

Transferencia de conocimiento e ideas. Es un espacio para compartir novedades, mejores prácticas y explorar nuevas iniciativas (como la IA aplicada), generando un ambiente de aprendizaje colectivo.

Al reunir a toda la organización, estas jornadas fortalecen el sentido de pertenencia y la colaboración entre las diferentes áreas y personas.

En resumen, las jornadas trimestrales son el pulso estratégico de la empresa, diseñadas para mantener a toda la organización en la misma página, adaptarse rápidamente, impulsar la excelencia y construir el futuro de la empresa de manera conjunta y consciente.

2.4.2.3 Estrategias Claves

En las jornadas se definen las estrategias claves de los principales pilares de la empresa que delinearan las actividades, la planificación y los trabajos de los próximos trimestres. Veremos que muchas veces se combinan las áreas y los círculos para los objetivos en común.

Dentro de las estrategias técnicas, los mayores involucrados son los círculos de *DevOps* y RT. Se planifica que en los próximos trimestres se migrarán los sistemas internos a versiones más actuales de Odoo, adaptando el ERP a la metodología de la empresa. De la mano con lo

anteriormente mencionado se fomentará el uso de las funcionalidades del ERP internamente para identificar mejoras y aprovechar los beneficios del propio producto.

Otro punto importante en donde el área de DevOps está involucrada es en el uso de la IA. Actualmente la empresa utiliza la IA como una herramienta en el día a día tanto a nivel funcional como técnico para optimizar la generación y gestión de documentación, para la generación de actas de reunión, para construir, mantener y mejorar la arquitectura de sistemas.

Lo que se busca de cara al futuro es desarrollar un Modelo Mínimo Funcional Completo (MPC) interno para facilitar la obtención de información y ahorrar tiempo. La exploración de procesadores de lenguaje locales de IA para mejorar la seguridad de datos y no comprometer la información empresarial.

Para prevenir incidencias y tener una trazabilidad de las mismas en el ERP, se quiere desarrollar sistemas de agentes aplicados al ERP y establecer un *backlog* para priorizar su gestión. Hoy se está utilizando un centro de incidencias con IA, el *Sentry*, el cual evalúa las incidencias y le asigna de responsable, dependiendo de cuál sea el área afectada.

Desde RT van a implementar pruebas globales de reléase para detectar errores críticos antes del lanzamiento. Se va a mejorar de la robustez en actualizaciones de módulos y despliegues de test.

A nivel seguridad de la información se determinó implementar un sistema de *fingerprinting*[17] para recopilar información detallada sobre los logueos[18] del correo empresarial y del correo instantáneo utilizado (Slack).

Por último, se definió la utilización de SaltStack para la automatización de *scripts* y mantenimiento remoto del *hardware* corporativo. Está herramienta se destaca por su velocidad,

[17] Fingerprinting: huella digital
[18] Logueo: acción de ingresar a un sistema utilizando un usuario y contraseña

escalabilidad y por permitir tanto ejecución remota como gestión basada en estados. A nivel seguridad de la información está herramienta no solo asegura la propagación automatizada de las configuraciones, sino que también puede reaccionar ante acontecimientos, ya que registra qué tipo de comunicación se intercambia en la infraestructura. (Ionos Digital Guide 2023)

A nivel funcional se abordará una transformación operativa orientada a la excelencia metodológica. Será un gran cambio organizativo con la introducción de nuevos roles (*Launch Manager* y *Manager Assistant*) para la fase de arranque de proyectos, y *Service Managers* y *Service Manager Assistants* para la evolución del producto. Cada persona funcional se centrará en un único rol para evitar la dualidad de funciones.

Se realizará el desarrollo de un nuevo marco de capacidad y asignación de trabajo basado en datos para optimizar la toma de decisiones y mejorar la calidad de vida de los empleados.

En el área comercial se mejorará la propuesta de valor, ampliando la propuesta comercial, presentándola de manera más personal para destacar el valor diferencial de la empresa.

En cuanto al área de marketing se activará la generación de contenido de producto (videos, demos) para dar visibilidad a las funcionalidades clave del ERP. Se continuará con los eventos en vivo dónde se presentan los casos de éxito.

Se realizará el lanzamiento de campañas en redes sociales y email marketing (*newsletter* específica para el ERP). Se buscará optimizar la *web* de la empresa para aumentar el tráfico orgánico.

Por último se buscará mejorar la tasa de recomendación directa de clientes existentes (actualmente solo un 3%) con un programa de fidelización.

En cuanto a capital humano se pretende consolidar y mejorar continuamente el proceso de onboarding para nuevas incorporaciones y estudiantes en prácticas, tanto de perfiles funcionales, como desarrolladores e incluso duales. Mientras que para los profesionales se rescatará el plan de formación y desarrollo profesional funcional.

El objetivo en lo que respecta al reconocimiento, es fomentar la cultura de *feedback* y reconocimiento, destacando a quienes contribuyen al desarrollo de sus compañeros. Impulsar un sistema de ideas con reconocimiento, especialmente relacionado con el producto.

2.4.3 Seguridad de la Información como Acompañamiento Estratégico

En el contexto observado de la empresa, implementar, mejorar y estandarizar el SGSI es el medio para llegar al objetivo de la Seguridad de la Información. Con esto en mente, la empresa podrá transformar el producto físico para la excelencia operativa. La protección sistemática de los activos de información son condición necesario para mantener la confianza de los clientes, asegurar la continuidad del servicio y sumar un valor diferencial al producto tecnológico.

Desde la perspectiva de la gobernanza, un SGSI alineado con ISO/IEC 27001 nos permitiría integrar la gestión de riesgos de seguridad en los mismos procesos en los que se definen los pilares estratégicos, las estrategias empresariales trimestrales y los indicadores de desempeño. Esto implica pasar de prácticas reactivas y dispersas a un modelo planificado, documentado y medible, donde la seguridad de la información acompaña la toma de decisiones sobre nuevas versiones del ERP, uso de IA, migraciones de entorno y expansión comercial.

3. Diagnóstico del estado actual del SGSI de la Empresa

3.1 Introducción

En el presente capítulo abordaremos el análisis del estado actual del SGSI de la organización. El objetivo no es auditar el cumplimiento de la norma ISO/IEC 27001, si no comprender cómo se gestiona actualmente en la práctica los activos de información, los mecanismos de controles que existen, qué nivel de formalización tienen los procesos de Seguridad de la Información y el nivel de formación y concientización de los empleados.

Este diagnóstico constituye la base empírica del trabajo y será lo que nos permitirá identificar la brecha entre las prácticas actuales y los lineamientos de gestión establecidos por las normas ISO/IEC 27000, puntualmente la ISO/IEC 27001, sirviendo de fundamento para el posterior análisis GAP y la elaboración de la propuesta de mejora del SGSI.

El diagnóstico se sustenta en la aplicación de un cuestionario interno, entrevistas con personal clave de la organización y una intensiva revisión de la documentación organizacional disponible.

3.2 Alcance y Objetivo del Diagnóstico

Para saber qué tan lejos se encuentra la empresa de poder aplicar a la certificación ISO/IEC 27001 uno de los pilares fundamentales a conocer es el conocimiento de sus colaboradores. Para eso se realizó una encuesta[19] con un muestreo probabilístico estratificado por área (desarrolladores, funcionales, capital humano y administración) y rol (líderes y

[19] Ver en anexo las preguntas de la encuesta.

colaboradores)[20]. Esto nos dará un panorama para que todos los subgrupos más relevantes del SGSI estén representados.

El criterio de inclusión de los integrantes de la muestra tiene dos criterios principales: personal con más de tres meses de antigüedad en su rol actual y participación directa en operaciones que impliquen datos de clientes de sus clientes.

Para ajustar la selección se decidió que se haría exclusión a personal en licencia prolongada durante el trabajo de campo, pasantes con menos de tres meses de antigüedad y terciarizados sin acceso a información ni sistemas corporativos.

