# Universidad de Buenos Aires

Facultad de Ciencias Económicas, Ciencias Exactas y Naturales e Ingeniería


*Carrera de Especialización en*

## SEGURIDAD INFORMÁTICA

# TRABAJO FINAL

**Título:**

"Implementación de un **Sistema de Gestión** Integrado que cumple requisitos de **Seguridad de la Información**, en empresa comercial situada en el noroeste argentino"

**Autor**: Marcelo Adrián García

**Tutor**: Mara Irene Mismo Macías

*Marzo 2022*

**- Cohorte 2021 -**

## Declaración Jurada del origen de los contenidos

Por medio de la presente, el autor manifiesta conocer y aceptar el “Reglamento de Trabajos Finales” vigente y se hace responsable que la totalidad de los contenidos del presente documento son originales y de su creación exclusiva, o bien pertenecen a terceros u otras fuentes, que han sido adecuadamente referenciados y cuya inclusión no infringe la legislación Nacional e Internacional de Propiedad Intelectual.

“FIRMADO”

_____

**Marcelo Adrián García**

DNI 35.657.667

# Resumen

La información de una organización constituye un activo valioso y vulnerable. Un ataque puede comprometerla total o parcialmente y afectar su disponibilidad, integridad y/o confidencialidad, causando retrasos y un alto costo económico y reputacional para la compañía. Es por lo que la implementación de un Sistema de Gestión de Seguridad de la Información (SGSI) contribuiría con el propósito de proteger la información y los activos informáticos relacionados.

El objetivo de este trabajo es efectuar una observación del estado actual del Sistema de Gestión (SG), certificado por IRAM – ISO 9001 en calidad (SGC), de una empresa dedicada a la comercialización de productos químicos para la industria, ubicada en la provincia de Tucumán, Argentina. A partir de esta primera evaluación, se realizará un estudio de tipo explicativo y descriptivo, analizando los requerimientos que adicionalmente debería cumplir la organización para certificar su SG en el marco de ISO 27001 (requisitos para la implementación de un SGSI).

Cabe destacar, que las normas mencionadas cuentan con una estructura de alto nivel con apartados de títulos idénticos, términos comunes y, entre otros, definiciones esenciales indicadas en el anexo SL de la Directiva ISO/IEC, parte 1, "*Consolidated ISO Supplement*", lo que hace que su implementación conjunta sea compatible.

La puesta en marcha de un sistema de gestión que cumpla simultáneamente con requerimientos de Calidad y Seguridad de la Información se presenta como una propuesta factible para la entidad objeto de estudio, que contribuiría a la mejora continua de sus procesos de negocio y al aumento de su patrimonio para sus accionistas.



**Palabras Clave**: Sistema de Gestión, Seguridad de la Información, Framework, ISO

# Tabla de Contenidos

# Tabla de Ilustraciones

# 1 Marco Teórico

## 1.1 Introducción

El objetivo de este capítulo es definir y entender en su dimensión teórica, el concepto de gestión estratégica de la seguridad de la información, identificando su relevancia en el campo de la ciencia de la Administración.

Luego de haber efectuado un relevamiento de bibliografía y un análisis de marcos de cumplimiento afines, a continuación, se desarrolla un cuerpo teórico que versa sobre los principales postulados y problemáticas que plantea esta disciplina en relación a los SGSI.

## 1.2 Activos de la Información

La Resolución Técnica Nº 16 de la Federación Argentina de Consejos Profesionales de Ciencias Económicas (FACPCE) titulada “Marco Conceptual de las Normas Contables Profesionales”, en el texto que hace referencia a los “Activos”, establece que “un ente tiene un activo cuando debido a un hecho ya ocurrido, controla los beneficios económicos que produce un bien (material o inmaterial con valor de cambio o de uso…)” (p. 6). Y prosigue indicando que “se considera que algo tiene valor para una organización cuando representa fondos, equivalentes de este o tiene aptitud para generarlos (por sí o en combinación con otros bienes)” (FACPCE, 2002, pág. 6).

Si definimos el término activo, como todo aquello que tiene valor para una organización por su capacidad para generar futuros flujos de fondos o equivalente, podríamos decir por analogía que el concepto de “activo de información” hace referencia a la información valiosa y necesaria para el giro normal del negocio y toda aquella infraestructura que la contiene. En otras palabras, es cualquier información o sistema relacionado con su tratamiento que posea valor para la organización, por lo que es de esperar que sea susceptible de ataques intencionales o accidentales, pudiendo originar consecuencias económicas, legales o reputacionales para la organización.

En el glosario de términos de ciberseguridad, una guía de aproximación para el empresario, publicado por Instituto Nacional de Ciberseguridad del Gobierno de España, se define el término “activo de Información”, de la siguiente manera:

> *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, 2021, pág. 12).

La valuación de estos activos de información depende de las particularidades del negocio y de sus necesidades concretas. Esta valoración determinará los tipos de controles y las pruebas sustantivas necesarias para garantizar su seguridad.

Es por esto que resulta importante clasificar e identificar aquella que es más relevante para llevar a cabo la misión organizacional. De esta manera, los responsables de la gestión del negocio deberán tener presente cuales son los principales activos que deben proteger.

Por otra parte, cuando nos referimos a información no solo implica aquella que se encuentra en formato papel o electrónico, sino también a otras formas como ser fotografías, cintas de audio, material digital, etc. Es decir, que la protección de la información es independiente al soporte de su formato y que la misma puede realizarse a través de adecuados controles físicos y/o lógicos.

A modo de ejemplo se transcribe el copete de una nota sobre la temática, escrita en la revista "*Infotechnology":*

> *En el último tiempo la industria sanitaria se ha convertido en una de las más vulnerables frente a los ataques cibernéticos ¿Qué tiene el sector que la convierte en el objetivo preferido de los atacantes? La respuesta es contundente: el valor de la información que manejan es alto y su precio pagado en el mercado negro* (Bravo, Año 22, N° 252, pág. 20).

## 1.3 Seguridad de la Información

El Instituto Nacional de Ciberseguridad del gobierno de España, en su plataforma web define a la Seguridad de la Información como “el conjunto de medidas aplicadas para la protección de los activos de la información” (INCIBE, 2021). Esta es una enunciación que resume sencillamente lo que implica este concepto, sin embargo, es importante destacar que la seguridad de la información es un concepto más amplio que el de la seguridad de los recursos informáticos, pues tiene como objetivo proteger la información de los diversos riesgos que pueden afectarla, en sus diferentes formas y estados.

Otra definición al respecto, nos la ofrece Baca Urbina y en la cual reza que,

> *La seguridad informática es la disciplina que, con base en políticas y normas internas y externas de la organización, se encarga de proteger la integridad y privacidad de la información que se encuentra almacenada en un sistema informático, contra cualquier tipo de amenazas, minimizando los riesgos tanto físicos como lógicos, a los que está expuesta* (Baca Urbina, 2016, pág. 12)*.*

En este sentido, la Seguridad de la Información involucra todo lo referido a la preservación de la confidencialidad, integridad y disponibilidad de la información; además pueden estar involucradas otras propiedades como la autenticidad, responsabilidad, no-repudio y confiabilidad.

La norma ISO 27000, que desarrolla la descripción y el vocabulario a utilizar para la implementación de un Sistema de Gestión de seguridad de la información, define al término abordado en este apartado de la siguiente manera:

> *La seguridad de la información garantiza la confidencialidad, disponibilidad e integridad de la información. Involucra la aplicación y gestión de controles apropiados que implican la consideración de una amplia gama de amenazas, con el objetivo de garantizar el éxito y la*

*continuidad sostenida del negocio y minimizar las consecuencias de los incidentes de seguridad de la información.*

*(…) se logra mediante la implementación de un conjunto de controles aplicables, seleccionados a través del proceso de gestión de riesgos elegido y gestionados mediante un SGSI, que incluye políticas, procesos, procedimientos, estructuras organizativas, software y hardware para proteger los activos de información identificados. Estos controles deben especificarse, implementarse, monitorearse, revisarse y mejorarse cuando sea necesario, para garantizar que se cumplan los objetivos del negocio y de seguridad de la información específicos de la organización. Se espera que los controles de seguridad de la información relevantes se integren a la perfección con los procesos comerciales de una organización* (ISO/IEC 27000, 2014).

Por otra parte, Laudon & Laudon define a la seguridad como “las políticas, procedimientos y medidas técnicas que se utilizan para evitar el acceso sin autorización, la alteración, el robo o el daño físico, a los sistemas de información” (Laudon, 2016).

Respecto a esta definición, cuando el autor hace referencia a "políticas", debería utilizar un término más apropiado. En este aspecto, indicaría que se refiere al planeamiento estratégico de la organización y al apetito al riesgo considerado aceptable. Esta estrategia debe diseñarse en base a una adecuada evaluación del negocio y su contexto. A partir de ella, no sólo surgirán políticas, sino que también se deberán diseñar objetivos y metas e implementar programas y planes acordes. Además, la estructura organizacional se deberá adecuar para acompañar esta visión corporativa.

En segundo lugar, el término "procedimientos", podría cambiarse por aspectos relacionados a la "ejecución de la estrategia" y el "cómo" se cumplirán los objetivos y las metas propuestas.

En cuanto a "medidas técnicas", se utiliza un término bastante restrictivo, pues existen otras actividades como ser la concientización. La seguridad no es únicamente un inconveniente técnico, sino que es un problema de negocios, en el que se debe invertir recursos para asegurar la continuidad del mismo.

Por otra parte, el concepto de Seguridad Informática aporta elementos que se están volviendo indispensables en la gestión empresarial y obliga a permanecer alerta ante la presencia de un entorno inseguro si no se toman las precauciones necesarias. Según manifiesta Lardent “las nuevas herramientas de comunicación crean nuevas soluciones, pero también generan nuevos problemas que son necesarios preverlos, detectarlos y solucionarlos” (Lardent, 2001, pág. 227).

Actualmente, las organizaciones deben asegurar su información, la cual en la mayoría de los casos no se encuentra físicamente, sino que está almacenada en formato digital, alojada en medios tecnológicos, pudiéndose encontrar dentro o fuera de las instalaciones de la compañía y en muchos casos, desconociéndose la ubicación exacta de ella, pues se encuentran en la nube. A todo esto, se le suman las amenazas cibernéticas que evolucionan diariamente y a una mayor velocidad que las salvaguardas para mitigarlas.

La doctrina actual de la disciplina está de acuerdo en que la seguridad de la información se basa en articular y asegurar tres propiedades:

- Confidencialidad: garantiza que la información estará accesible únicamente al personal autorizado a acceder a ella (INCIBE, 2021, pág. 29). Esta característica no debe ser confundida con la “privacidad”, relacionada con la protección de la asociación de la identidad de los usuarios y sus actividades.
- Integridad: es la propiedad por la que se garantiza la exactitud de los datos transportados o almacenados, asegurando que no se produjo su alteración, pérdida o destrucción, ya sea de forma accidental o intencionada, por errores de software, hardware o por condiciones medioambientales (INCIBE, 2021, pág. 51). Es decir que asegura que los datos no hayan sido manipulados o modificados sin la correspondiente autorización.
- Disponibilidad: se trata de la capacidad de un servicio, un sistema o una información, de ser accesible y utilizable por los usuarios o procesos autorizados cuando éstos lo requieran (INCIBE, 2021, pág. 37). Esta característica de la información es la única que se relaciona con el factor tiempo.

## 1.4 Relación de la Seguridad de la Información con la Administración

De manera genérica, podríamos definir qué Administración es la ciencia social que tiene por objeto el estudio de las organizaciones y la técnica encargada de la planificación, organización, dirección y control de sus recursos, con el fin de obtener el máximo beneficio posible, pudiendo este ser social o económico, dependiendo de los fines perseguidos por el ente (Gestion.org, s.f.). Es decir que esta disciplina, hace énfasis en las organizaciones y en los recursos que la componen, entre estos, como ya se ha plasmado anteriormente, la información.

Como cualquier otro activo, la información otorga valor a la compañía, por lo tanto, debe ser resguardada de las amenazas que pudiera sufrir.

En este sentido, cobra significativa importancia el concepto de "Seguridad de la Información", la cual se encarga de proteger la integridad, disponibilidad y confidencialidad de la información, contra cualquier tipo de amenaza, minimizando los riesgos a los que estuviera expuesta. Esto posibilita, por lo tanto, el normal desenvolvimiento de las actividades del negocio y el cumplimiento de su misión corporativa.

El objetivo de la seguridad informática no solo consiste en prevenir los riesgos y potenciales ataques internos, externos, físicos y lógicos, sino también se encarga del diseño e implementación de los planes de recuperación en caso de haberse concretado daños. Este método se relaciona estrechamente con la continuidad del negocio, aspecto estrictamente necesario para la labor profesional de la administración.

## 1.5 Sistema de Gestión. Conceptualización

Un sistema de gestión es una herramienta que le permite a las organizaciones obtener un óptimo y ordenado desempeño, mejorando de este modo su posicionamiento en el mercado. Además, constituye una importante fuente de información, para profesionales de cualquier actividad económica. En él se establece la estructura, los roles y responsabilidades, una adecuada planificación, operación, políticas y reglas. Asimismo, se definen las creencias, objetivos y procesos necesarios para lograr las metas establecidas en la estrategia corporativa.

## 1.6 Sistema de Gestión de Seguridad de la Información

### *1.6.1 Definición.*

Un SGSI es el proceso sistémico, documentado y conocido por toda la organización que posibilita que la seguridad de la información sea gestionada adecuadamente. Está compuesto por un conjunto de políticas, procedimientos, directrices, recursos y actividades asociadas y colectivamente gestionadas con el propósito de proteger sus activos de información. Parte de una evaluación de riesgos relacionados con la información y sus niveles de aceptación. Incluye un análisis de los requisitos y la aplicación de controles adecuados para proteger los activos de información, a través de un ciclo de mejora continua.

El glosario de términos de ciberseguridad de INCIBE, por su parte indica que,

> *Un Sistema de Gestión de Seguridad de la Información 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, 2021, pág. 69).