El diagnóstico lo centraremos en los aspectos organizacionales y de gestión de la Seguridad de la Información, sin realizar evaluaciones técnicas detalladas de configuraciones de infraestructura, pruebas de penetración ni análisis forense de sistemas.

3.3 Metodología de Relevamiento

A continuación detallaremos los criterios de selección de la muestra, la tasa de participación lograda y los procedimiento técnicos que utilizamos para procesamiento y análisis de los datos obtenidos.

3.3.1 Población y Muestra

El total de los empleados en el momento de las encuestas era de 78 personas, de las cuales 10 eran de gestión, 33 de desarrollo y 35 de consultoría. Además, en ese número se

[20] Ver anexo para ver el perfil de los encuestados

incluyen 7 personas de prácticas y 2 de licencia indeterminada, las cuales fueron excluidas, quedando un total de 68.

3.3.2 Tasa de Respuesta

Hemos enviado un cuestionario estructurado a un total de 10 integrantes de la organización pertenecientes a distintas áreas funcionales y niveles de responsabilidad.

Hemos recibido un total de 7 respuestas completas, lo que representa una tasa de respuesta del 70%. No se registraron cuestionarios incompletos. Los encuestados fueron 3 de gestión, 2 de desarrollo y 2 de consultoría. De las personas de desarrollo y consultoría tomamos un líder y un colaborador.

Si bien la encuesta no fue anónima, le aclaramos a los participantes que la información sería utilizada exclusivamente con fines académicos y de diagnóstico organizacional, para favorecer las respuestas sinceras y tratando de reducir posibles sesgos.

3.3.3 Forma de Análisis de los Datos

El instrumento de recolección de datos consistió en un cuestionario distribuido en formato de planilla electrónica, compuesta mayormente por preguntas cerradas de tipo dicotómico (Sí/No/No sabe-No contesta), complementada en algunos casos por campos de comentarios y una pregunta final de valoración general mediante puntuación, con una escala del 1 al 5.

Dado el tamaño de la muestra reducido, el análisis de la información lo basamos de manera manual mediante revisión directa de las respuestas. Elaboramos tablas de consolidación por pregunta, calculando proporciones de respuesta y tendencias generales, priorizando la

identificación de patrones de comportamiento organizacional por sobre el análisis estadístico inferencial.

La información la completamos con entrevistas informales mantenidas con miembros de la Dirección y revisando la documentación interna disponible, permitiendo triangular los resultados del cuestionario con evidencia organizacional.

3.3.4 Limitaciones del Estudio

El diagnóstico obtenido corresponde a un estudio de caso aplicado a una única organización, por lo que sus resultados no pretenden ser generalizables a otras empresas del mismo tipo.

Entre las principales limitaciones nos encontramos con que los investigadores desempeñamos trabajo como funcional dentro de la organización. Si bien esto nos facilitó el acceso a la información y a la documentación interna, también podría influir en la interpretación de ciertos resultados debido al conocimiento previo del contexto organizacional.

Otro sesgo importante con el que nos encontramos es con de las respuestas de las encuestas. Al no ser anónimas, puede ser que algún colaborador haya respondido en función de lo socialmente esperado o alineado a las prácticas formales de la empresa y no estrictamente a su comportamiento cotidiano.

El tamaño de la muestra también es un sesgo a tener en cuenta. La cantidad de respuestas obtenidas limita la realización de análisis estadísticos más profundos. Por este motivo es que hemos adoptado un enfoque cualitativo-interpretativo, orientado a la identificación de tendencias y brechas, más que a la medición cuantitativa.

La organización no posee un SGSI formalizado ni métricas históricas de Seguridad de la Información, lo que nos impide realizar una evolución temporal.

3.4 Resultados

Presentaremos en las siguientes páginas los resultados obtenidos de las encuestas realizadas, agrupadas por contenido sobre los aspectos de la empresa que necesitábamos recabar para acercarnos al diagnóstico.

3.4.1 Conocimientos Generales del SGSI en la Empresa

En este apartado nos interesa saber el conocimiento de los colaboradores de la empresa en cuanto a los SGSI que se tienen, si se tienen, si hay un conocimiento sobre ello, los propósitos principales del SGSI. Además nos interesa saber qué tanto conocimiento tienen sobre la certificación de ISO/IEC 27001 y por qué es importante para la empresa. Y lo más importante en está sección es saber si han recibido información o capacitación sobre las políticas de seguridad de la información.

En los resultados de las encuestas podemos ver que la mitad de las personas encuestadas indican no saber si tiene, un cuarto de la muestra afirma que no hay y el resto indican que si tienen pero que habría que revisarla. Solamente capital humano afirma que si hay y comenta que se maneja de manera externalizada los acuerdos de confidencialidad de los colaboradores, pero en cuanto a los datos de los clientes no comentan nada. Además, la mitad afirma no conocer los objetivos y el resto tampoco está completamente seguro.

En cuanto a los conocimientos de la certificación de la ISO/IEC 27001 está dividido en mitades, una parte conoce el significado y la importancia de contar con él y la otra parte no lo sabe o no cree que sea importante.

En la parte que más nos interesaba conocer nos hemos encontrado con una mayoría que afirma no haber tenido ningún tipo de capacitación sobre seguridad de la información y la pequeña parte que si la tuvo comenta que fue en talleres con inscripción voluntaria.

3.4.2 Política y Alcance de Seguridad de la Información en la Empresa

En la segunda sección queremos saber si los colaboradores conocen la Política de Seguridad de la Información de la empresa, si saben dónde consultarla y cuáles son los procedimientos de seguridad de la información. Saber si entienden cómo se aplica la Política de Seguridad de la Información en sus tareas diarias, si están definidas las responsabilidades en materia de seguridad dentro de cada área y si han recibido instrucciones claras sobre cómo proteger la información que manejan.

En el área de capital humano, el área técnica y funcional indican conocer las Políticas de Seguridad de la Información de la empresa y dónde consultarla junto con los procedimientos de Seguridad de la Información, también entienden cómo se aplica en sus tareas diarias, a diferencia del área administrativa que no las conoce o lo hace parcialmente.

Hay una parte muy baja de la muestra que afirma haber tenido algún tipo de capacitación sobre seguridad de la información en el último año.

Las responsabilidades en cada área no están definidas en su totalidad en base a los resultados de las encuestas, más allá de que alguna área sea unipersonal.

Solamente un área ha definido de manera interna cómo proteger la información que manejan pero comentan que creen tener carencias. El resto de las áreas no sabe qué pasos tendría que seguir, sino que lo hace de manera intuitiva.

3.4.3 Gestión de Riesgos en la Empresa

Está sección es muy importante porque nos sirve para detectar el nivel de gestión de riesgos de la empresa por parte de los colaboradores, si saben qué hacer en caso de detectar un incidente de seguridad de la información, si sienten capacitados para identificar riesgos en el trabajo diario y si conocen los riesgos que existen en el trabajo.

El cien por ciento de los encuestados indican que no saben si se realizan evaluaciones periódicas de riesgos de seguridad de la información y algunos afirman que no se realizan. En cuanto a los controles específicos para proteger los activos de información la mitad dicen que si hay, pero ninguno específica el procedimiento a seguir para mitigar los riesgos que se identifican.

No hay una respuesta uniforme a la pregunta sobre si la empresa cumple con leyes o regulaciones sobre protección de datos y seguridad de la información y no están seguros del cómo.

Todos consideran que la empresa toma acciones cuando identifica riesgos o incidentes.

3.4.4 Responsabilidades, Competencias y Recursos de Seguridad de la Información en la Empresa

En el cuarto apartado indagamos sobre las responsabilidades de la empresa. Queremos conocer si se conocen cuáles son las responsabilidades de cada función, quiénes son los

responsables de seguridad de la información en la empresa, si hay recursos disponibles para cumplir las responsabilidades y si se evalúa el desempeño de los equipos en relación a la seguridad de la información.

Ninguno de los encuestados considera que las responsabilidades relacionadas con la seguridad de la información están claramente asignadas en la empresa. Mientras que la mitad de las personas indicaron contar con la capacitación o formación necesaria para proteger la información durante sus funciones.

La totalidad afirma que no se evalúa el desempeño o el del equipo en relación con la seguridad de la información y además, indican no contar con los recursos necesarios para cumplimentar estas medidas.

3.4.5 Concientización y Cultura de Seguridad de la Información en la Empresa

Está sección está dedicada a conocer el nivel de concientización sobre la seguridad de la información y cómo lo aborda la empresa. Si hay iniciativas internas, material disponible y documentación sobre el tema. Además queremos saber el nivel de interes y el compromiso de los participantes.

Todos consideran importante y útil las capacitaciones y los materiales sobre seguridad de la información, pero solo la mitad afirma haber participado en actividades de concientización sobre seguridad de la información. Así mismo, prácticamente todos indican querer recibir más información al respecto.

La mitad de los encuestados conoce las consecuencias o sanciones si alguien incumple las normas de seguridad de la información. Esto se da debido a que se manifiesta que la empresa

no promueve del todo una cultura de seguridad de la información entre sus empleados y a que la dirección no está del todo comprometida según la encuesta.

Sin embargo el cincuenta por ciento de las personas dicen que hay una mejora continua de las medidas de seguridad de la información.

3.4.6 Documentación y Control en la Empresa

En este último apartado analizaremos la existencia de la documentación disponible sobre seguridad de la información.

Más de la mitad de los encuestados no sabe cuáles son las políticas, las normativas o los procedimientos relevantes para el rol que cumplen. Aunque la mayoría dice tener acceso a la información necesaria para realizar las tareas de manera segura.

No hay un responsable claro en las áreas para aprobar o actualizar documentos de seguridad de la información en base a lo respondido. Pero todos afirman conocer las medidas que se toman para proteger la información.

3.5 Conclusiones Generales

A partir del análisis realizado, concluimos que la empresa se encuentra en una etapa inicial de madurez en relación con la gestión del SGSI, presentando tanto fortalezas como oportunidades de mejora de cara a una futura implementación formal de un SGSI basado en la norma ISO/IEC 27001.

Como aspecto positivo, podemos identificar la existencia de documentación y prácticas vinculadas a la seguridad de la información en algunas áreas. Asimismo, los colaboradores manifiestan interés y predisposición para recibir capacitación, lo cual constituye una base

favorable para el desarrollo de una cultura organizacional orientada a la seguridad de la información.

No obstante, observamos que el conocimiento sobre el SGSI, sus objetivos y la certificación ISO/IEC 27001 no se encuentra uniformemente distribuido entre los colaboradores. La documentación existente se presenta de forma dispersa y con un nivel de formalización desigual, lo que limita su aplicación homogénea en toda la organización.

Por otra parte, la gestión de riesgos, la asignación de responsabilidades y la evaluación del desempeño en materia de seguridad de la información se presentan como áreas incipientes. Si bien los colaboradores perciben que la empresa actúa ante incidentes, la falta de procesos formalizados y conocidos evidencia la necesidad de fortalecer estos aspectos.

En síntesis, la empresa cuenta con condiciones favorables para avanzar hacia la consolidación de un SGSI, especialmente en términos de compromiso potencial de los colaboradores. Para acercarse a una eventual certificación ISO/IEC 27001, será necesario reforzar la formalización de procesos, la capacitación continua y el involucramiento de la Dirección, permitiendo así una gestión del SGSI más consistente y alineada con las buenas prácticas internacionales. En el capítulo siguiente realizaremos un análisis GAP tomando como marco la norma ISO/IEC 27001.

4. Análisis GAP ISO – Sistema de Gestión de Seguridad de la Información (ISO/IEC 27001)

4.1 Introducción

A continuación transcribimos las preguntas con sus respectivos hallazgos, evidencias, comentarios, posibles impactos a nivel económico, de procesos y reputacional junto con recomendaciones del análisis de brecha entre el estado actual de la empresa y los requisitos de la ISO/IEC 27001. Nos centraremos en los puntos más relevantes y generales de la norma, con el objetivo de obtener un panorama lo más completo posible, ya que consideramos que no podemos abarcar todas y cada una de las cláusulas que contiene la normativa. Esta información fue obtenida en base a la documentación presentada por parte de la empresa, por la encuesta realizada y detallada en el punto anterior y por último por una entrevista realizada a la Dirección General de la empresa.

4.2 Contexto de la Organización

En este apartado los requisitos de la norma ISO/IEC 27001 implicados son los del Capítulo 4: “Contexto de la Organización” y el Capítulo 6: “Planificación”. Del capítulo 4, los puntos desatacados son los 4.1: “Comprensión de la Organización y su Contexto”; 4.2: “Comprensión de las Necesidades y Expectativas de las Partes Interesadas”; 4.3: “ Determinación del Alcance del SGSI”; y el 4.4: “Sistema de Gestión de la Seguridad de la Información”. Del capítulo 6 la primera sección, la 6.1: “Acciones para Tratar Riesgos y Oportunidades”.

¿La organización evalúa los riesgos y oportunidades del contexto para asegurar que el Sistema de Gestión de Seguridad de la Información (SGSI) puede alcanzar los resultados previstos, reducir los efectos no deseados y lograr la mejora continua?

En un análisis FODA del nivel de madurez y cultura de seguridad de la información basado en la encuesta se han dado los siguiente aspectos.

Fortalezas - Las áreas de Capital Humano y los colaboradores funcionales muestran un conocimiento parcial sobre la protección de datos (GDPR), la importancia de la certificación ISO/IEC 27001 y la confidencialidad en relación a clientes y proyectos. - En los comentarios se observa una predisposición a mejorar los conocimientos y las prácticas de seguridad. - Se han promovido talleres puntuales desde los propios colaboradores.	Oportunidades - Las personas se encuentran predispuestas para introducir una campaña de seguridad de la información, entrenamiento por áreas, simulaciones de phishing y talleres prácticos obligatorios. - Crear una cultura sólida de protección de datos. - Estandarizar y documentar procesos de políticas claras, definir responsables y centralizar documentación.
Debilidades - Bajo nivel general de conocimientos sobre SGSI, sin conocimiento de los objetivos que tiene, las políticas y procedimientos y no han recibido información sobre el tema. - Ausencia de una capacitación obligatoria estructurada. - Falta de claridad en los roles y responsabilidades en cuanto a la seguridad de la información de las áreas. - La seguridad de la información se percibe más como una obligación que como parte del trabajo diario.	Amenazas - El desconocimiento general del SGSI aumenta la probabilidad de pérdidas de información interna, filtración de base de datos de clientes, sanciones regulatorias, e incumplimientos contractuales con clientes. - La falta de información aumenta la probabilidad de *phishing*, configuraciones inseguras y manejo inapropiado de datos.

¿Se tienen identificadas y documentadas las "Partes Interesadas" del negocio pertinentes a la Seguridad de la Información? Se evidencia falta de documentación sobre las partes interesadas del negocio, sin embargo los colaboradores manifiestan identificarlos y tomar algunas medidas de seguridad de la información de manera intutiva.

¿Se tienen identificados y documentados los requisitos de las partes interesadas pertinentes a la seguridad de la información y sus obligaciones? (incluyendo leyes aplicables, regulaciones, contratos, etc.). Actualmente la empresa cuenta con documentación dispersa sobre la seguridad de la información y las obligaciones. No hay un documento específico.