Un SGSI resguarda la confidencialidad, integridad y disponibilidad de la información a través de la implementación de un proceso de gestión de riesgos, otorgando de este modo, confianza a las partes interesadas. Su ejecución es estratégica y debe integrarse con los procesos de negocio de la organización. Es decir que la seguridad de la información debe tenerse en cuenta al efectuarse el diseño de los procesos organizacionales, los sistemas informáticos y los controles. Estos últimos se irán adaptando conforme a las necesidades de la organización (ISO/IEC 27001, 2013, pág. 7).

La norma ISO 27000 indica que la implementación de un SGSI, contribuye a que el ente pueda alcanzar los siguientes elementos:

a) satisfacer los requisitos de seguridad de la información de los clientes y otras partes interesadas;

b) mejorar los planes y actividades de una organización;

c) cumplir con los objetivos de seguridad de la información de la organización;

d) cumplir con las regulaciones, la legislación y los mandatos de la industria; y

e) administrar los activos de información de una manera organizada que facilite la mejora continua y el ajuste a los objetivos organizacionales actuales (ISO/IEC 27000, 2014, pág. 13).

### *1.6.2 Controles para la Seguridad de la Información.*

Las organizaciones de todo tipo y tamaño recopilan, procesan, almacenan y transmiten información en muchos formatos, incluyendo electrónico, físico y verbal.

En un mundo interconectado, la información y los procesos son valiosos para el negocio de la organización y, por lo tanto, precisan una adecuada protección contra distintos peligros.

Los activos están sujetos a amenazas intencionales y/o accidentales. Los procesos, sistemas, redes y personas poseen vulnerabilidades inherentes. Por lo tanto, dada la variedad de formas en las cuales las amenazas pueden aprovechar las vulnerabilidades para perjudicar a la compañía, siempre están presentes los riesgos respecto de la seguridad de la información. Una seguridad eficaz reduce estos riesgos y, en consecuencia, disminuye el impacto sobre sus activos.

La Seguridad de la Información se alcanza implementando un conjunto adecuado de controles, que incluyen personas, políticas, procesos, procedimientos, estructuras organizativas y funciones de software y hardware. Es necesario que estos se establezcan, implementen, monitoreen, revisen y mejoren, si corresponde, para garantizar que se cumplan los objetivos del negocio y, en esa línea, los específicos de seguridad.

Actualmente, en base a las amenazas existentes, la seguridad que se puede lograr por medios tecnológicos debe ser reforzada con una gestión y procedimientos apropiados, sumando a la personas y procesos en la ecuación.

### *1.6.3 Norma ISO/IEC 27001.*

Este marco de cumplimiento se elaboró con el fin de abordar los requisitos para el establecimiento, implementación, mantenimiento y mejora continua del Sistema de Gestión de Seguridad de la Información en el contexto de los riesgos de negocio de la organización. Su establecimiento está relacionado con las necesidades y objetivos de la organización, sus procesos, tamaño y estructura, los cuales cambiarán con el paso del tiempo.

Todas las organizaciones pueden utilizar como base para la implementación de un SGSI los requisitos que plantea ISO / IEC 27001, independientemente de su tipo, tamaño y naturaleza.

## 1.7 Evaluación de la Seguridad de la Información

La seguridad de la información no es un producto o servicio que pueda adquirirse. Es un proceso continuo que debe afianzarse en la cultura organizacional.

Las empresas están conformadas por capital humano (colaboradores), quienes interactúan con otras personas, procesos, recursos y tecnología. Estos son considerados el punto más débil en la cadena de la seguridad de la información (o la primera línea de defensa).

En el proceso de implementación de un SGSI, es fundamental contar con una sólida cultura de seguridad, para evitar la resistencia en los usuarios con relación a las políticas y controles a aplicar.

Generalmente, en primer lugar, se busca cambiar la percepción de los beneficios y la necesidad de contar con un SGSI a través de la participación, asignación de recursos y la concientización (término en inglés: "*awareness"*).

## 1.8 Alcance de la Seguridad de la Información

La seguridad de la información involucra a tres elementos que están presentes en todo tipo de organizaciones: las tecnologías, los procesos y el capital humano. Estos deben funcionar de manera conjunta y coordinada.

Con el concepto de tecnología se hace referencia a las medidas técnicas de protección que van a utilizarse. Ejemplos de ello serían: productos y herramientas de seguridad o métodos de encriptación a utilizar, entre otros.

En cuanto a los procesos, son aquellos que examinan la correcta labor interrelacionada entre las tecnologías y el capital humano.

Finalmente, el capital humano son las personas que manipulan y utilizan la tecnología e intervienen en los procesos.

## 1.9 Diseño e Implementación de un SGSI

El diseño y la implementación de un Sistema de Gestión de Seguridad de la Información dependerá de los objetivos y las necesidades del negocio. Es decir, debe tenerse en cuenta cuestiones como aspectos de seguridad de la información requeridas, los procedimientos operativos, el tamaño y la estructura de la organización, entre otros.

En este apartado se hace hincapié en que los sistemas de soporte a las operaciones del negocio, en general, deberían adaptarse al contexto. Por lo tanto, correspondería que el diseño del SGSI acompañe a los cambios del entorno, las prioridades y los riesgos que esto produzca, en línea con las adecuaciones necesarias para dar respuesta a las nuevas condiciones del mercado y a las necesidades informadas por la dirección de la organización.

En este sentido, cobra relevancia el “Ciclo de Deming”, también conocido como PDCA, por su sigla en inglés “*plan, do, check, act*”, que en español significa “planificar, hacer, verificar y actuar”. Asimismo, este concepto es conocido como “espiral de mejora continua”, el cuál es ampliamente utilizado en sistemas de gestión de calidad, ambiental y seguridad de la información, regulados por el marco de referencia ISO (Wikipedia, 2021).


*Ilustración 1: Ciclo de Deming*

Teniendo en cuenta el objeto del presente trabajo, se presenta el Ciclo de Deming" adaptado a un Sistema de Gestión de Seguridad de la Información:

- Planificar: se refiere a establecer los documentos y acciones necesarios en un SGSI. Entre ellos, se encuentran los siguientes,
  - Definición de la política y los objetivos generales de la seguridad de la información
  - Realización del análisis de riesgo y de impacto en el negocio ("*Business Impact Analysis*" - BIA), con la finalidad de definir las prioridades
  - Establecimiento de las prioridades y el alcance del SGSI
  - Selección de los controles aplicables teniendo en cuenta el "Anexo A" de la norma ISO 27001
  - Determinación de las competencias requeridas por el capital humano, autoridades y sus respectivas responsabilidades
  - Diseño de indicadores de gestión y métricas de seguridad para el seguimiento del avance.
- Hacer: implica todo aquello que está relacionado a la implementación y operación del SGSI. En este aspecto es necesaria la ejecución y operación de la Política de Seguridad, controles, procesos, procedimientos, métricas, etc.
- Verificar**:** hace referencia al seguimiento y reconocimiento del SGSI. Es decir, la inspección del sistema de gestión, la planificación, ejecución de auditorías internas y el chequeo de los indicadores de gestión y métricas de seguridad contra los objetivos planificados. Se espera una revisión periódica por parte de la Dirección para verificar el cumplimiento de los objetivos de gestión.
- Actuar**:** a partir de los resultados de la fase anterior, es decir el análisis de la brecha entre los objetivos pretendidos y lo realmente logrado, se procede a recopilar lo aprendido, para la confección de acciones correctivas y mejoras necesarias. Se analizan nuevos riesgos o vulnerabilidades, se ajustan los objetivos y se adaptan las medidas y controles. Estas brechas derivan de la

auditoría interna o externa, la revisión por parte de la Dirección, revisiones propias o cualquier otra información relevante.

### 1.10 Requisitos

Para alcanzar el objetivo de cumplimiento, en primer lugar, deben conocerse los requerimientos y sus respectivas fuentes, para poder de este modo, mapearlos y planificar el SGSI. Ellos tienen los siguientes orígenes:

- Requisitos especificados por el marco de cumplimiento ISO 27001
- Otros marcos de trabajo o estándares complementarios, como, por ejemplo: NIST, ISA, CISS, CRA, *Carnegie Mellon*, etc.
- Exigencias no establecidas en la norma antes mencionada, pero necesarios para el desempeño esperado. Este apartado alude a normativas propias de la organización
- Requisitos legales y regulatorios asociados al contexto o a la actividad en particular

### 1.11 Responsabilidades de la Dirección

Se espera que la dirección demuestre liderazgo y compromiso con respecto al SGSI (ISO/IEC 27001, 2013, pág. 9):

Entre las actividades principales relacionadas a la dirección del sistema de gestión, se destacan a continuación las siguientes:

- Establecimiento de los objetivos y el alcance de la organización para alinearlos al SGSI
- Creación de la Política de Seguridad de la Información
- Determinación de roles y responsabilidades del Capital Humano
- Impulsar la concientización y capacitación del personal en el ámbito de la Seguridad de la Información
- Asignación de los recursos necesarios para alcanzar los objetivos esperados
- Fijación de los criterios para la aceptación del riesgo y el umbral aceptable (apetito al riesgo)
- Revisión periódica de SGSI en lo relacionado a los objetivos de gestión

- Aseguramiento de las condiciones necesarias para la realización de auditorías internas
- Promoción de las acciones pertinentes para lograr la mejora continua

## 1.12 Requisitos de Documentación de ISO / IEC 27001

El SGSI de la organización debe incluir la información documentada requerida por la norma y aquella que sea considerada necesaria para lograr su eficacia. “El grado de documentación puede variar entre entidades a causa del tamaño, nivel de actividad, complejidad de los procedimientos y la competencia del capital humano que interviene” (ISO/IEC 27001, 2013, pág. 14). La misma debe estar disponible y apta para su uso cuando se la requiera y adecuadamente protegida para mantener su debida confidencialidad e integridad.

La documentación del SGSI es necesaria por los siguientes aspectos:

- Efectuar un registro de decisiones de la dirección
- Atestiguar la trazabilidad de las acciones correctivas del sistema
- Gestionar adecuadamente el sistema de gestión del conocimiento
- Evidenciar que los resultados sean reproducibles

| DOCUMENTO | REQUISITO |
|---|---|
| Alcance del SGSI | 4.3 |
| Política de Seguridad de la Información | 5.2 |
| Evaluación del riesgo respecto a la seguridad de la información | 6.1.2 |
| Declaración de aplicabilidad | 6.1.3 (d) |
| Tratamiento de riesgos de seguridad | 6.1.3 |
| Objetivos de Seguridad de la Información y planificación | 6.2 |
| Registro de formación, habilidades, experiencia y calificaciones | 7.2 |
| Evaluación del riesgo a la seguridad de la información | 8.2 |
| Tratamiento del riesgo a la seguridad de la información | 8.3 |
| Resultados de monitoreo y medición | 9.1 |
| Programa y resultados de auditoría interna | 9.2 |
| Revisión por parte de la dirección | 9.3 |
| No conformidades y acciones correctivas | 10.1 |
| Documentación solicitada en los controles del "Anexo A" | |

*Ilustración 2: Requisitos de documentación de la norma ISO 27001*

## 1.13 Cuerpo normativo común entre ISO 27001 e ISO 9001

Los estándares ISO 27001:2013 e ISO 9001:2015 utilizan una estructura de cláusulas, términos comunes y requisitos, indicados en el anexo SL de la Directiva ISO/IEC, parte 1, *Consolidated ISO Supplement*, conocido como estructura común de alto nivel (por sus siglas en inglés "*High Level Structure"* - HLS), para los estándares de sistema de gestión. La adopción de HLS permite a una organización alinear e integrar múltiples estándares de sistemas de gestión. Según lo indica el informe ISO-IEC PDTR 20000-7, "la relación entre estos estándares es muy estrecha; por lo tanto, es posible que muchas organizaciones ya reconozcan los beneficios de adoptarlos conjuntamente". (ISO / IEC, 2018, pág. 6). Entre otros, se destacan los siguientes:

- Los costos de implementación de un sistema de gestión integrado son menores y los esfuerzos para mantenerlos actualizados se reducen
- Las partes interesadas (*stakeholders*) manifiestan un mayor grado de confiabilidad hacia la organización que posee un único sistema de gestión integrado
- Se puede evidenciar que los procesos de negocio son más efectivos y que existe una mejor comunicación en la organización, al acelerar la interacción entre procesos de calidad, seguridad de la información y su sistema de gestión.

Sin embargo, cabe destacar que un sistema de gestión integrado debe especificar qué cláusulas de cada estándar se están cumplimentando.

| N° | ESTRUCTURA DE ALTO NIVEL PARA LOS ESTÁNDARES DEL SG |
|---|---|
| **4** | **Contexto de la organización** |
| 4.1 | Comprensión de la organización y su contexto |
| 4.2 | Comprensión de las expectativas y las partes interesadas |
| 4.3 | Determinación del alcance del Sistema de Gestión de [xxx][1] |
| 4.4 | Sistema de Gestión de [xxx] |

*Ilustración 3: ISO-IEC PDTR 20000-7, p. 3*

[1] Léase "Calidad" en ISO 9001:2015 y "Seguridad de la Información" en ISO 27001:2013

| N° | ESTRUCTURA DE ALTO NIVEL PARA LOS ESTÁNDARES DEL SG |
|---|---|
| **5** | **Liderazgo** |
| 5.1 | Liderazgo y compromiso |
| 5.2 | Política |
| 5.3 | Roles, responsabilidades y autoridades en la organización |
| **6** | **Planificación** |
| 6.1 | Acciones para tratar los riesgos y oportunidades |
| 6.2 | Objetivos de [xxx] y planificación para lograrlos |
| **7** | **Soporte** |
| 7.1 | Recursos |
| 7.2 | Competencia |
| 7.3 | Concientización |
| 7.4 | Comunicación |
| 7.5 | Información documentada |
| **8** | **Operación** |
| 8.1 | Planificación y control operativo |
| **9** | **Evaluación de desempeño** |
| 9.1 | Seguimiento, medición, análisis y evaluación |
| 9.2 | Auditoría Interna |
| 9.3 | Revisión por parte de la Dirección |
| **10** | **Mejora** |
| 10.1 | No conformidad y acción correctiva |
| 10.2 | Mejora continua |

Ilustración 3: ISO-IEC PDTR 20000-7, p. 3

A continuación, se desarrolla un cuadro comparativo entre las normas ISO 9001 y 27001, mostrando cada una de sus cláusulas.

| Nº | ISO 9001:2015 | ISO 27001:2015 |
|---|---|---|
| 0 | Introducción | Introducción |
| 1 | Objeto y Campo de Aplicación | Objeto y Campo de Aplicación |
| 2 | Referencias Normativas | Documentos normativos para consulta |
| 3 | Términos y Definiciones | Términos y Definiciones |

*Ilustración 4: Estructura comparativa entre normas de Sistemas de Gestión*

| Nº | ISO 9001:2015 | ISO 27001:2015 |
|---|---|---|
| 4 | Contexto de la Organización | Contexto de la Organización |
| 5 | Liderazgo | Liderazgo |
| 6 | Planificación | Planificación |
| 7 | Apoyo | Soporte |
| 8 | Operación | Operación |
| 9 | Evaluación de Desempeño | Evaluación de Desempeño |
| 10 | Mejora | Mejora |
| **ANEXOS** | | |
| A | Aclaración de la nueva estructura, terminología y conceptos | Objetivos de control y controles de referencia |
| B | Otras normas internacionales sobre gestión de la calidad y sistemas de gestión de la calidad desarrollados por el comité técnico ISO / TC176 | Bibliografía |
| C | Bibliografía | Integrantes de los organismos de estudio |

*Ilustración 4: Estructura comparativa entre normas de Sistemas de Gestión*

# 2 Empresa objeto de estudio

## 2.1 Introducción

Teniendo en cuenta la información relevada de la organización objeto de estudio, en este capítulo se presentan sus características generales, con la finalidad de comprender de una manera acabada su sistema de gestión, cuyo estudio de tipo explicativo y descriptivo será desarrollado en la próxima sección.

## 2.2 Presentación de la empresa

Posicionada en la región centro y norte del país, el objeto social de la organización analizada es la comercialización y distribución de productos químicos para la Industria. La misma manifiesta en su sitio web ofrecer un servicio de calidad mediante una política de inversión permanente en estructura, capital humano, tecnología y buenas prácticas.

En Tafí Viejo, provincia de Tucumán, se encuentran sus oficinas administrativas y centro de distribución, equipado con depósitos especialmente diseñados para contener hipoclorito de sodio, ácido clorhídrico, ácido sulfúrico e hidróxido de sodio (soda cáustica), entre otros productos.

Todo su personal, tanto de planta como de logística, recibe permanente capacitación en manipulación, transporte y almacenaje de sustancias peligrosas, contemplando estrictas normas de seguridad.

Además, cuenta con un Sistema de Gestión de Calidad certificado IRAM/ISO 9001:2015, constituyendo una demostración más de su compromiso con la calidad y la mejora continua.

Se hace referencia a que cuenta con un departamento de calidad, compuesto por un laboratorio para el control y garantía de cumplimiento de las especificaciones técnicas de los productos, desde su origen hasta la entrega a sus clientes, asegurando su trazabilidad. El personal altamente capacitado, posee idoneidad y una vasta experiencia.

Asimismo, cuenta con una importante flota de vehículos de mediano y gran porte, especialmente equipados para el traslado de productos químicos a granel, cumpliendo con todas las reglamentaciones vigentes para el

transporte de cargas peligrosas. Las unidades cuentan con un sistema de seguimiento satelital en tiempo real, seguros de contingencia y servicio de remediación ante emergencias químicas.

## 2.3 Lineamientos Estratégicos

A continuación, se describe la misión, visión y valores de la empresa analizada, según los datos que se pudieron recabar:

### *2.3.1 Misión.*

“Somos una empresa dedicada a la comercialización y logística de productos químicos, comprometida con la mejora continua y persuadida que la calidad de nuestros productos, procesos y servicios son un aspecto fundamental para el crecimiento sustentable, logrando de este modo una total satisfacción de nuestros aliados estratégicos”.

### *2.3.2 Visión.*

“Ser la empresa líder en comercialización y logística de productos químicos de la región, reconocidos por nuestra orientación al cliente, cumpliendo con sus requerimientos de una manera ágil, segura y con altos estándares de calidad”.

### *2.3.3 Valores.*

La organización se compromete a trabajar con los siguientes valores, con el objeto de alcanzar su visión propuesta:

- Honestidad
- Responsabilidad
- Orientación al cliente
- Cumplimiento de requerimientos legales y regulatorios
- Crecimiento sustentable
- Compromiso con el medio ambiente

### *2.3.4 Política de Calidad.*

En este apartado, se desarrolla la “Política de Calidad” definida por la dirección de la empresa analizada:

“Somos conscientes que la Calidad de los productos que comercializamos y de los procesos y servicios que brindamos, son componentes claves para un crecimiento sostenido y sustentable, enfocados a una total satisfacción de nuestros aliados comerciales. Por lo tanto, establecemos como Política de Calidad los siguientes principios:

- Alcanzar la total satisfacción y fidelidad de nuestros clientes, disponiendo de la flexibilidad suficiente para adaptarnos a sus requisitos, en un contexto dinámico y competitivo.
- Comprometernos con la mejora continua de nuestros procesos, productos y servicios, logrando la eficacia en nuestro Sistema de Gestión de Calidad.
- Definir anualmente nuestros objetivos estratégicos de calidad, estableciendo prioridades e iniciando las acciones necesarias para la prevención, planificación, corrección y continua adecuación.
- Lograr la concientización, motivación y participación de nuestro capital humano en el Sistema de Gestión de Calidad, junto con la información y la formación necesaria para que el desarrollo de su actividad sea consecuente con la Política de Calidad, constituyendo su retroalimentación los cimientos de nuestro compromiso con la mejora continua.
- Cumplir con todos los requisitos legales y reglamentarios aplicables a los productos que comercializamos”.

## 2.4 Implementación de un Sistema de Gestión Integrado

Las organizaciones, en relación a su misión corporativa, deben orientar su gestión para poder mantener la satisfacción de cada uno de sus *stakeholders*. Para lograrlo se deben implementar y mantener sistemas de gestión eficaces y eficientes en el logro de sus objetivos, gestionados por personas calificadas para tal fin, y contar con el liderazgo de la alta dirección (IRAM, s.f.).

En este sentido, se hace referencia a que las buenas prácticas en gobierno corporativo aportan seguridad económica y jurídica, fomentando el crecimiento sostenible de las empresas (Deloitte, s.f.).

El gobierno corporativo es el conjunto de normas, principios y procedimientos que regulan la estructura y el funcionamiento de los órganos

de gobierno. Su correcto funcionamiento otorga credibilidad, estabilidad y favorece a estimular la generación de riqueza, haciendo corporaciones más competitivas.

Actualmente, quienes tienen a su cargo la dirección de una organización deben optimizar y fomentar el uso de tecnologías, tanto para la gestión como para la comunicación. Sin ella, se tornaría muy dificultosa la supervivencia en un mercado que requiere una presencia constante y una respuesta en tiempo real. Por lo tanto, la inversión en infraestructura tecnológica puede representar una proporción importante sobre las erogaciones de un ente, sobre todo, si se tienen en cuenta las implementaciones en materia de ciberseguridad (Arrarte, 2019).

En relación a este tema, toma importancia el gobierno corporativo de TI, que es el que gestiona los procesos relativos a los servicios de la información y comunicación. Para ello, se recomienda la utilización de estándares internacionales como ser COBIT, ITIL e ISO. Estos tres son los marcos de gobierno IT más reconocidos internacionalmente para gestionar las tareas relacionadas con la tecnología y la seguridad de la información, a nivel interno y con terceros. Cabe destacar que ninguno, por sí solo, cumple todos los procesos que implican el gobierno IT, pero tienen significativas fortalezas para ello y se complementan adecuadamente (Itgovernance, s.f.). Estos respaldan el cumplimiento de la misión corporativa y otorgan considerable importancia a la informática para alcanzar los objetivos propuestos. Asimismo, se abordan aspectos como ser: continuidad de negocios, recuperación ante desastres, gobierno corporativo, de la información y de seguridad de la información, gestión del conocimiento, cumplimiento normativo, liderazgo, gestión de proyectos y riesgos, entre otros.

El *framework* que presenta ISO 27001 es uno de los que cobró mayor relevancia en el último tiempo debido a la necesidad de seguridad de la información en corporaciones altamente informatizadas. En este caso, la empresa objeto de estudio tiene implementado un Sistema de Gestión de Calidad, por lo que lo más adecuado será implementar un “Sistema de Gestión Integrado” que cumpla simultáneamente con requisitos de Calidad y Seguridad de la Información. Las diferencias entre las normas

provechosamente se integran entre sí, lo cual contribuye positivamente a incrementar el éxito del negocio.

Se hace mención a que ambos marcos de cumplimiento poseen los siguientes requisitos en común: contexto, partes interesadas, responsabilidad de la dirección, competencia, concientización, comunicación, control documental, auditoría interna, revisión por la dirección, acciones correctivas y no conformidad.

Debe tenerse en cuenta que, si bien algunos requerimientos parecen iguales y pueden ser cubiertos con el mismo proceso, no significa que vayan a tener los mismos resultados para ambos estándares (Escuela Europea de Excelencia, 2016).

En definitiva, se considera que la puesta en marcha de un sistema de gestión con las características indicadas anteriormente, se presenta como una propuesta factible para la entidad analizada, agregando valor y contribuyendo a la mejora continua de sus procesos.

# 3 Requisitos para la implementación de un SGSI

## 3.1 Introducción

En el presente capítulo se efectúa una observación del estado actual del Sistema de Gestión, certificado por IRAM – ISO 9001 en calidad, de la empresa analizada. A partir de esta primera evaluación, se realizará un estudio de tipo explicativo y descriptivo, analizando los requerimientos que adicionalmente debería cumplir para certificar un "Sistema de Gestión Integrado" que satisfaga requerimientos del marco ISO 27001 (requisitos para la implementación de un SGSI).

## 3.2 Contexto de la Organización

Teniendo en cuenta la primera fase del "Ciclo de Deming", la cual implica "planificar", se hace referencia a que es importante inicialmente conocer a la organización y al contexto en el cual está inserta. Deben identificarse las necesidades y expectativas de las partes interesadas y el alcance y particularidades del SGSI.

### *3.2.1 Comprensión de la organización y su contexto.*

El apartado 4.1 de ISO 27001, establece que la entidad debe determinar los aspectos internos y externos que permiten explicar su posicionamiento en el mercado y las cuestiones que afectan su capacidad para lograr resultados esperados.

El análisis del contexto posibilitará detectar sistemáticamente las dificultades internas y externas e identificar aspectos a tener en cuenta en la gestión de riesgos.

Este marco de cumplimiento no especifica cómo cumplimentar este requisito, sin embargo, pueden optarse metodologías como, por ejemplo: FODA[2], PEST[3], PASTEL[4], cinco fuerzas de Porter[5], entre otros.

---

[2] Técnica utilizada para identificar fortalezas, oportunidades, debilidades y amenazas.

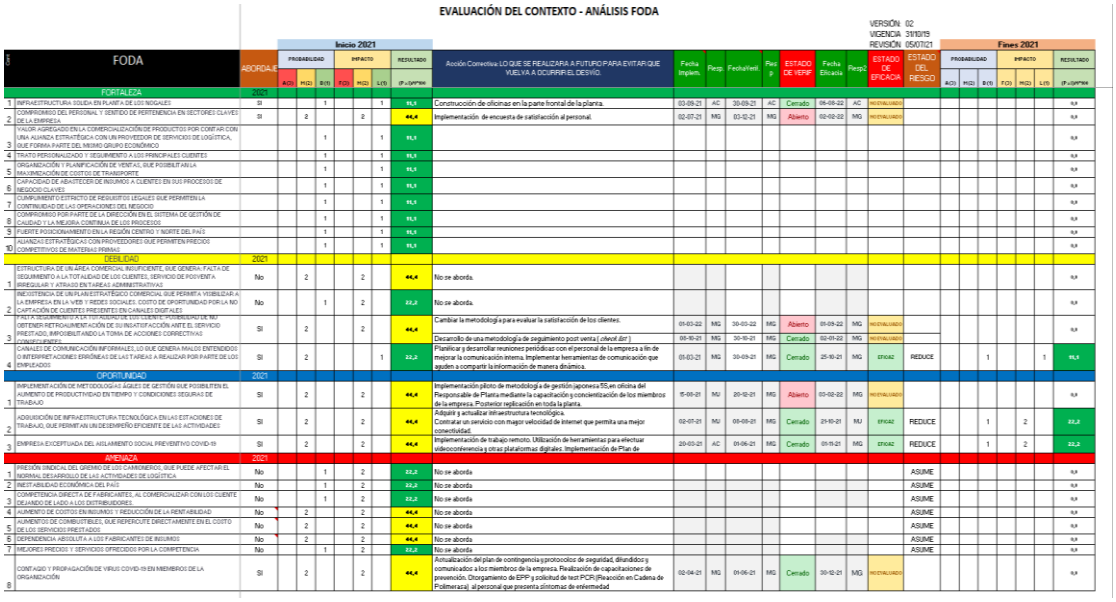
[3] Se lleva a cabo para reconocer los factores del entorno general de una organización.

[4] Análisis que permite conocer el contexto global de un ente.

[5] Diagrama estratégico diseñado para analizar fuerzas competitivas: poder de negociación de los clientes, poder de negociación de los proveedores, amenaza de nuevos competidores entrantes, amenaza de nuevos productos sustitutos y rivalidad entre competidores.

Se verifica que la empresa objeto de estudio, efectúa un análisis para la comprensión de su funcionamiento y contexto, a través de la herramienta FODA.