Las últimas tres preguntas están agrupadas debido a que la respuesta es la misma: *¿El alcance SGSI se encuentra correctamente definido y documentado? ¿Tienen implementado, mantienen y mejoran continuamente un SGSI en base a un marco de cumplimiento? Ejemplo: ISO/IEC 27001, NIST, etc. ¿Cuentan con un "mapa de interacción de los procesos críticos" incluidos en el alcance del SGSI?* No hay documentación del SGSI directamente, si no como lo hemos comentado anteriormente, hay información dispersa.

Impacto potencial y acciones recomendadas

En este primer apartado por la falta de identificación de requisitos legales y por la inexistencia de la documentación pertinente la organización podría llegar a tener un impacto altamente negativo en caso de incidentes de seguridad de la información por fuga de datos sensibles con multas elevadas según la normativa europea GDPR, dependiendo la gravedad.

La ausencia de procedimientos formales de seguridad de la información y la poca definición de los roles en estos casos podría ralentizar la gestión de incidentes, podría frenar las operaciones frenando la entrega de servicios de calidad a los clientes y como consecuencia final una pérdida reputacional devenida en una posible pérdida de clientes.

Aprovechando las fortalezas y oportunidades que se presentaron en el análisis FODA se recomienda elaborar un análisis de contexto y de las partes interesadas.

Lo principal seria definir el alcance del Sistema de Seguridad de la Información, los objetivos, la metodología de evaluación y tratamiento de riesgos. Comenzar a registrar las formaciones, habilidades y experiencias de los colaboradores referidas a seguridad de la información. Tener documentados los procedimientos operativos de la gestión diaria, hacer una evaluación de riesgos y comenzar con un seguimiento y medición de los mismos.

4.3 Liderazgo

El apartado de liderazgo se refiere al capítulo 5: “Liderazgo”, puntualmente a la cláusula 5.1: “Liderazgo y Compromiso”, a la cláusula 5.2: “Política”, a la 5.3: “Roles, Responsabilidades y Autoridades en la Organización”, y el capítulo 7, cláusula 7.4: “Comunicación” que se refiere a sus cinco aspectos claves: qué comunicar, cuándo comunicar, a quién comunicar, quién debe comunicar y los procesos mediante los cuales se debe llevar a cabo la comunicación.

¿La "Alta Dirección" demuestra liderazgo y compromiso en relación al SGSI? Hay un esfuerzo personal de la Alta Dirección en al compromiso en relación al SGSI, pero no llega a trascender por la disponibilidad y el esfuerzo que requiere actualmente hacerlo. Desde la AD hay una predisposición y un apoyo a los colaboradores que demuestran interés y proactividad.

¿Poseen una "Política de Seguridad de la Información" definida y documentada? ¿Existe un proceso de comunicación a las partes interesadas? ¿Las responsabilidades y las autoridades para los roles pertinentes a la Seguridad de la Información están asignados y comunicados? Hay documentación dispersa bajo otros título o junto con otros procedimientos. Si bien, hay una mención en la documentación interna, de que el círculo de DevOps es el encargado de velar por la mejora metodológica de desarrollo, tanto a nivel tecnológico como cultural. Sobre todo el ciclo de desarrollo del *software* de manera que los procesos son muchos

más ágiles y seguros. No se encuentra evidencia de cómo se encarga, ni da detalles de acentuando la importancia de tomar ciertas medidas.

Impacto potencial y acciones recomendadas

La falta de evidencia de liderazgo claro a nivel seguridad de la información implica una duplicación de esfuerzos y una inversión infeciente. Si las actividades son aisladas y no se alinean con la estrategia, todo esfuerzo dará pérdidas a nivel económico con horas perdidas o proyectos incompletos.

A nivel operativo el impacto se da por dejar librado a cada área que se maneje "a su manera" haciendo que quizás no sea tan efectivo para el resto de la organización, haciendo más complejo un desbloqueo en caso de incidentes. Por supuesto que todo esto tendría un impacto reputacional alto si sucede con algún proceso de algún cliente.

Como no encontramos una política formal, solo referencias generales en diferentes documentos, lo ideal es redactar una política SI clara y que este aprobada por la Alta Dirección. En la misma debe incluir principios, alcances, objetivos, roles, sanciones, requisitos legales y compromisos. Una vez definida y aprobada publicarla en la *wiki* interna, comunicarla en reuniones y canales corporativos como la newsletter.

4.4 Planificación

En esta sección abordaremos el capítulo 6: "Planificación" de la ISO/IEC 27001. Específicamente a las cláusulas 6.1.1: "Generalidades", la 6.1.2: "Evaluación de riesgos de Seguridad de la Información", la 6.1.3: "Tratamiento de los riesgos de Seguridad de la

Información", la 6.2: "Objetivos de Seguridad de la Información y planificación para lograrlos", y por último, la cláusula 6.3: "Planificación de los cambios".

¿El diseño y la planificación del SGSI se realizó teniendo en cuenta los riesgos y oportunidades del contexto y las necesidades de las partes interesadas? No se realizó un SGSI, si no que la información se encuentra bajo diferentes títulos o procedimientos documentados, por lo que obviamente no creemos que haya habido relacionadas a este punto. Lo que hay es lo que se fue haciendo de manera intuitiva e implícita con respecto a la seguridad en general.

¿Existe un proceso definido para la evaluación de los riesgos y oportunidades? Incluye: análisis y valoración del riesgo. El círculo de DevOps suele tomar medidas cuando identifican algún riesgo, pero no hay un proceso definido ni documentado. Es el mismo caso para la pregunta *¿Disponen de un proceso documentado para tratar los riesgos de seguridad de la información identificados?*

¿Se tienen definidos y documentados los "objetivos" de Seguridad de la Información? Tampoco encontramos una única documentación sobre este apartado, simplemente se anonimizan las bases de datos de los entornos de TEST de los clientes. Pero fuera de eso no hemos encontrado ningún procedimiento a seguir.

¿Existe un procedimiento que permita evidenciar que los cambios sustanciales en el SGSI se llevan a cabo de manera planificada? Esta pregunta es de fácil análisis, cómo no hay un SGSI documentado, procedimentado ni establecido con consciencia, los cambios no siguen ningún tipo de estrictas indicaciones para los cambios.

Impacto potencial y acciones recomendadas

El impacto a nivel económico puede ser muy alto si no se conocen las vulnerabilidades y los riesgos de cada activo y procedimiento de la organización. No se gestionan los riesgos críticos, no se priorizan las medidas de protección haciendo que sea mucho más complejo y por ende costos reconocer un incidente de seguridad de la información. Siempre es mucho más costoso tomar medidas reactivas en lugar de estratégicas.

No tener definidos los objetivos de la seguridad de la información ni los procesos hace más difícil la implementación de controles que prevengan la interrupción de los procesos.

Diseñar y documentar el SGSI desde cero con la definición del alcance, los procesos, y con toda la estructura documental. Implementar una metodología de análisis y tratamiento de riesgos. Definir los objetivos de la Seguridad de la Información alineados al negocio, más allá de la base de datos de los clientes. Por último, lo ideal, sería tener un procedimiento de gestión de cambios del SGSI para cuando se vayan haciendo mejoras y adaptaciones.

4.5 Soporte

En este inciso abarcaremos el contenido del capítulo 7: “Apoyo”. Indagaremos sobre los hallazgos relacionados puntualmente a las cláusulas 7.2: “Competencia”, la 7.3: “Toma de consciencia”, la 7.4: “Comunicación”; la 7.5: “Información documentada” y dentro de esta última, la 7.5.1: “Generalidades”, 7.5.2: “Creación y actualización” y la 7.5.3: “Control de información documentada”.

¿Existe en la organización un organigrama definido y documentado? Hay un organigrama definido y documentado de la empresa. No hay una actualización al día, pero la estructura mantiene la esencia.