Se evidencia el archivo “Objetivos - Partes interesadas – FODA V02”



EVALUACIÓN DEL CONTEXTO - ANÁLISIS FODA

VERSIÓN 02 VIGENCIA 31/10/19 REVISIÓN 05/07/21

| # | FODA | ABORDAJE | Inicio 2021 PROBABILIDAD A(O) | PROBABILIDAD P(O) | IMPACTO B(S) | IMPACTO P(O) | RESULTADO L(S) | RESULTADO (P x L)=RISK | Acción Correctiva: LO QUE SE REALIZARA A FUTURO PARA EVITAR QUE VUELVA A OCURRIR EL DESVIO. | Fecha Implem. | Resp. | Fecha Verif. | Resp | ESTADO DE VERIF | Fecha Eficacia | Resp | ESTADO DE EFICACIA | ESTADO DEL RIESGO | Fines 2021 PROBABILIDAD A(O) | PROBABILIDAD P(O) | IMPACTO B(S) | IMPACTO P(O) | RESULTADO L(S) | RESULTADO (P x L)=RISK |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | FORTALEZA | 2021 | | | | | | | | | | | | | | | | | | | | | | |
| 1 | INFRAESTRUCTURA SOLIDA EN PLANTA DE LOS NOGALES | SI | | | 1 | | 1 | 11,1 | Construcción de oficinas en la parte frontal de la planta. | 03-09-21 | AC | 30-09-21 | AC | Cerrado | 06-08-22 | AC | NO EVALUADO | | | | | | | 0,0 |
| 2 | COMPROMISO DEL PERSONAL Y SENTIDO DE PERTENENCIA EN SECTORES CLAVES DE LA EMPRESA | SI | | 2 | | 2 | | 44,4 | Implementación de encuesta de satisfacción al personal. | 02-07-21 | MG | 03-12-21 | MG | Abierto | 02-02-22 | MG | NO EVALUADO | | | | | | | 0,0 |
| 3 | VALOR AGREGADO EN LA COMERCIALIZACIÓN DE PRODUCTOS POR CONTAR CON UNA ALIANZA ESTRATÉGICA CON UN PROVEEDOR DE SERVICIO DE LOGÍSTICA, QUE FORMA PARTE DEL MISMO GRUPO ECONÓMICO | | | | 1 | | 1 | 11,1 | | | | | | | | | | | | | | | | 0,0 |
| 4 | TRATO PERSONALIZADO Y SEGUIMIENTO A LOS PRINCIPALES CLIENTES | | | | 1 | | 1 | 11,1 | | | | | | | | | | | | | | | | 0,0 |
| 5 | ORGANIZACIÓN Y PLANIFICACIÓN DE VENTAS, QUE POSIBILITAN LA MAXIMIZACIÓN DE COSTOS DE TRANSPORTE | | | | 1 | | 1 | 11,1 | | | | | | | | | | | | | | | | 0,0 |
| 6 | CAPACIDAD DE ABASTECER DE INSUMOS A CLIENTES EN SUS PROCESOS DE NEGOCIO CLAVES | | | | 1 | | 1 | 11,1 | | | | | | | | | | | | | | | | 0,0 |
| 7 | CUMPLIMIENTO ESTRICTO DE REQUISITOS LEGALES QUE PERMITEN LA CONTINUIDAD DE LAS OPERACIONES DEL NEGOCIO | | | | 1 | | 1 | 11,1 | | | | | | | | | | | | | | | | 0,0 |
| 8 | COMPROMISO POR PARTE DE LA DIRECCIÓN EN EL SISTEMA DE GESTIÓN DE CALIDAD Y LA MEJORA CONTINUA DE LOS PROCESOS | | | | 1 | | 1 | 11,1 | | | | | | | | | | | | | | | | 0,0 |
| 9 | FUERTE POSICIONAMIENTO EN LA REGIÓN CENTRO Y NORTE DEL PAÍS | | | | 1 | | 1 | 11,1 | | | | | | | | | | | | | | | | 0,0 |
| 10 | ALIANZAS ESTRATÉGICAS CON PROVEEDORES QUE PERMITEN PRECIOS COMPETITIVOS DE MATERIAS PRIMAS | | | | 1 | | 1 | 11,1 | | | | | | | | | | | | | | | | 0,0 |
| | DEBILIDAD | 2021 | | | | | | | | | | | | | | | | | | | | | | |
| 1 | ESTRUCTURA DE UN ÁREA COMERCIAL INSUFICIENTE, QUE GENERA: FALTA DE SEGUIMIENTO A LA TOTALIDAD DE LOS CLIENTES, SERVICIO DE POSVENTA IRREGULAR Y ATRASO EN TAREAS ADMINISTRATIVAS | No | | 2 | | 2 | | 44,4 | No se aborda. | | | | | | | | | | | | | | | 0,0 |
| 2 | INEXISTENCIA DE UN PLAN ESTRATÉGICO COMERCIAL QUE PERMITA VISIBILIZAR A LA EMPRESA EN LA WEB Y REDES SOCIALES. COSTO DE OPORTUNIDAD POR LA NO CAPTACIÓN DE CLIENTES PRESENTES EN CANALES DIGITALES | No | | | 1 | 2 | | 22,2 | No se aborda. | | | | | | | | | | | | | | | 0,0 |
| 3 | FALTA SEGUIMIENTO A LA TOTALIDAD DE LOS CLIENTE POSIBILITA DE NO OBTENER RETROALIMENTACIÓN DE SU INSATISFACCIÓN ANTE EL SERVICIO PRESTADO, IMPOSIBILITANDO LA TOMA DE ACCIONES CORRECTIVAS CONDUCENTES. | SI | | 2 | | 2 | | 44,4 | Cambiar la metodología para evaluar la satisfacción de los clientes.<br>Desarrollo de una metodología de seguimiento post venta ( ofrecer dar ) | 01-03-22<br>01-10-21 | MG<br>MG | 30-03-22<br>30-10-21 | MG<br>MG | Abierto<br>Cerrado | 01-03-22<br>02-01-22 | MG<br>MG | NO EVALUADO<br>NO EVALUADO | | | | | | |
| 4 | CANALES DE COMUNICACIÓN INFORMALES, LO QUE GENERA MALOS ENTENDIDOS O INTERPRETACIONES ERRÓNEAS DE LAS TAREAS A REALIZAR POR PARTE DE LOS EMPLEADOS | SI | | 2 | | | 1 | 22,2 | Planificar y desarrollar reuniones periódicas con el personal de la empresa a fin de mejorar la comunicación interna. Implementar herramientas de comunicación que ayuden a compartir la información de manera dinámica. | 01-03-21 | MG | 30-03-21 | MG | Cerrado | 25-10-21 | MG | EFICAZ | REDUCE | | 1 | | 1 | 11,1 |
| | OPORTUNIDAD | 2021 | | | | | | | | | | | | | | | | | | | | | | |
| 1 | IMPLEMENTACIÓN DE METODOLOGÍAS ÁGILES DE GESTIÓN QUE POSIBILITEN EL AUMENTO DE PRODUCTIVIDAD EN TIEMPO Y CONDICIONES SEGURAS DE TRABAJO | SI | | 2 | | 2 | | 44,4 | Implementación piloto de metodología de gestión japonesa 5S,en oficina del Responsable de Planta mediante la capacitación y concientización de los miembros de la empresa. Posterior replicación en toda la planta. | 15-09-21 | MJ | 20-12-21 | MG | Abierto | 02-02-22 | MG | NO EVALUADO | | | | | | | 0,0 |
| 2 | ADQUISICIÓN DE INFRAESTRUCTURA TECNOLÓGICA EN LAS ESTACIONES DE TRABAJO, QUE PERMITAN UN DESEMPEÑO EFICIENTE DE LAS ACTIVIDADES | SI | | 2 | | 2 | | 44,4 | Adquirir y actualizar infraestructura tecnológica.<br>Contratar un servicio con mayor velocidad de internet que permita una mejor conectividad. | 02-07-21 | MJ | 03-09-21 | MG | Cerrado | 21-10-21 | MJ | EFICAZ | REDUCE | | 1 | | 2 | 22,2 |
| 3 | EMPRESA EXCEPTUADA DEL AISLAMIENTO SOCIAL PREVENTIVO COVID-19 | SI | | 2 | | 2 | | 44,4 | Implementación de trabajo remoto. Utilización de herramientas para efectuar videoconferencia y otras plataformas digitales. Implementación de Plan de | 20-03-21 | AC | 01-06-21 | MG | Cerrado | 01-11-21 | MG | EFICAZ | REDUCE | | 1 | | 2 | 22,2 |
| | AMENAZA | 2021 | | | | | | | | | | | | | | | | | | | | | | |
| 1 | PRESIÓN SINDICAL DEL GREMIO DE LOS CAMIONEROS, QUE PUEDE AFECTAR EL NORMAL DESARROLLO DE LAS ACTIVIDADES DE LOGÍSTICA | No | | | 1 | 2 | | 22,2 | No se aborda | | | | | | | | | ASUME | | | | | | 0,0 |
| 2 | INESTABILIDAD ECONÓMICA DEL PAÍS | No | | | 1 | 2 | | 22,2 | No se aborda | | | | | | | | | ASUME | | | | | | 0,0 |
| 3 | COMPETENCIA DIRECTA DE FABRICANTES, AL COMERCIALIZAR CON LOS CLIENTE DEJANDO DE LADO A LOS DISTRIBUIDORES. | No | | | 1 | 2 | | 22,2 | No se aborda | | | | | | | | | ASUME | | | | | | 0,0 |
| 4 | AUMENTO DE COSTOS EN INSUMOS Y REDUCCIÓN DE LA RENTABILIDAD | No | | 2 | | 2 | | 44,4 | No se aborda | | | | | | | | | ASUME | | | | | | 0,0 |
| 5 | AUMENTOS DE COMBUSTIBLES, QUE REPERCUTE DIRECTAMENTE EN EL COSTO DE LOS SERVICIOS PRESTADOS | No | | 2 | | 2 | | 44,4 | No se aborda | | | | | | | | | ASUME | | | | | | 0,0 |
| 6 | DEPENDENCIA ABSOLUTA A LOS FABRICANTES DE INSUMOS | No | | 2 | | 2 | | 44,4 | No se aborda | | | | | | | | | ASUME | | | | | | 0,0 |
| 7 | MEJORES PRECIOS Y SERVICIOS OFRECIDOS POR LA COMPETENCIA | No | | | 1 | 2 | | 22,2 | No se aborda | | | | | | | | | ASUME | | | | | | 0,0 |
| 8 | CONTAGIO Y PROPAGACIÓN DE VIRUS COVID-19 EN MIEMBROS DE LA ORGANIZACIÓN | SI | | 2 | | 2 | | 44,4 | Actualización del plan de contingencia y protocolos de seguridad, difundidos y comunicados a los miembros de la empresa. Realización de capacitaciones de prevención. Otorgamiento de EPP y solicitud de test PCR (Reacción en Cadena de Polimerasa) al personal que presenta síntomas de enfermedad | 02-04-21 | MG | 01-06-21 | MG | Cerrado | 30-12-21 | MG | NO EVALUADO | | | | | | | 0,0 |

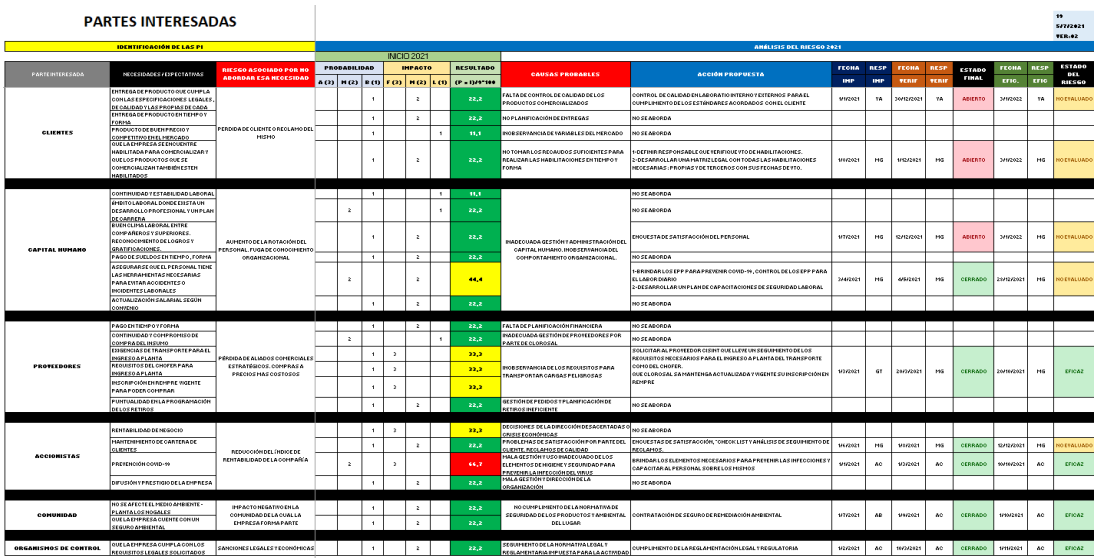
*Ilustración 5: Comprensión de la organización y su contexto (FODA)*

### *3.2.2 Necesidades y expectativas de las partes interesadas.*

Posteriormente, en su apartado 4.2, se indica que la organización debe establecer las partes interesadas que son oportunas para el SGSI en general y en particular a la seguridad de la información. Su pertinencia puede derivar de exigencias legales, reglamentarias y contractuales.

Se verifica que la compañía analizada identifica sus partes interesadas y las necesidades y expectativas relacionadas. Las mismas son las siguientes: clientes, capital humano, proveedores, accionistas, comunidad y organismos de control.

Cabe destacar que la gestión de partes interesadas tiene un fuerte enfoque en la calidad. Por lo tanto, deberían identificarse aspectos que afecten a la seguridad de la información.



PARTES INTERESADAS

| PARTE INTERESADA | NECESIDADES / EXPECTATIVAS | RIESGO ASOCIADO POR NO ABORDAR ESA NECESIDAD | PROBABILIDAD A (-) | PROBABILIDAD M (+) | IMPACTO B (-) | IMPACTO F (-) | IMPACTO M (+) | IMPACTO L (+) | RESULTADO (P × I)*100 | CAUSAS PROBABLES | ACCIÓN PROPUESTA | FECHA IMP | RESP IMP | FECHA VERIF | RESP VERIF | ESTADO FINAL | FECHA EFIC. | RESP EFIC | ESTADO DEL RIESGO |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| CLIENTES | ENTREGA DE PRODUCTO QUE CUMPLA CON LAS ESPECIFICACIONES LEGALES, DE CALIDAD Y LAS PROPIAS DE CADA | PERDIDA DE CLIENTE O RECLAMO DEL MISMO | | | 1 | | 2 | | 22,2 | FALTA DE CONTROL DE CALIDAD DE LOS PRODUCTOS COMERCIALIZADOS | CONTROL DE CALIDAD EN LABORATIO INTERNO Y EXTERNOS PARA EL CUMPLIMIENTO DE LOS ESTANDARES ACORDADOS CON EL CLIENTE | 1/11/2021 | YA | 31/12/2021 | YA | ABIERTO | 31/12/2022 | YA | NO EVALUADO |
| | ENTREGA DE PRODUCTO EN TIEMPO Y FORMA | | | | 1 | | 2 | | 22,2 | NO PLANIFICACIÓN DE ENTREGAS | NO SE ABORDA | | | | | | | | |
| | PRODUCTO DE BUEN PRECIO Y COMPETITIVO EN EL MERCADO | | | | 1 | | | 1 | 11,1 | INOBSERVANCIA DE VARIABLES DEL MERCADO | NO SE ABORDA | | | | | | | | |
| | QUE LA EMPRESA SE ENCUENTRE HABILITADA PARA COMERCIALIZAR Y QUE LOS PRODUCTOS QUE SE COMERCIALIZAN TAMBIÉN ESTÉN HABILITADOS | | | | 1 | | 2 | | 22,2 | NO TOMAR LOS RECAUDOS SUFICIENTES PARA REALIZAR LAS HABILITACIONES EN TIEMPO Y FORMA | 1-DEFINIR RESPONSABLE QUE VERIFIQUE VTO DE HABILITACIONES.<br>2-DESARROLLAR UNA MATRIZ LEGAL CON TODAS LAS HABILITACIONES NECESARIAS, PROPIAS Y DE TERCEROS CON SUS FECHAS DE VTO. | 1/11/2021 | MG | 1/12/2021 | MG | ABIERTO | 31/12/2022 | MG | NO EVALUADO |
| CAPITAL HUMANO | CONTINUIDAD Y ESTABILIDAD LABORAL | AUMENTO DE LA ROTACIÓN DEL PERSONAL, PÉRDIDA DE CONOCIMIENTO ORGANIZACIONAL | | | 1 | | | 1 | 11,1 | INADECUADA GESTIÓN Y ADMINISTRACIÓN DEL CAPITAL HUMANO, INOBSERVANCIA DEL COMPORTAMIENTO ORGANIZACIONAL | NO SE ABORDA | | | | | | | | |
| | ÁMBITO LABORAL DONDE EXISTA UN DESARROLLO PROFESIONAL Y UN PLAN DE CARRERA | | | 2 | | | | 1 | 22,2 | | NO SE ABORDA | | | | | | | | |
| | BUEN CLIMA LABORAL ENTRE COMPAÑEROS Y SUPERIORES. RECONOCIMIENTO DE LOGROS Y GRATIFICACIONES. | | | | 1 | | 2 | | 22,2 | | ENCUESTA DE SATISFACCIÓN DEL PERSONAL | 1/11/2021 | MG | 15/12/2021 | MG | ABIERTO | 31/12/2022 | MG | NO EVALUADO |
| | PAGO DE SUELDO EN TIEMPO , FORMA | | | | 1 | | 2 | | 22,2 | | NO SE ABORDA | | | | | | | | |
| | ASEGURARSE QUE EL PERSONAL TIENE LAS HERRAMIENTAS NECESARIAS PARA EVITAR ACCIDENTES O INCIDENTES LABORALES | | | 2 | | | 2 | | 44,4 | | 1-ERRADICAR LOS EPP PARA PREVENIR COVID-19 , CONTROL DE LOS EPP PARA EL LABOR DIARIO<br>2-DESARROLLAR UN PLAN DE CAPACITACIONES DE SEGURIDAD LABORAL | 31/12/2021 | MG | 16/12/2021 | MG | CERRADO | 23/12/2021 | MG | NO EVALUADO |
| | ACTUALIZACIÓN SALARIAL SEGÚN CONVENIO | | | | 1 | | 2 | | 22,2 | | NO SE ABORDA | | | | | | | | |
| PROVEEDORES | PAGO EN TIEMPO Y FORMA | PÉRDIDA DE ALIADOS COMERCIALES ESTRATÉGICOS. COMPRAS A PRECIOS MAS COSTOSOS | | | 1 | | 2 | | 22,2 | FALTA DE PLANIFICACIÓN FINANCIERA | NO SE ABORDA | | | | | | | | |
| | CONTINUIDAD Y COMPROMISO DE COMPRA DEL INSUMO | | | 2 | | | | 1 | 22,2 | INADECUADA GESTIÓN DE PROVEEDORES POR PARTE DE LA ORGSAL | NO SE ABORDA | | | | | | | | |
| | EXIGENCIAS DE TRANSPORTE PARA EL INGRESO A PLANTA | | | | 1 | 3 | | | 33,3 | INOBSERVANCIA DE LOS REQUISITOS PARA TRANSPORTAR CARGAS PELIGROSAS | SOLICITAR AL PROVEEDOR CLIENTE QUE LLEVE UN SEGUIMIENTO DE LOS REQUISITOS NECESARIOS PARA EL INGRESO A PLANTA DEL TRANSPORTE COMO DEL CHOFER.<br>QUE LA ORGSAL SAMANTENGA ACTUALIZADA Y VIGENTE SU INSCRIPCIÓN EN REPRE | 1/11/2021 | GT | 23/12/2021 | MG | CERRADO | 23/12/2021 | MG | EFICAZ |
| | REQUISITOS DEL CHOFER PARA INGRESO A PLANTA | | | | 1 | 3 | | | 33,3 | | | | | | | | | | |
| | INSCRIPCIÓN EN REPRE VIGENTE PARA PODER COMPRAR | | | | 1 | 3 | | | 33,3 | | | | | | | | | | |
| | PUNTUALIDAD EN LA PROGRAMACIÓN DE LOS RETIROS | | | | 1 | | 2 | | 22,2 | GESTIÓN DE PEDIDOS Y PLANIFICACIÓN DE RETIROS INEFICIENTE | NO SE ABORDA | | | | | | | | |
| ACCIONISTAS | RENTABILIDAD DE NEGOCIO | REDUCCIÓN DEL ÍNDICE DE RENTABILIDAD DE LA COMPAÑÍA | | | 1 | 3 | | | 33,3 | DECISIONES DE LA DIRECCIÓN DE ESA CENTRADAS A CRISIS ECONÓMICAS | NO SE ABORDA | | | | | | | | |
| | MANTENIMIENTO DE CARTERA DE CLIENTES | | | | 1 | | 2 | | 22,2 | PSICOLOPIAS DE SATISFACCIÓN POR PARTE DEL CLIENTE, RECLAMOS DE CALIDAD | ENCUESTAS DE SATISFACCIÓN, "CHECK LIST Y ANÁLISIS DE SEGUIMIENTO DE RECLAMOS. | 1/11/2021 | MG | 1/11/2021 | MG | CERRADO | 15/12/2021 | MG | NO EVALUADO |
| | PREVENCIÓN COVID-19 | | | 2 | | 3 | | | 66,7 | FALA GESTIÓN Y/O CONOCIMIENTO DE LOS ELEMENTOS DE HIGIENE Y SEGURIDAD PARA PREVENIR LA INFECCIÓN DEL VIRUS | BRINDAR LOS ELEMENTOS NECESARIOS PARA PREVENIR LAS INFECCIONES Y CAPACITAR AL PERSONAL SOBRE LOS MISMOS | 1/11/2021 | AC | 1/12/2021 | AO | CERRADO | 16/11/2021 | AO | EFICAZ |
| | DIFUSIÓN Y PRESTIGIO DE LA EMPRESA | | | | 1 | | 2 | | 22,2 | FALA GESTIÓN Y DIRECCIÓN DE LA ORGANIZACIÓN | NO SE ABORDA | | | | | | | | |
| COMUNIDAD | NO SE AFECTE EL MEDIO AMBIENTE - PLANTAS LOCALES | IMPACTO NEGATIVO EN LA COMUNIDAD DE LA CUAL LA EMPRESA FORMA PARTE | | | 1 | | 2 | | 22,2 | NO CUMPLIMIENTO DE LA NORMATIVA DE SEGURIDAD DE LOS PRODUCTOS Y AMBIENTAL DEL LUGAR | CONTRATACIÓN DE SEGURO DE REMEDIACIÓN AMBIENTAL | 1/11/2021 | AB | 1/11/2021 | AO | CERRADO | 1/11/2021 | AO | EFICAZ |
| | QUE LA EMPRESA CUENTE CON UN SEGURO AMBIENTAL | | | | 1 | | 2 | | 22,2 | | | | | | | | | | |
| ORGANISMOS DE CONTROL | QUE LA EMPRESA CUMPLA CON LOS REQUISITOS LEGALES SOLICITADOS E | SANCIONES LEGALES Y ECONÓMICAS | | | 1 | | 2 | | 22,2 | SEGUIMIENTO DE LA NORMATIVA LEGAL Y REGLAMENTARIA IMPUESTA PARA LA ACTIVIDAD | CUMPLIMIENTO DE LA REGLAMENTACIÓN LEGAL Y REGULATORIA | 1/12/2021 | AC | 16/12/2021 | AO | CERRADO | 1/11/2021 | AO | EFICAZ |

*Ilustración 6: Partes Interesadas*

### *3.2.3 Alcance del SGSI.*

El alcance es una declaración documentada de la extensión y los límites del SGSI. El mismo debe establecerse teniendo en cuenta las unidades de negocio, los procesos relevantes, los activos de la información que le dan soporte y su ubicación física.

En el enunciado 4.3, el marco de referencia establece que la organización debe determinar los límites y la aplicabilidad del SGSI en un informe documentado. Deben indicarse los activos críticos a proteger y el enfoque que se le dará al SG, en base al cual se confeccionará la “declaración de aplicabilidad” posteriormente requerida.

Cabe destacar en este punto que deben identificarse las interfaces y dependencias entre actividades efectuadas por cuenta propia y aquellas que son elaboradas por terceros contratados, pues todas están bajo la responsabilidad de la compañía.

Se verifica que la organización objeto de estudio posee en el archivo “Alcance del Sistema de Gestión V00”, el respectivo alcance de su Sistema de Gestión de Calidad. Sin embargo, este difiere a lo solicitado por ISO 27001, pues cada norma añade requisitos específicos. Por lo tanto, debería efectuarse una adecuación de este punto, teniendo en cuenta el mapa de interacción de procesos, para cumplimentar apropiadamente la exigencia.

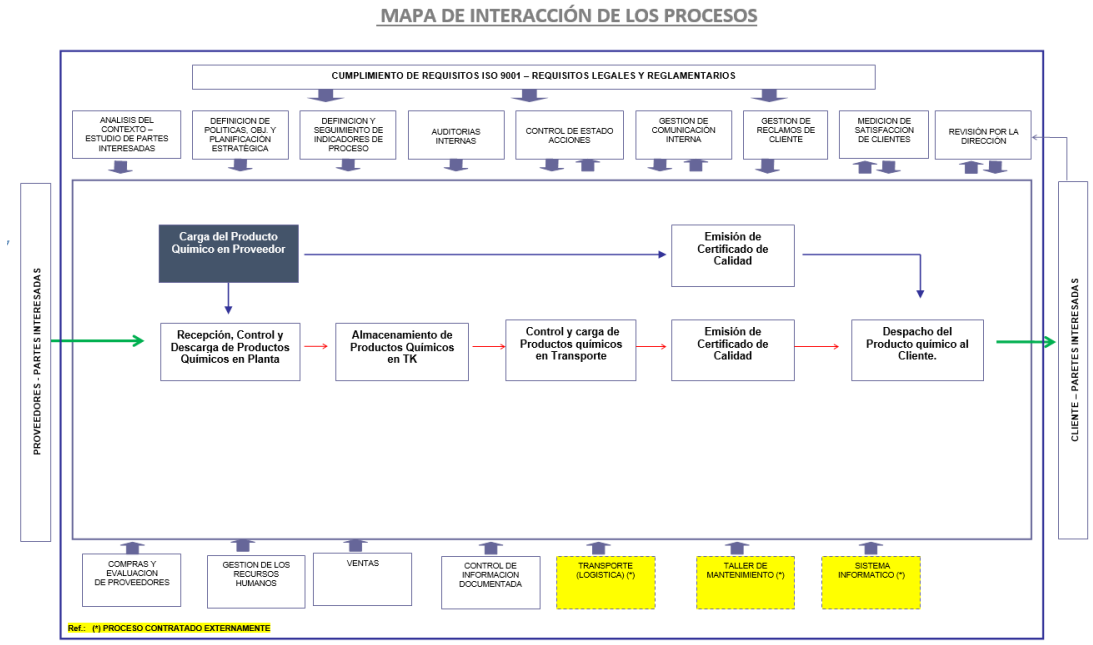



*Ilustración 7: Mapa de interacción de procesos*

## 3.3 Liderazgo

### *3.3.1 Liderazgo y compromiso.*

El requisito 5.1 de la norma reza que la alta dirección debe manifestar liderazgo y compromiso respecto a la implementación y seguimiento del SGSI. Este aspecto puede evidenciarse con alguna de las siguientes situaciones:

- Estableciendo la política y los procedimientos de seguridad
- Integrando los requisitos de la norma con los procesos del negocio
- Facilitando los recursos necesarios para una adecuada implementación del SGSI
- Contribuyendo a la conformación de una sólida cultura de seguridad
- Haciendo mentoría para contribuir a la eficiencia del SGSI y asegurar el logro de los resultados esperados
- Incentivando a la mejora continua
- Formando perfiles de liderazgo en la organización

Para una correcta implementación de un SGSI, debe tenerse en consideración la cultura organizacional y los recursos disponibles para dar cumplimiento a los objetivos de seguridad propuestos.