¿La organización cuenta con "Perfiles de Puesto" documentados que prevén las habilidades que debe tener cada colaborador, teniendo en cuenta su rol y función desempeñada? La empresa tiene detallados los perfiles de puestos, conocidos como roles. Están documentados en una wiki y una descripción muy completa con la misión del rol, las responsabilidades principales, las funciones y los objetivos con sus indicadores de desempeño.

¿Poseen un legajo físico del personal en donde se incluyen sus antecedentes de formación, habilidades, experiencia y calificaciones del personal? No hay evidencia de que el área de capital humano posea un legajo físico con todo lo mencionado. De todas maneras se puede sacar un seguimiento de los cursos internos sobre el sistema que se fueron haciendo con los resultados obtenidos.

¿Se efectúan evaluaciones periódicas de desempeño al personal? Hay evaluaciones periódicas trimestrales de dos tipos. Primero, las devoluciones 360, que son las observaciones de todas las personas con las que se trabaja, sin importar el área o el rol que cumplan, cualquiera puede indicar cosas positivas o negativas con un caso real que lo demuestre. Segundo, las *One and One*[21] en donde los superiores con algún representante de capital humano hacen una evaluación de los objetivos alcanzados, de los pendientes y de las áreas de mejora.

¿Los procedimientos de negocio relevantes o críticos están documentados? Hay documentación de todos los procedimientos de negocios relevantes o críticos. Están divididos por área y por círculo.

¿Tienen definido un cronograma anual de capacitación y concientización de Seguridad de la Información? ¿Los miembros de la organización tienen acceso y conocen todos los aspectos que aborda la Política de Seguridad de la Información? ¿Se prevén sanciones disciplinarias para el personal que incumpla con los requisitos del SGSI? ¿La organización

[21] One and One: reuniones uno a uno del colaborador con su responsable directo.

cuenta con un "Plan de Comunicación Interna y Externa" respecto al SGSI? ¿La organización posee la información documentada que requiere ISO 27001? Todas estas preguntas se pueden recopilar y responder de manera conjunta. No hemos encontrado ningún cronograma de capacitación ni de concientización de Seguridad de la Información. Ha habido algún taller no obligatorio dentro de las jornadas trimestrales. Al no haber tampoco un SGSI detallado, identificado, ordenado, documentado, reconocido y compartido, no hay sanciones posibles, no hay un plan de comunicación y por último, no se posee la información requerida por la ISO/IEC 27001.

¿Los documentos correspondientes al SGSI cumplen los siguientes requisitos? Identificación, descripción, formato y medio apropiado, especificación de la persona que realizó su revisión, aprobación y adecuación. Hay algunos documentos que pueden llegar a cumplimentar el formato indicado, pero tienen que ver más que nada con la definición de roles, con los servicios y productos brindados, con los contratos de clientes y similares.

¿La información documentada del SGSI está adecuadamente protegida y disponible para su uso por parte de las personas autorizadas? En este caso podríamos afirmar que está disponible de manera protegida y disponible en una wiki interna de la empresa que sólo las personas de la misma pueden ingresar. No están abiertas a los clientes ni a agentes externos.

Impacto potencial y acciones recomendadas

Las deficiencias en la formalización y estandarización de actividades de seguridad de la información tienden a traducirse en mayor probabilidad de errores humanos y respuestas inconscientes ante incidentes, lo que puede generar interrupciones de servicios que se luego pasan a ser más horas en recuperación elevando los costes operativos.

Lo primero y más sencillo de hacer es mantener actualizado el organigrama. Tener legajos de personal completos con un seguimiento de competencias adquiridas. Integrar requerimientos de Seguridad de la Información a los perfiles. Implementar un programa anual de capacitación y concientización.

4.6 Operación

Las siguientes preguntas buscan recopilar información sobre el capítulo 8 de la ISO/IEC 27001, llamado "Operación". En esta sección veremos las cláusulas 8.2: "Evaluación de los riesgos de Seguridad de la Información" y la 8.3: "Tratamiento de los riesgos de la Seguridad de la Información".

¿Efectúan una evaluación del riesgo a la seguridad de la información de manera periódica? No ha surgido en las entrevistas ni en los cuestionarios la idea de que haya una evaluación periódica del riesgo, es algo más proactivo y reaccionario. Cuando se sospecha sobre algo se hace una evaluación, en ocasiones *post mortem*[22] y en otras se prueban vulnerabilidades puntuales en base a sugerencias o noticias que promueven a la acción.

¿Realizan el adecuado tratamiento del riesgo de Seguridad de la Información sobre los activos de información identificados? ¿El procedimiento está documentado? Se realiza una anonimización sobre la base de datos de los clientes, el único activo identificado hasta el momento como el más importante. Está documentado el procedimiento en la wiki para el área de DevOps que es la encargada de realizarlo y controlarlo.

[22] Post mortem: análisis realizado posterior al hecho concluido.

Impacto potencial y acciones recomendadas

El impacto potencial en este caso radica en que la organización debe actuar de manera reactiva, demorando en la detección de vulnerabilidades generando en consecuencia mayores tiempos de recuperación ante incidentes con posibles reducciones o interrupciones del servicio.

Formalizar un proceso periódico de análisis de riesgos. Previo a eso es necesario inventariar y clasificar todos los activos, documentar y ampliar los tratamientos de riesgo, no solo anonimizar la base de datos. Por último estandarizar los procedimientos operativos mínimos relacionados a la seguridad de la información.

4.7 Evaluación de Desempeño

En este punto recabaremos información basándonos en el capítulo 9: "Evaluación de desempeño" con enfoque en las cláusulas 9.1: "Seguimiento, medición, análisis y evaluación", la 9.2: "Auditoría interna", y la 9.3: "Revisión por la Dirección".

¿La organización posee un "Plan Operativo Anual" para el monitoreo y medición de los resultados? (*Dashboard* [23]/ Métricas) La empresa presenta en cada trimestre los resultados de todas las áreas, con una comparativa con el trimestre previo y a con el mismo trimestre en el año anterior. En este sentido la organización se encuentra muy ordenada y estructurada para la monitorización y medición de los resultados.

¿La organización posee un "Programa Anual de Auditoría Interna"? ¿Su procedimiento está documentado? No hay evidencia de que la empresa cuente con un programa de auditoría interna de ningún tipo. No es algo que ningún colaborador haya mencionado.

[23] Dashboard: panel visual que muestra información clave de forma resumida

Podrían llegar a tener algo que la AD o capital humano hayan olvidado mencionar por no ser de carácter continuo.

¿Se presenta anualmente a la "Alta Dirección" un reporte con las principales actividades realizadas relacionadas a la eficacia y la mejora continua del SGSI? No nos han comentado si tienen un reporte anual a la Alta Dirección con las principales actividades relacionadas al SGSI, pero dentro del balance trimestral se presentan las incorporaciones, las mejoras y todo lo relacionado a la seguridad en general. Siempre incluido dentro de los círculos o de las áreas, no de manera puntual y transversal.

Impacto potencial y acciones recomendadas

La empresa se ve con una capacidad limitada para detectar fallos estructurales en los controles de seguridad de la información antes de que deriven en inconvenientes. Esto puede generar un impacto operativo relevante con falta de trazabilidad y menor capacidad de anticipación.

Crear un plan operativo anual del SGSI con métricas e indicadores. Preparar un informe trimestral para las jornadas sobre el desempeño, incidentes y estado del SGSI.

4.8 Mejora

En este último apartado preguntaremos en base al capítulo 19: “Mejora”, enfocándonos en dos cláusulas, la 10.1: “No conformidad y acciones correctivas” y la 10.2: “Mejora continua”.

¿Cuentan con un registro de "no conformidades" y/o "acciones correctivas"? ¿Se realizan actividades que permitan evidenciar la "Mejora Continua" en la gestión de la empresa

respecto a la Seguridad de la Información? Todas las tareas, las mejoras o proyectos que se llevan a cabo en la empresa cuentan con un registro, se lleven a cabo o no. Por lo tanto, está disponible la evidencia de las mejoras las cuales se informan a través de los *newsletter* semanales y en las jornadas trimestrales.

Impacto potencial y acciones recomendadas

Desde un punto de vista operativo, disponer de estos registros reduce la posibilidad de duplicar esfuerzos, favorece la continuidad de los proyectos y permite reaccionar con mayor rapidez ante necesidades emergentes.

Formalizar un registro de no conformidades para identificar, detallar y rastrear cualquier incumplimiento de requisitos de seguridad de la información y acciones correctivas. Establecer un proceso de mejora continua con revisión trimestral del SGSI y establecer un criterio de priorización basado en riesgos. En términos económicos y reputacionales, contar con evidencias claras de mejora continua puede fortalecer la percepción de madurez organizacional frente a clientes, auditores o socios estratégicos.

4.9 Plan de Acción

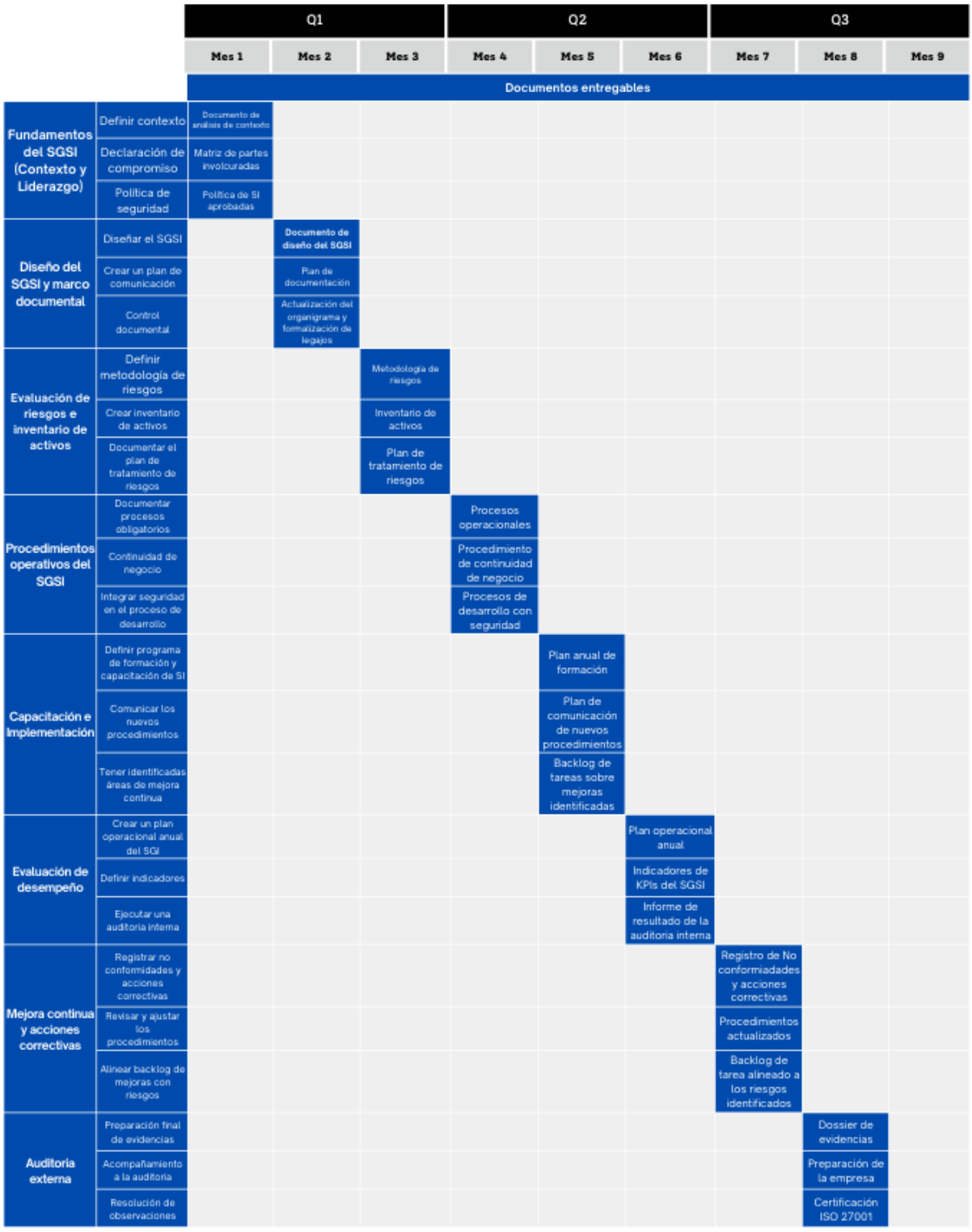
A continuación resumiremos en una matriz de criticidad todos los aspectos del análisis de la brecha de seguridad de la información de la empresa, en base a las recomendaciones de la ISO/IEC 27001 y al finalizar propondremos un *road map* para acercarnos a lo propuesto de una certificación en menos de un año. Para determinar la criticidad de cada acción se tomará en cuenta el impacto potencial que tiene la brecha detectada sobre la tríada de la Información (confidencialidad, integridad y disponibilidad) y el cumplimiento legal de la ley GDPR.

El objetivo del plan de acción no es la obtención inmediata de la certificación, si no la implementación progresiva de un SGSI, alineado con los requisitos y las buenas prácticas de la ISO/IEC 27001.

Categoría / Control	Criticidad	Hallazgo	Acción recomendada	Plazo (meses)	Esfuerzo estimado	Recursos
Contexto de la organización	Media	Falta de análisis estructurado de partes interesadas y riesgos del contexto	Definir la estructura y las paprtes interesadas y los riesgos del contexto	Corto (1-2)	40-60 h	Dirección + SGSI
Liderazgo	Alta	Falta evidencia de compromiso formal de cara a la seguridad de la información, no hay una política de SI, ni una comunicación oficial sobre SGSI	Crear una declaración de compromiso sobre seguridad de la información, aprobar política de SI y establecer plan de comunicación interna sobre seguridad	Corto (1)	40-60 h	Alta Dirección + SGSI
Planificación	Alta	Evaluación de riesgos incompleta sin metodología, tratamiento de riesgos de manera informal y reactivo	Diseñar una evaluación de riesgos. Crear y documentar una metodología de riesgos.	Corto-Medio (3-4)	120-160 h	SGSI + Responsables del área + Dirección
Soporte	Media	Organigrama desactualizado, falta de legajos personales completos con seguimiento de competencias. Falta de plan de capacitación.	Actualizar organigrama, formalizar legajos, añadir requisitos de Seguridad de la Información a los roles, crear programas anual de capacitación.	Medio (2-3)	80-120 h	Capital Humano + SGSI
Operación	Alta	No hay evaluaciones de riesgos. Análisis de vulnerabilidades reactivas.	Darle más fuerza a los tratamiento de riesgos. Implementar controles para mantener el nivel de riesgo aceptable.	Medio (2-3)	100-150 h	SGSI + TI + DevOps
Evaluación del desempeño	Media	No existe un plan operativo anual del SGSI, no hay auditorías internas	Crear un plan operativo anual con métricas, implementar programas de auditorias internas.	Medio (2)	40-60 h	Dirección
Mejora	Media	Faltan registros formales de no conformidades y acciones correctivas	Documentar las no conformidades y las acciones correctivas.	Corto-Medio (1-2)	30-50 h	SGSI

1 Matriz de criticidad, acción, plazo, esfuerzo y recursos

Roadmap hacia la certificación ISO/IEC 27001



4 Diagrama de Gantt

5. Conclusiones

En el transcurso del trabajo se realizó una investigación dentro de una empresa de desarrollo de sistema de gestión ubicada en la ciudad de Madrid, España, dentro de un marco teórico sobre los principales postulados que plantea la gestión del SGSI, considerando la normativa GDPR y las recomendaciones del estándar ISO/IEC 27001. El objetivo fue analizar la brecha de seguridad de la información para proponer acciones de mejora que fortalezcan la protección de los activos de información.