### *3.3.2 Cultura de Seguridad de la Información.*

Comprender el comportamiento de las personas frente a los temas de seguridad es un tema de percepción y de valoración personal, de acuerdo con múltiples variables que cada uno de ellos conoce.

La psicología de la seguridad de la información pasa por un reconocimiento del riesgo y una percepción del mismo, que mantiene o no alerta a la persona frente a situaciones que pueden vulnerar su espacio individual o comunitario, cuando de manejo de información u otra situación se trate (IT-Insecurity, 2009).

Por lo tanto, comprender los riesgos, actuar conforme a ese entendimiento y hacer visible una acción en los procesos de negocios, debe ser un quehacer diario en la dirección de una organización. Si no se valora la información como lo que ella es, un activo de la organización, y no se reconocen en los procesos de negocios la importancia de ella, se está advirtiendo una dinámica organizacional dispersa y animada por una informalidad en la administración de los riesgos de la información.

Cuando las expectativas del nivel directivo establecen que la información es un bien crítico y sensible para la permanencia de la organización, cada uno de los colaboradores activa un programa de prevención y control de los riesgos de seguridad. Si en cambio este no muestra interés legítimo con sus actuaciones respecto de la protección de los recursos de información, la organización asumirá que la pérdida de información, la inconsistencia de archivos y su eliminación son eventos atribuibles sólo al área de tecnología y no detectará el mensaje negativo dado por la falta de impulso de los directivos.

Una cultura de seguridad de la información fuerte y consistente no implica una compañía sin incidentes de seguridad ni fraudes, sino de una que destruye sus propias auto restricciones para conocer y atender nuevas formas de equivocarse, aprendiendo de ellas (Cano M., 2013).

En este sentido, se torna indispensable la capacitación y la concientización de los usuarios respecto a la problemática de la (in) Seguridad de la Información. Este proceso constante permitirá construir una fuerte

cultura de seguridad de la información. Los colaboradores deben trabajar en un entorno de control, tomando los resguardos que sean necesarios.

La concientización es una pieza clave en toda estrategia de seguridad, por lo que es recomendable efectuar previamente a su ejecución, un adecuado análisis de las necesidades de formación, teniendo en cuenta la resistencia al cambio y la cultura organizacional existente.

### *3.3.3 Política de Seguridad de la Información.*

La exigencia 5.2 de la norma, indica que la alta dirección debe establecer una “Política de Seguridad de la Información” (PSI) acorde al objeto social de la organización. La misma debe contener los objetivos de seguridad e incluir el compromiso de cumplimiento de los requerimientos aplicables y de mejora continua.

En este sentido, se presenta la siguiente definición, con la finalidad de profundizar el entendimiento de este concepto:

> *Una Política de Seguridad de la Información es un documento central para la protección de los datos y de los recursos utilizados para su tratamiento, que define la postura de una organización respecto al comportamiento que espera de empleados, autoridades y terceros que tomen contacto con dichos datos y/o recursos, para su protección.* (Dirección Nacional de Ciberseguridad. Jefatura de Gabinete de Ministros, 2022).

Es importante tener en cuenta que dicha política debe estar formalmente documentada y debe ser eficazmente comunicada. Además, se espera que pueda ser accedida por las partes interesadas cuando así lo requieran.

Se verifica que la organización objeto de estudio tiene definida una “Política de Calidad”. Por lo tanto, deberá efectuar una adecuación de la existente para dar cumplimiento conjuntamente a los requisitos de Calidad y de Seguridad de la Información; o en su defecto establecer una política independiente y específica a tal fin.

A continuación, se propone la estructura de la PSI que debería desarrollar el ente analizado en el presente trabajo. Para ello se tuvo en consideración lo señalado en el anexo del “Modelo Referencial de Política de Seguridad de la Información” establecido en la Disposición 01/2022, la cuál es aplicable al sector público nacional argentino (Dirección Nacional de Ciberseguridad. Jefatura de Gabinete de Ministros, 2022).

Se sugiere que los apartados de la “Política de Seguridad de la Información” sean los siguientes:

a) Introducción: en ella, se debe realizar una fundamentación respecto al valor que posee la información para la organización, enfatizando la necesidad e importancia de su adecuada protección. Debe tenerse en cuenta que lo anteriormente indicado es independiente del formato y soporte utilizado para su creación, ciclo de vida y eventual destrucción, desuso o archivo definitivo.

Por otro lado, pueden mencionarse las posibles amenazas y riesgos existentes en relación al tipo de actividad u objeto social llevado a cabo.

Será necesario también evidenciar la relevancia que tiene la aplicación de controles y mecanismos de seguridad, los cuales incluyen procedimientos, programas, normas, estructuras organizacionales, *software*, *hardware*, entre otros. Estos deberán aplicarse o utilizarse en forma coordinada con el resto de los procesos del negocio.

Se recomienda explicitar la importancia del acatamiento de la legislación aplicable, normas internas y buenas prácticas de seguridad propuestas en marcos de cumplimiento relacionados.

Finalmente, podrán desarrollarse otros aspectos considerados pertinentes para la correcta comprensión de este documento.

b) Objeto: en esta sección debe exteriorizarse la intención, orientación, nociones generales, reglamentaciones fundamentales y los mecanismos de comunicación para la protección de la información y la infraestructura utilizada a tal fin.

c) Alcance: debe establecerse el ámbito de aplicación, los recursos disponibles y los procesos de negocio por donde fluye la información.

En esta sección se encuentran involucradas las personas que cumplen funciones directivas, administrativas y técnicas, cualquiera sea su relación contractual, nivel jerárquico o situación laboral (internas o externas).

d) Principios Básicos: debe indicarse de qué manera se asegurarán las características de confidencialidad, integridad y disponibilidad de la información y de los activos utilizados para su gestión, teniendo en cuenta la valoración de la criticidad que presenta cada uno de ellos. Por lo tanto, se deberá efectuar una evaluación de riesgo y una posterior gestión del mismo.

En el mismo sentido, debe considerarse la protección de los derechos de los titulares de los datos personales procesados y de la información sensible que resguarda la organización.

Lo abordado en este apartado debe alinearse y complementarse con el resto de las políticas y normas internas, enfatizando la importancia de una eficaz gestión de la seguridad de la información.

Por otra parte, debe manifestarse que la dirección ejercerá el liderazgo en cuanto a la mejora continua de los procesos de seguridad de la información, consolidando su correcto funcionamiento. Además, debe hacerse hincapié en el compromiso de la organización respecto a la concientización y capacitación de sus empleados, a fin de contribuir de este modo a afianzar una sólida cultura de seguridad de la información.

También es fundamental que el ente exteriorice su interés de cumplir con la normativa legal o reglamentaria y esté dispuesto a adaptarse a futuras normas, requisitos del contexto interno o externo y a aquellos que surjan de la vinculación con otras partes interesadas.

Finalmente se deben mencionar las sanciones disciplinarias que conlleva el desacato o la inobservancia de lo establecido en este documento, en relación a la dimensión y particularidades del aspecto no cumplido.

e) Revisión y actualización: la empresa debe comprometerse a revisar periódicamente la política de seguridad (preferentemente en ciclos inferiores o iguales a un año), adaptándola a las nuevas condiciones organizativas y del mercado. Además, deberá manifestar la intención de comunicar a todo su personal y a los terceros involucrados los cambios que se originen de estas correcciones.

Del mismo modo, corresponde efectuar las modificaciones que sean consideradas pertinentes cuando la situación lo amerite.

f) Lineamientos específicos: para concluir, deberían indicarse los principales aspectos a tener en cuenta, relacionados mínimamente a los

siguientes controles de seguridad de la información. Para ello, puede utilizarse como referencia lo señalado en el “Anexo A” de ISO 27001:

- Organización de la Seguridad de la información
- Seguridad del Capital Humano
- Gestión de Activos de Información
- Autenticación, autorización y control de accesos
- Uso de herramientas criptográficas
- Seguridad física y ambiental
- Seguridad operativa
- Seguridad de las comunicaciones
- Adquisición y mantenimiento de sistemas de información
- Relación con proveedores
- Gestión de incidentes de seguridad
- Aspectos de seguridad para la continuidad de la gestión
- Cumplimiento

### *3.3.4 Roles, responsabilidades y autoridades.*

El apartado 5.3 de la norma ISO 27001 establece que la alta dirección debe asegurar que las responsabilidades y los roles relacionados a la seguridad de la información se determinen y se comuniquen. Esto tiene como finalidad lograr una alineación entre los requisitos de la norma y los del SGSI. También, se espera que estos perfiles informen a la Dirección sobre el desempeño del Sistema de Gestión.

Para efectuar un efectivo gobierno y gestión de la SI, es necesario contar con una adecuada estructura, dentro de la cual deben definirse perfiles, roles y funciones. Cabe destacar que, dependiendo de la magnitud y las características de la organización, el tipo de estructura y la cadena de mandos podría diferir.

En este sentido, el CISO[6] encabezará la estructura mencionada anteriormente, siendo la persona responsable de velar por la seguridad de la

[6] Por sus siglas en inglés el CISO (*Chief Information Security Officer)* es el responsable de seguridad de la información en una organización. Generalmente es un rol desempeñado a nivel ejecutivo y su principal función es alinear la seguridad de la información con los objetivos de negocio.

información. Este podrá tomar el rol de director, gerente o responsable del sector, teniendo en cuenta las particularidades de la organización.

Al igual que cualquier otro líder de área, el CISO debería constituir un equipo de trabajo idóneo, que le permita alcanzar el cumplimiento de los objetivos propuestos. El sector debe estar integrado por personal que posea una sólida formación técnica y habilidades comunicativas y creativas, para educar y concientizar sobre la temática al resto de la compañía.

La persona que ocupa esta función, debe poder “hablar el lenguaje de la organización”, dar a conocer eficazmente los objetivos de seguridad y su relación con los del negocio, contribuyendo al fortalecimiento de una cultura de seguridad de la información. Además, es importante que se comunique con un “lenguaje común” y que sea un hábil negociador, para poder acompañar a la organización implementando un nivel de seguridad adecuado, no siendo un obstáculo sino un asesor de la compañía, colaborando de este modo con lo que se definió en la estrategia del negocio.

En cuanto a las características particulares de la organización abordada, se evidencia que no posee personal que se encargue de cuestiones relacionadas a TI y seguridad de la información.

Al presentar características de pequeña envergadura, debería plantearse la posibilidad de incorporar a una persona que cumpla el rol de dirección del “sistema de gestión integrado”. Correspondería que el mismo posea conocimientos en el ámbito de Calidad y Seguridad de la Información.

Otra alternativa, sería incorporar al organigrama una posición que se encargue específicamente de cuestiones relacionadas a la gestión de la seguridad de la información. De esta manera, el “sistema de gestión integrado” asumiría un líder en calidad y otro en seguridad de la información.

Se propone a continuación, un perfil de puesto para el “Responsable de Gestión de la Seguridad de la Información” (CISO):

| **PERFIL DE PUESTO** |
| --- |
| **Puesto:** Responsable de Gestión de Seguridad de la Información (CISO)<br>Horario: lunes a viernes 08:30 a 17:00 hs. Sábados 8:30 a 13:00. |
| **Sector: Oficina** |

| CARACTERÍSTICAS DEL PUESTO |
| --- |
| **OBJETIVO GENERAL**: coordinar las actividades relacionadas con el análisis, detección, tratamiento, almacenamiento y protección de la información .<br><br>**LABORES Y RESPONSABILIDADES**<br><br>➢ Conocer las actividades propias del negocio, las partes interesadas relacionadas con la Seguridad de la Información. documentar las necesidades y las expectativas en línea con las prioridades del negocio.<br><br>➢ Coordinar y efectuar recomendaciones sobre las acciones necesarias para proteger la información en general.<br>➢ Diseñar un plan de inducción, capacitación y concienciación sobre la seguridad de la información.<br>➢ Identificar riesgos y coordinar los controles, tratamientos y controles de efectividad. Tomar en cuenta los resultados de las auditorías realizadas.<br>➢ Seleccionar e implementar salvaguardias ante los riesgos identificados.<br>➢ Mantener contacto fluido y permanente con la dirección y los grupos de interés.<br>➢ Redactar los documentos concernientes a la seguridad de la información (estrategia, política, normas y procedimientos), en línea con las prioridades de la organización, manteniéndolos actualizados. |
| **Reporta a:** Presidencia |
| **Supervisa a:** Departamento de TI y Seguridad de la Información |
| **Autoridad**<br>➢ Responsable de área funcional<br>➢ De acuerdo al otorgado por la dirección |
| PERFIL REQUERIDO |
| **Estudios requeridos**<br>➢ Preferentemente estudios universitarios en Ingeniería en Sistemas, computación o afines.<br>➢ Conocimientos sobre tecnología de la información y procesos de negocio |

| |
|---|
| ➢ Formación y experiencia en gestión de la norma ISO 27001 (estudios de posgrado o certificaciones internacionales). |
| **Requisitos**<br>➢ Sexo: indistinto<br>➢ Edad: mayor a 30 años<br>➢ Conocimiento sobre Gestión y Dirección de SGSI<br>➢ Buenas relaciones interpersonales, capacidad de negociación, comunicación y conocimiento del negocio<br>➢ Orientación hacia las personas y los resultados |
| **Competencias necesarias**<br>➢ Experiencia mínima de 3 años en puestos similares<br>➢ Buenas relaciones interpersonales<br>➢ Capacidad para la comunicación y negociación<br>➢ Confiabilidad<br>➢ Proactividad<br>➢ Responsabilidad<br>➢ Capacidad de toma de decisiones<br>➢ Cordialidad y buen trato<br>➢ Manejo de pc y sistemas informáticos<br>➢ Idoneidad en las labores a realizar |

*Ilustración 8: Perfil de puesto para el "Responsable de Gestión de Seguridad de la Información"*

## 3.4 Planificación

La norma en este capítulo trata uno de los requerimientos centrales del SGSI, el cual es la gestión de riesgos. Además, dentro de la planificación aborda la definición de los objetivos de seguridad de la información, para los que se deben definir acciones, recursos y responsables.

En este sentido, es relevante la definición de ciertos conceptos relacionados a la temática:

### *3.4.1 Riesgo.*

Según el diccionario de la Real Academia Española, "riesgo" es una contingencia o proximidad de un daño (Real Academia Española, s.f.). Además, nos informa que dicha palabra proviene del árabe "*rizq*", que significa

“lo que depara la providencia”. Según (Coraminas, 1961), este término tiene la misma etimología que risco que significa peñasco alto y escarpado de difícil tránsito, por el peligro que se sufre al andar por él.

En el ámbito de la seguridad de la información, podríamos decir que son todos aquellos eventos que pueden poner en peligro la información, comprometiendo de este modo las actividades habituales del negocio. También podría ser definido como la posibilidad de que no se obtengan los resultados deseados. Por ello, es importante poder cuantificar el impacto que puede generar en la compañía y determinar cuáles de ellos son más importantes.

El riesgo es la combinación entre la probabilidad que se produzca un evento (desastres naturales, fortuitos o intencionados) y sus consecuencias negativas.

Según lo define ISO 27005, el riesgo implica la posibilidad de que una amenaza concreta pueda aprovechar una vulnerabilidad para causar una pérdida o daño en un activo de información (ISO/IEC 27005, 2012).

Debido a que cada organización tiene activos de información, características y necesidades específicas, la evaluación del riesgo es un proceso particular para cada una de ellas. La probabilidad puede calcularse mediante determinaciones empíricas basadas en sucesos del pasado o medios subjetivos, como por ejemplo la opinión de peritos o expertos en la materia.

Dada esta situación, es sumamente importante la aplicación de contramedidas para mitigar la existencia de los riesgos en las organizaciones. En la esfera de la seguridad informática, los estándares internacionales definen “contramedidas” como las políticas, procedimientos, prácticas y estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo tolerable por la dirección (apetito al riesgo).

Los riesgos de TI son un componente del universo de riesgos a los que está sometida una organización. Otros a los que se enfrenta pueden ser: estratégicos, ambientales, de mercado, de crédito, operativos y de cumplimiento.

### *3.4.2 Vulnerabilidad.*

La palabra vulnerable tiene su origen latín y proviene del vocablo "*vulnus*" que significa herida y el sufijo "*abilis*" que expresa posibilidad (Significados.com, s.f.)

Llevado este término al ámbito de la seguridad de la información, podríamos afirmar que vulnerabilidad es una debilidad que puede poner en peligro a la información del negocio y al buen funcionamiento de su actividad. Constituye un hecho que permite concretar una amenaza. Ella se puede hacer presente en los activos de información, dada la escasez o la falta de medidas que los resguarden, posibilitando a un atacante transgredir la confidencialidad, integridad y/o disponibilidad de la información.

El ente siempre está amenazado de sufrir algún daño en su sistema de información, estas amenazas son mayores cuando se presentan puntos débiles o "vulnerabilidades". De este modo, se tiene mayor o menor riesgo dependiendo de la cantidad y número de vulnerabilidades presentes. Al disminuir las vulnerabilidades, también disminuirá el riesgo de sufrir daños, no sólo en el aspecto informático, sino en toda la organización.

Las vulnerabilidades componen debilidades que exteriorizan las organizaciones frente a riesgos o amenazas que presentan los activos de información. Es por ello, que deben conocerse e identificarse las vulnerabilidades asociadas a los mismos.

El punto de partida es la realización de un inventario de los activos que estarán alcanzados por el SGSI, en donde se consignan entre otros datos: tipo de información, dueño, personal autorizado a su acceso, formato de almacenamiento, preservación y dependencias.

### *3.4.3 Amenaza.*

Una amenaza es todo elemento que aprovecha una vulnerabilidad para atentar contra la seguridad de un activo de información. Si la amenaza impacta sobre la vulnerabilidad se produce un incidente de seguridad, comprometiéndose la seguridad de la información. Se trata de una condición del entorno de los sistemas, áreas o dispositivos que contienen información valiosa que ante determinada circunstancia podría dar lugar a que se

produjese una violación de seguridad, afectando parte de la información y de la infraestructura tecnológica de la organización.

Algunos de los objetivos de la seguridad informática son: identificar las amenazas a las cuales está expuesta la información, minimizar los riesgos de esa exposición, gestionar la adecuada utilización de las TIC que tiene la organización, garantizar que en caso de un desastre informático se tenga una recuperación del negocio inmediata e integral, y cumplir con el marco legal que se exige por el manejo de datos personales y empresariales de los clientes y socios de la empresa (Baca Urbina, 2016).

### *3.4.4 Acciones para tratar el riesgo.*

El apartado 6.1 de la norma propone un conjunto de acciones que deben llevarse a cabo para tratar el riesgo y las oportunidades. Sin embargo, para abordarlo, podrían utilizarse adicionalmente, como marco de cumplimiento alguna de las siguientes normas: ISO 31000:2018 “Guía para la gestión de Riesgos” o ISO 27005:2018 “Gestión de los riesgos de Seguridad de la Información”. Cabe destacar que (ISO/IEC 27001, 2013, pág. 11), indica que la organización debe conservar información documentada sobre el proceso llevado a cabo para dar cumplimiento a este requerimiento.

Posteriormente a la identificación de los activos de la información, sus vulnerabilidades y riesgos, se debe proseguir a estimar su valor y ponderarlos, para darles un adecuado tratamiento. Las posibles acciones a realizar son aceptarlo, transferirlo, eliminarlo o mitigarlo.

Por lo anteriormente descripto, cobra relevancia el concepto de control, que implica el conjunto de actividades orientadas a mitigar un riesgo. Estos pueden ser:

- Automático: llevados a cabo por un sistema computarizado
- Manual: efectuados por una persona de forma manual
- Preventivo: se los implementa con el objetivo de impedir que ocurran eventos no deseados
- Detectivo: ejecutados para descubrir situaciones no queridas
- Correctivo: se los implementa para corregir un riesgo o mitigarlo con posterioridad a la ocurrencia del acontecimiento

La dirección del ente debe determinar el apetito de riesgo. A partir de ello, el área técnica propondrá todos los controles que sean necesarios, comparándolos con los indicados en el “Anexo A” de ISO 27001, corroborando que no se hayan omitido otros considerados pertinentes (se expondrá el riesgo remanente a la dirección para concientizar sobre el riesgo asumido).

En este aspecto es importante aclarar que debe efectuarse un documento que contenga una “declaración de aplicabilidad” respecto a los controles necesarios y la justificación de su inclusión o exclusión en la organización en particular.

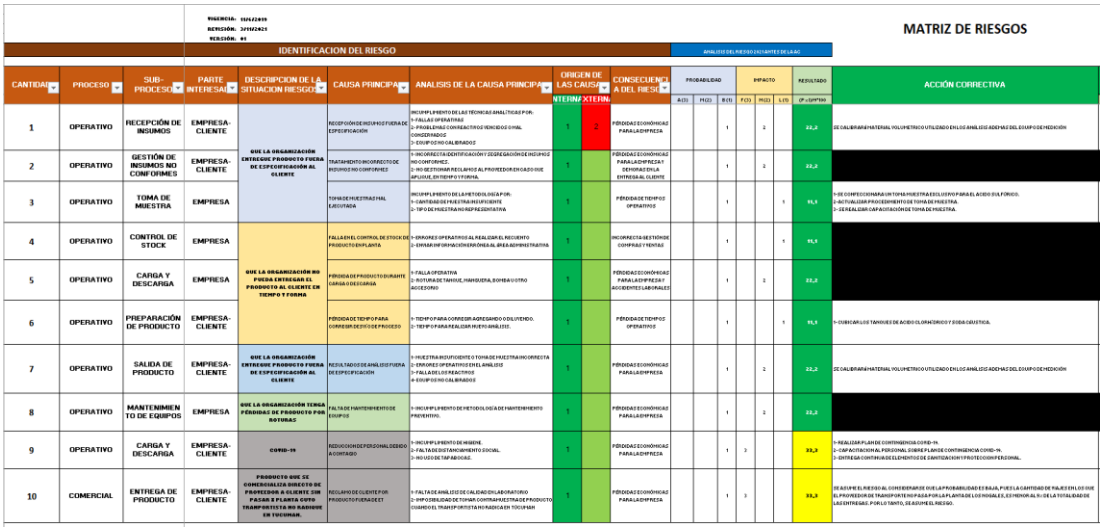
Finalmente, a cada riesgo identificado se le determinará la efectividad del control asociado, lo que implica su capacidad (o en conjunto con otros) para reducir su probabilidad de ocurrencia y/o el impacto evaluado.

Se hace referencia a que el activo de información puede quedar expuesto a un riesgo remanente, a pesar de la aplicación de controles sobre sus riesgos inherentes. A esto se lo conoce como riesgo residual, que es aquel que el control no llega a atenuar. Matemáticamente se lo representa como el producto entre el riesgo inherente y la efectividad del control.

Se verifica que la organización objeto de estudio efectúa una evaluación de riesgos en los siguientes documentos:

- Análisis de Contexto – FODA (contexto)
- Partes Interesadas (contexto)
- Matriz de riesgos de proceso (negocio)
- Planilla de Seguimiento de reclamos, desvíos y acciones correctivas

Sin embargo, para cumplimentar lo requerido en ISO 27001, se deberá efectuar una evaluación del riesgo sobre aquellos que afectan específicamente a la seguridad de la información. En este sentido, deberá confeccionarse la declaración de aplicabilidad de dichos controles. Asimismo, como se hizo mención anteriormente, sería recomendable la implementación de una técnica para la gestión de riesgo que se base en un estándar internacional, como ser ISO 31000 o ISO 27005.



MATRIZ DE RIESGOS

| CANTIDAD | PROCESO | SUB-PROCESO | PARTE INTERESADA | DESCRIPCION DE LA SITUACION RIESGOSA | CAUSA PRINCIPAL | ANALISIS DE LA CAUSA PRINCIPAL | ORIGEN DE LAS CAUSAS | | CONSECUENCIA DEL RIESGO | PROBABILIDAD | | | IMPACTO | | | RESULTADO | ACCIÓN CORRECTIVA |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | INTERNA | EXTERNA | | A(3) | M(2) | B(1) | F(3) | M(2) | L(1) | (P x IMPTO) | |
| 1 | OPERATIVO | RECEPCIÓN DE INSUMOS | EMPRESA-CLIENTE | QUE LA ORGANIZACIÓN ENTREGUE PRODUCTO FUERA DE ESPECIFICACIÓN AL CLIENTE | RECEPCIÓN DE INSUMO FUERA DE ESPECIFICACIÓN | INCUMPLIMIENTO DE LAS TÉCNICAS ANALÍTICAS DEBIDO POR:<br>1- FALLAS OPERATIVAS<br>2- PROBLEMAS CON REACTIVOS VENCIDOS O MAL CONSERVADOS<br>3- EQUIPOS NO CALIBRADOS | 1 | 2 | PÉRDIDAS ECONÓMICAS PARA LA EMPRESA | | | 1 | | 2 | | 2,2 | DE CALIBRAR MATERIAL VOLUMETRICO UTILIZADO EN LOS ANÁLISIS AGREGAR DEL EQUIPO DE MEDICIÓN |
| 2 | OPERATIVO | GESTIÓN DE INSUMOS NO CONFORMES | EMPRESA-CLIENTE | | TRATAMIENTO INCORRECTO DE INSUMOS NO CONFORMES | 1- INCORRECTA IDENTIFICACIÓN Y SEGREGACIÓN DE INSUMOS NO CONFORMES.<br>2- NO GESTIONAR RECLAMOS AL PROVEEDOR EN CASO QUE APLIQUE, EN TIEMPO Y FORMA. | 1 | | PÉRDIDAS ECONÓMICAS PARA LA EMPRESA Y DEMORA EN LA ENTREGA AL CLIENTE | | | 1 | | 2 | | 2,2 | |
| 3 | OPERATIVO | TOMA DE MUESTRA | EMPRESA | | TOMA DE MUESTRA FINAL LIGUITADA | INCUMPLIMIENTO DE LA METODOLOGÍA POR:<br>1- CANTIDAD DE MUESTRA INSUFICIENTE<br>2- TIPO DE MUESTRA NO REPRESENTATIVA | 1 | | PÉRDIDAS DE TIEMPOS OPERATIVOS | | | 1 | | | 1 | 1,1 | 1- SE CONFECCIONARÁ UN TOMA MUESTRA EXCLUSIVO PARA EL ACIDO CLORHÍDRICO.<br>2- ACTUALIZAR PROCEDIMIENTO DE TOMA DE MUESTRA.<br>3- SE REALIZARÁ CAPACITACIÓN DE TOMA DE MUESTRA. |
| 4 | OPERATIVO | CONTROL DE STOCK | EMPRESA | QUE LA ORGANIZACIÓN NO PUEDA ENTREGAR EL PRODUCTO AL CLIENTE EN TIEMPO Y FORMA | FALLA EN EL CONTROL DE STOCK DE PRODUCTO EN PLANTA | 1- ERRORES OPERATIVOS AL REALIZAR EL RECUENTO<br>2- DEMORA EN INFORMACIÓN ERRÓNEA AL ÁREA ADMINISTRATIVA | 1 | | INCORRECTA GESTIÓN DE COMPRAS Y VENTAS | | | 1 | | | 1 | 1,1 | |
| 5 | OPERATIVO | CARGA Y DESCARGA | EMPRESA | | PÉRDIDA DE PRODUCTO DURANTE CARGA O DESCARGA | 1- FALLA OPERATIVA<br>2- ROTURA DE TANQUE, MANGUERA, BOMBA U OTRO ACCESORIO | 1 | | PÉRDIDAS ECONÓMICAS PARA LA EMPRESA Y ACCIDENTES LABORALES | | | 1 | | 2 | | 2,2 | |
| 6 | OPERATIVO | PREPARACIÓN DE PRODUCTO | EMPRESA-CLIENTE | | PÉRDIDA DE TIEMPO PARA CORREGIR DEFECTO DEL PROCESO | 1- TIEMPO PARA CORREGIR AGREGANDO O DILUYENDO.<br>2- TIEMPO PARA REALIZAR NUEVO ANÁLISIS. | 1 | | PÉRDIDAS DE TIEMPOS OPERATIVOS | | | 1 | | | 1 | 1,1 | 1- CUBICAR LOS TANQUES DE ÁCIDO CLORHÍDRICO Y SODA CÁUSTICA. |
| 7 | OPERATIVO | SALIDA DE PRODUCTO | EMPRESA-CLIENTE | QUE LA ORGANIZACIÓN ENTREGUE PRODUCTO FUERA DE ESPECIFICACIÓN AL CLIENTE | RESULTADO DE ANÁLISIS FUERA DE ESPECIFICACIÓN | 1- MUESTRA INSUFICIENTE O TOMA DE MUESTRA INCORRECTA<br>2- ERRORES OPERATIVOS EN EL ANÁLISIS<br>3- FALLAS EN LOS REACTIVOS<br>4- EQUIPOS NO CALIBRADOS | 1 | | PÉRDIDAS ECONÓMICAS PARA LA EMPRESA | | | 1 | | 2 | | 2,2 | DE CALIBRAR MATERIAL VOLUMETRICO UTILIZADO EN LOS ANÁLISIS AGREGAR DEL EQUIPO DE MEDICIÓN |
| 8 | OPERATIVO | MANTENIMIENTO DE EQUIPOS | EMPRESA | QUE LA ORGANIZACIÓN TENGA PÉRDIDAS DE PRODUCTO POR ROTURAS | FALTA DE MANTENIMIENTO DE EQUIPOS | 1- INCUMPLIMIENTO DE METODOLOGÍA DE MANTENIMIENTO PREVENTIVO. | 1 | | PÉRDIDAS ECONÓMICAS PARA LA EMPRESA | | | 1 | | 2 | | 2,2 | |
| 9 | OPERATIVO | CARGA Y DESCARGA | EMPRESA-CLIENTE | COVID-19 | REDUCCIÓN DE PERSONAL DEBIDO A CONTAGIO | 1- INCUMPLIMIENTO DE HIGIENE.<br>2- FALTA DE DISTANCIAMIENTO SOCIAL.<br>3- NO USO DE TAPABOCAS. | 1 | | PÉRDIDAS ECONÓMICAS PARA LA EMPRESA | | | 1 | 3 | | | 3,3 | 1- REALIZAR PLAN DE CONTINGENCIA COVID-19.<br>2- CAPACITACIÓN AL PERSONAL SOBRE PLAN DE CONTINGENCIA COVID-19.<br>3- ENTREGA CONTINUA DE ELEMENTOS DE DANTIDAD CON PROTOCOLO PERSONAL. |
| 10 | COMERCIAL | ENTREGA DE PRODUCTO | EMPRESA-CLIENTE | PRODUCTO QUE SE COMERCIALICE DIRECTO DE PROVEEDOR A CLIENTE SIN PASAR X PLANTA CUYO TRANSPORTISTA NO RADIQUE EN TUCUMAN. | RECLAMO DE CLIENTE POR PRODUCTO FUERA DE ESET | 1- FALTA DE ANÁLISIS DE CALIDAD EN LABORATORIO<br>2- IMPOSIBILIDAD DE TOMAR CONTRAMUESTRA DE PRODUCTO CUANDO EL TRANSPORTISTA NO RADICA EN TUCUMAN | 1 | | PÉRDIDAS ECONÓMICAS PARA LA EMPRESA | | | 1 | 3 | | | 3,3 | DE AGUARDAR EL RIESGO AL CONSIDERARSE QUE LA PROBABILIDAD ES BAJA, PUES LA CANTIDAD DE PALETS EN LOS QUE EL PROVEEDOR DE TRANSPORTE NO PASA POR LA PLANTA DE LOS PEDIDOS, ES MENOR AL 5% DE LA TOTALIDAD DE LAS ENTREGAS. POR LO TANTO, SE ASUME EL RIESGO. |