Se realizó un estudio de campo dentro de la organización en el que accedimos a documentación interna, se aplicaron cuestionarios al personal y se llevaron a cabo entrevistas con responsables de diferentes áreas y sectores. A partir de este relevamiento se contrastaron las prácticas actuales en materia de seguridad de la información con los requisitos necesarios para la certificación ISO/IEC 27001.

Acá nos adentramos en los objetivos específicos de este trabajo. El primero es evaluar las políticas y controles de seguridad de la información actualmente implementados en la empresa, comparar dichos controles con los requerimientos de la norma ISO/IEC 27001. Podremos observar que no hay una estructura en cuanto a materia de seguridad de la información. La documentación encontrada está dispersa en las diferentes áreas y no se encuentra ninguna capacitación obligatoria a realizar.

Identificamos múltiples vulnerabilidades y riesgos derivados de las brechas detectadas. Entre ellas consideramos que la más importante es la falta de una política interna de seguridad de la información y la carencia de concientización del personal sobre las amenazas y riesgos derivados de los propios activos de información empresariales y de sus clientes.

Determinamos el impacto potencial de dichas brechas en el ámbito económico, operativo y reputacional en función de la comparación entre los requisitos del sistema de

gestión de seguridad de la información recomendado para la certificación ISO/IEC 27001 y la situación real de la empresa.

En conclusión, a partir del relevamiento realizado determinamos que el nivel de madurez de la seguridad de la información en la empresa es incipiente o bajo. Esta calificación se fundamenta en la ausencia de un Sistema de Gestión de Seguridad de la Información (SGSI) formal, la carencia de políticas centralizadas y debido a la dispersión en la documentación y ausencia de evidencia estandarizada. Actualmente, la organización opera con prácticas mayormente reactivas e intuitivas, con información dispersa en diferentes áreas y sin una gobernanza transversal clara.

Por último, creemos que es plenamente viable que la empresa implemente un proyecto de mejora y progrese hacia una certificación. Esta viabilidad se sustenta en la alta predisposición de los colaboradores para recibir capacitación y en el apoyo detectado por parte de la Alta Dirección para fortalecer la seguridad. El roadmap propuesto demuestra que es posible reducir sustancialmente la brecha en un período menor a un año mediante la formalización de procesos y roles. No se plantea como objetivo inmediato obtener la certificación ISO/IEC 27001 ya que consideramos que primero hay que acotar la brecha, fomentar una cultura de la Seguridad de la Información más intrínseca en los colaboradores y cuando ese funcionamiento ya se encuentre más afianzado y estandarizado, se podría planear obtener la certifiacción ISO.

La implementación de estas mejoras no sólo asegurará el cumplimiento normativo, sino que generará un beneficio directo para el negocio al garantizar la continuidad operativa y minimizar costos por incidentes. Para las partes interesadas, especialmente los clientes que confían sus datos al ERP de la compañía, este avance se traduce en una mayor confianza, transparencia y una ventaja competitiva que asegura la protección de su información sensible

a largo plazo. Finalmente, las estrategias propuestas permitirán a la empresa transitar desde una seguridad informal hacia un modelo de gestión profesional alineado con los mejores estándares internacionales.

Bibliografía

Report, Data Brench Investigation. 2023.

Laudon, Kenneth C., and Jane P. Laudon. 2021. *Management Information Systems.* Pearson College Div.

Incibe. 2020. "Glosario de términos de ciberseguridad." Madrid.

ISACA. n.d. *Manual CISA 28° edición.*

García, Ricardo Fernández. 2006. *Sistemas de gestión de la calidad, ambiente y prevención de riesgos laborales. Su integración.* Editorial Club Universitario.

Dirección General de Modernización Administrativa, Procedimientos e Impulso de la Administración Electrónica. 2012. *MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información.* Madrid. Ministerio de Hacienda y Administraciones Públicas.

2024. *Repsol.* Abril 10. https://www.repsol.com/es/energia-avanzar/personas/compliance/index.cshtml#:~:text=El%20Compliance%2C%20o%20cumplimiento%20normativo,a%20su%20sector%20y%20contexto.

Empresa. 2025. *Sitio Oficial de la empresa.* "Organización Interna." Madrid.

Ionos Digital Guide. 2023. "¿Qué es SaltStack?" *Ionos Digital Guide.* https://www.ionos.es/digitalguide/servidores/configuracion/que-es-saltstack/.

La Real Academia Española. 2025. *Diccionarios.* https://www.rae.es/.

International Organization Standardization - International Electrotechnical Commission. n.d. "ISO/IEC 27001:2022 Tecnología de la información — Técnicas de seguridad. Sistemas de gestión de la seguridad de la información. Requisitos."

International Organization for Standardization (ISO) - International Electrotechnical Commission (IEC). 2022. *ISO/IEC 27001:2022 Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de la Seguridad de la Información. Requisitos.* ISO.

International Organization for Standardization (ISO) - International Electrotechnical Commission (IEC). 2022. *ISO/IEC 27000:2022 Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de la Seguridad de la Información. Visión General y Vocabulario.* ISO.

Europea, Diario Oficial de la Unión. 2018. "Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos." BOE, Diciembre.

Anexo

Encuesta

Se realizó un muestreo probabilístico estratificado por áreas dentro de la empresa. La encuesta ha sido dividida en siete secciones, en las cuales se realizaron preguntas para responder como Si – No – No sabe/No contesta y un espacio en caso de que quisiera hacer algún comentario.

Preguntas por sección

Sección 1: Conocimientos Generales del SGSI

- ¿Sabes si la empresa cuenta con un Sistema de Gestión de Seguridad de la Información (SGSI)?
- ¿Conoces el propósito o los objetivos principales del SGSI?
- ¿Sabes qué significa la certificación ISO/IEC 27001 y por qué es importante para la empresa?
- ¿Has recibido información o capacitación sobre el SGSI o la Política de Seguridad de la Información?

Sección 2: Política y Alcance de Seguridad

- ¿Conoces la Política de Seguridad de la Información de la empresa?
- ¿Sabes dónde consultar la Política y los procedimientos de seguridad?
- ¿Has recibido información o capacitación sobre seguridad de la información en el último año?
- ¿Entiendes cómo se aplica la Política de Seguridad en tus tareas diarias?

- ¿Están claramente definidas las responsabilidades en materia de seguridad dentro de tu área?
- ¿Has recibido instrucciones claras sobre cómo proteger la información que manejas?

Sección 3: Gestión de Riesgos

- ¿Sabes qué hacer en caso de detectar una brecha o incidente de seguridad?
- ¿Te sientes capacitado para identificar riesgos de seguridad en tu trabajo diario?
- ¿Conoces qué tipos de riesgos de seguridad de la información existen en tu trabajo?
- ¿Participas o sabes si se realizan evaluaciones periódicas de riesgos de seguridad en la empresa?
- ¿Conoces si existen controles específicos (tecnológicos o administrativos) para proteger los activos de información? ¿Conoces el procedimiento que se sigue para tratar o mitigar los riesgos identificados?
- ¿Sabes si la empresa cumple con leyes o regulaciones sobre protección de datos y seguridad de la información? ¿Cómo?
- ¿Sabes si se mantiene información documentada sobre las evaluaciones y tratamientos de riesgos?
- ¿Consideras que la empresa toma acciones cuando identifica riesgos o incidentes?

Sección 4: Responsabilidades, Competencias y Recursos

- ¿Consideras que las responsabilidades relacionadas con la seguridad de la información están claramente asignadas en la empresa?
- ¿Cuentas con la formación o capacitación necesaria para proteger la información según tu rol?
- ¿La empresa conserva evidencia de la formación, experiencia o competencias del personal?

- ¿Se evalúa tu desempeño o el de tu equipo en relación con la seguridad de la información?
- ¿Dispones de los recursos necesarios (herramientas, tiempo, soporte) para cumplir con las medidas de seguridad?

Sección 5: Concientización y Cultura de Seguridad

- ¿Has participado en actividades de capacitación o concientización sobre seguridad de la información?
- ¿Consideras útiles las capacitaciones o materiales sobre seguridad que has recibido?
- ¿Te gustaría recibir más formación sobre temas de seguridad de la información?
- ¿Conoces las consecuencias o sanciones si alguien incumple las normas de seguridad?
- ¿Crees que la empresa promueve una cultura de seguridad entre sus empleados?
- ¿Conoces los canales internos para comunicar incidencias o sugerencias sobre seguridad?
- ¿Sientes que la dirección demuestra compromiso con la seguridad de la información?
- ¿Te informan sobre los resultados o mejoras relacionadas con la seguridad en la empresa?
- ¿Sabes si existen auditorías o revisiones internas sobre seguridad de la información?
- ¿Consideras que la empresa mejora continuamente sus medidas de seguridad?

Sección 6: Documentación y Control

- ¿Sabes qué documentos de seguridad son relevantes para tu puesto (políticas, procedimientos, manuales, etc.)?
- ¿Tienes acceso a la información necesaria para realizar tus tareas de manera segura?
- ¿Sabes quién es responsable de aprobar o actualizar los documentos de seguridad?

- ¿Conoces las medidas que se toman para proteger la información (contraseñas, accesos, *backups*, etc.)?
- ¿Cómo calificarías el nivel general de seguridad de la información en la empresa? (1 = Muy bajo – 5 = Excelente)

Sección 7: Preguntas Abiertas

- ¿Has tenido alguna situación en la que la seguridad de la información se haya visto comprometida? (sin mencionar datos confidenciales)
- ¿Qué sugerencias harías para mejorar la seguridad de la información en tu área?

Perfil de los Encuestados

1. Alta Dirección

La misión de la alta dirección es definir el rumbo estratégico de la organización, asegurando la coherencia entre la visión a largo plazo y la ejecución operativa. Su rol es fundamental para establecer la cultura organizacional basada en la libertad y la responsabilidad, facilitando los recursos necesarios para que cada área alcance su máximo potencial.

Esto incluye la toma de decisiones críticas, la gestión de relaciones institucionales y la supervisión del cumplimiento de los objetivos globales de la empresa. Además, actúa como el facilitador principal para eliminar barreras sistémicas, promoviendo un entorno de innovación y mejora continua. Su liderazgo no se basa en el control directo, sino en la inspiración y el diseño de un ecosistema que permita el crecimiento sostenible y la adaptabilidad ante los cambios del mercado.

2. Administración Financiera

Dentro de la misión del responsable financiero es asegurar una gestión financiera y administrativa integral, manteniendo la salud financiera de la empresa y cumpliendo con todas las obligaciones legales y fiscales.

Esto incluye la administración general, contabilidad, facturación, cobros y gestión fiscal, entre otras responsabilidades.

Su rol es clave para la estabilidad y el crecimiento sostenible de la empresa, proporcionando datos financieros precisos y asesoramiento estratégico a la dirección.

3. Líder Técnico

La misión del líder técnico es guiar al equipo de desarrollo de un área funcional en la implementación de soluciones técnicas, asegurar la calidad del código y la arquitectura del sistema, y mentorizar al equipo en las buenas prácticas de desarrollo.

4. Capital Humano

Gestiona de manera integral todos los aspectos relacionados con el capital humano de la empresa y su misión es alinear las prácticas del área con los objetivos estratégicos de la empresa.

Esto incluye atraer y seleccionar el talento adecuado, gestionar la incorporación y el desarrollo de los empleados, y velar por su bienestar y motivación. También implica diseñar y ejecutar políticas de compensación y beneficios, promover una cultura organizacional positiva, y asegurar el cumplimiento de normativas laborales. Además, debe facilitar la comunicación interna y actuar como enlace entre los empleados y la dirección para alinear los objetivos del personal con los estratégicos de la empresa.

5. Colaborador Funcional

Es el especialista funcional que asegura la continuidad operativa de los clientes ya implantados. Es el primer punto de contacto para resolver dudas, incidencias y tareas de mantenimiento evolutivo.

Dentro de algunas responsabilidades destacadas podemos mencionar la de resolver incidencias y consultas funcionales día a día, ejecutar tareas de mantenimiento evolutivo en los paquetes de su área, mantener actualizada la documentación funcional de los clientes, entre otras.

Resumen Normativo y Marco de Referencia para el Análisis de Brecha

Este resumen constituye la base legal utilizada para evaluar el nivel de cumplimiento de la organización objeto de estudio. Se centra en el Reglamento (UE) 2016/679 (RGPD) y la Ley Orgánica 3/2018 (LOPDGDD) de España, normativas que rigen el tratamiento de datos personales en el territorio donde opera la empresa. (Europea 2018)

1. Tabla de artículos clave y aplicación en el análisis de brecha

La siguiente tabla resume los artículos que actúan como "punto de control" para determinar las carencias documentales y procedimentales detectadas en la empresa.

Artículo (RGPD/LOPDGDD)	Requisito normativo principal	Aplicación en el Análisis de Brecha
Art. 5: Principios del tratamiento	Exige licitud, lealtad, transparencia, minimización de datos e integridad y confidencialidad	Evalúa si las prácticas actuales (ej. anonimización aislada) son suficientes o si existe riesgo de incumplimiento por falta de gobernanza transversal
Art. 6: Licitud del tratamiento	El tratamiento debe basarse en el consentimiento, ejecución de contrato o interés legítimo	Sirve para verificar si los contratos con clientes de ERP y B2B contemplan adecuadamente las bases legales de tratamiento

Art. 30: Registro de actividades de tratamiento (RAT)	Obligación de mantener un registro documentado de los fines, categorías de datos y destinatarios	Identifica la brecha documental, dado que la empresa tiene información dispersa y no cuenta con un RAT formalizado
Art. 32: Seguridad del tratamiento	Exige la aplicación de medidas técnicas y organizativas para garantizar la resiliencia	Contrasta la falta de un SGSI formal con la exigencia legal de medidas de seguridad adecuadas al riesgo detectado
Art. 33 y 34: Notificación de brechas de seguridad	Obliga a notificar violaciones de seguridad a la autoridad y a los interesados en caso de alto riesgo	Evalúa la carencia de planes de respuesta ante incidentes, ya que la gestión de riesgos en la empresa es actualmente reactiva
Art. 35: Evaluación de Impacto (EIPD)	Requerida cuando el tratamiento, por su naturaleza o tecnología, entrañe un alto riesgo	Se utiliza para analizar si la empresa ha evaluado los riesgos del uso de nuevas tecnologías como la IA en su software

2. Requisitos prácticos identificados para el caso de estudio

De acuerdo con la normativa citada, el análisis de brecha se ha enfocado en los siguientes requisitos prácticos obligatorios:

Gestión del consentimiento e información: el RGPD exige que el consentimiento sea una manifestación de voluntad libre, específica e informada. En la empresa, se ha evaluado la falta de una política interna clara que informe al personal y a los clientes sobre el tratamiento de sus activos de información.

Formalización documental: la normativa impone la obligación de demostrar la conformidad (responsabilidad proactiva). La ausencia detectada de un manual de procedimientos y de roles definidos constituye una brecha directa frente a la capacidad de auditoría exigida por la ley.

Medidas organizativas y concientización: el RGPD no solo exige herramientas técnicas, sino también capacitación del personal. El análisis GAP revela que la formación actual es voluntaria y escasa, lo que representa una vulnerabilidad operativa significativa frente a amenazas como el phishing.