*Ilustración 9: Matriz de riesgos de procesos*

| | | |
|---|---|---|
| PROBABILIDAD | ALTA | QUE EL EVENTO SE PRODUZCA TODOS LOS MESES |
| | MEDIA | QUE EL EVENTO SE PRODUZCA ENTRE ENTRE 2 A 3 VECES EN EL AÑO |
| | BAJA | QUE EL EVENTO SE PRODUZCA POR LO MENOS 1 VEZ EN EL AÑO |
| | | |
| IMPACTO | FUERTE | QUE EL EVENTO GENERE RECLAMOS EN CLIENTES EXTERNOS E INTERNOS O PERDIDA ECONOMICA EN LA ORGANIZACIÓN |
| | MODERADO | QUE EL EVENTO GENERE ALTERACION DEL PROCESO (RETRASOS) SIN PRODUCIR RECLAMOS O PERDIDAS ECONOMICAS |
| | LEVE | QUE EL EVENTO NO GENERE ALTERACION EN EL PROCESO NI RECLAMOS NI PERDIDAS ECONOMICAS |

*Ilustración 10: Criterios para el análisis del riesgo*

### *3.4.5 Objetivos de SI y planificación para los logros.*

El ente debe fijar objetivos de seguridad de la información de manera oportuna, para las distintas funciones y niveles organizacionales, a fin de garantizar la integridad, disponibilidad y confidencialidad de sus activos informáticos, teniendo en cuenta la criticidad de la información que manejan. Estos deben ser coherentes a la política fijada, medibles y acordes a las salidas de la evaluación y tratamiento del riesgo. Además, corresponde que sean comunicados a los miembros de la organización y actualizados con la periodicidad que corresponda.

También, al planificar los objetivos de seguridad de la información, debe asignarse un responsable para efectuar su actualización, seguimiento, establecer su adecuado momento de medición y metodología utilizada para la evaluación de sus resultados.

La empresa analizada no tiene establecidos objetivos de seguridad de la información, por lo que se proponen los siguientes (los mismos podrían ser re adecuados o ampliados a consideración de la dirección):

- Que los colaboradores realicen un uso aceptable, según los parámetros definidos, de los activos de la organización.
- Guardar la documentación papel en lugares adecuados para tal fin y bajo llave en caso de corresponder, según la clasificación de sensibilidad asignada.
- Que los integrantes de la compañía trabajen con una política de escritorios limpios y monitores despejados.
- Que se tomen los recaudos necesarios para la transferencia electrónica de información digital, evitando de este modo la violación de las características de confidencialidad, integridad y disponibilidad.
- Restringir la instalación de software sin licencia y de aquellos programas que no sean prescindibles para las labores habituales en las estaciones de trabajo.
- Realizar copias de seguridad periódicas.
- Asegurar la protección contra el software malicioso, a través de la instalación de antimalware y afines.
- Realizar controles criptográficos, para el envío de información y documentación digital confidencial.
- Mantener el debido cuidado con las bases de datos de proveedores y clientes, evitando la fuga de la información personal identificable.
- Impedir la extracción de la información confidencial de la empresa, mediante la inhabilitación de los puertos USB de las terminales de trabajo.

## 3.5 Soporte

En el apartado 7, la norma aborda cuestiones relacionadas a los recursos necesarios para el correcto funcionamiento de un SGSI, sus competencias necesarias y la concientización requerida. Además, se describen los requisitos documentales respecto a los controles de la información.

### *3.5.1 Recursos.*

Debe diseñarse una estructura dotada de los recursos necesarios para el establecimiento, mantenimiento y mejora continua de la seguridad de la

información. Estos están conformados por capital humano, recursos materiales, financieros, económicos y activos intangibles.

La norma, en su apartado 7.1, no establece un requerimiento específico que indique la manera de evidenciar la adecuada asignación de recursos. Es por ello que se recomienda realizar un detalle de aquellos considerados necesarios, vinculados con la implementación y seguimiento del sistema de gestión.

La empresa objeto de estudio debería realizar un listado de los recursos necesarios para la implementación de un SGSI (teniendo en cuenta el alcance previamente definido), pues no cuenta con los perfiles suficientes en el ámbito analizado en el presente trabajo. Sin embargo, se verifica la existencia de recursos materiales y tecnológicos adecuados para la realización de las tareas laborales que actualmente lleva a cabo el personal.

### *3.5.2 Competencia.*

En esta exigencia, se espera que la organización establezca la competencia necesaria del capital humano que efectúe tareas vinculadas con la seguridad de la información[7]. Esta competencia podrá ser evidenciada con el nivel de educación, capacitaciones o experiencia laboral de los perfiles. En caso de corresponder deberán realizarse las acciones necesarias para que el personal adquiera las habilidades requeridas (capacitaciones).

Como medio de prueba de las competencias de las personas involucradas en el SGSI, se deberá conservar la información documentada que sea necesaria: *currículum vitae*, registros de capacitación, matrices de polivalencia, evaluaciones de desempeño, entre otros.

Para cumplimentar este requisito, también deberá disponerse de documentación específica, como ser: perfiles de puestos, manual de funciones, procedimientos de trabajo, organigrama,

Se observa que la organización analizada posee un organigrama formalmente definido, perfiles de puesto y un conjunto de procedimientos escritos para dar cumplimiento a sus objetivos de negocio. Se evidencia la existencia de legajos del personal adecuadamente resguardados, que

[7] Véase apartado 3.3.4 - Roles, responsabilidades y autoridades.

conservan la documentación exigida por ISO 9001 y la normativa laboral vigente, para cada uno de ellos.

Sin embargo, debería hacerse una readecuación de la estructura de la empresa y sus perfiles de puesto, para dar cumplimiento a los requisitos de seguridad de la información que plantea ISO 27001. También correspondería definir procedimientos específicos vinculados a la temática tratada en el presente.

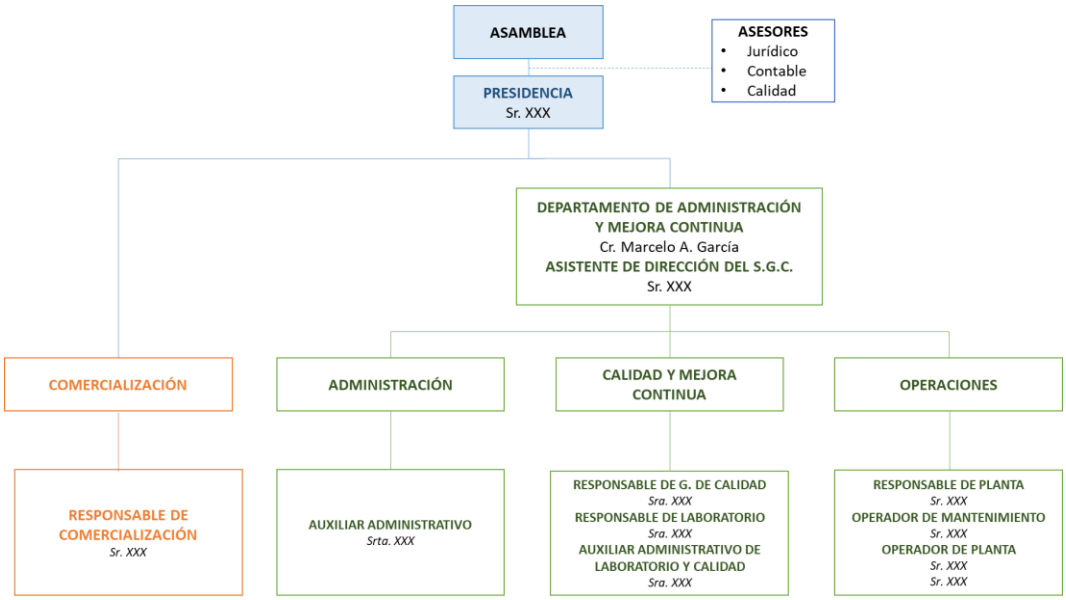



*Ilustración 11: Estructura organizacional de la empresa analizada*

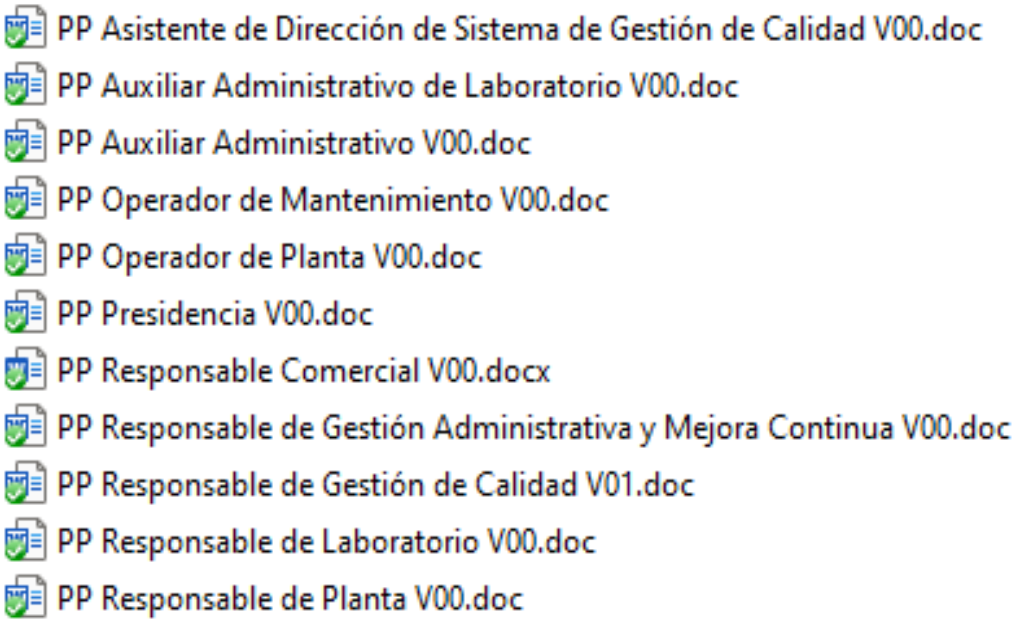



*Ilustración 12: Perfiles de puestos documentados*

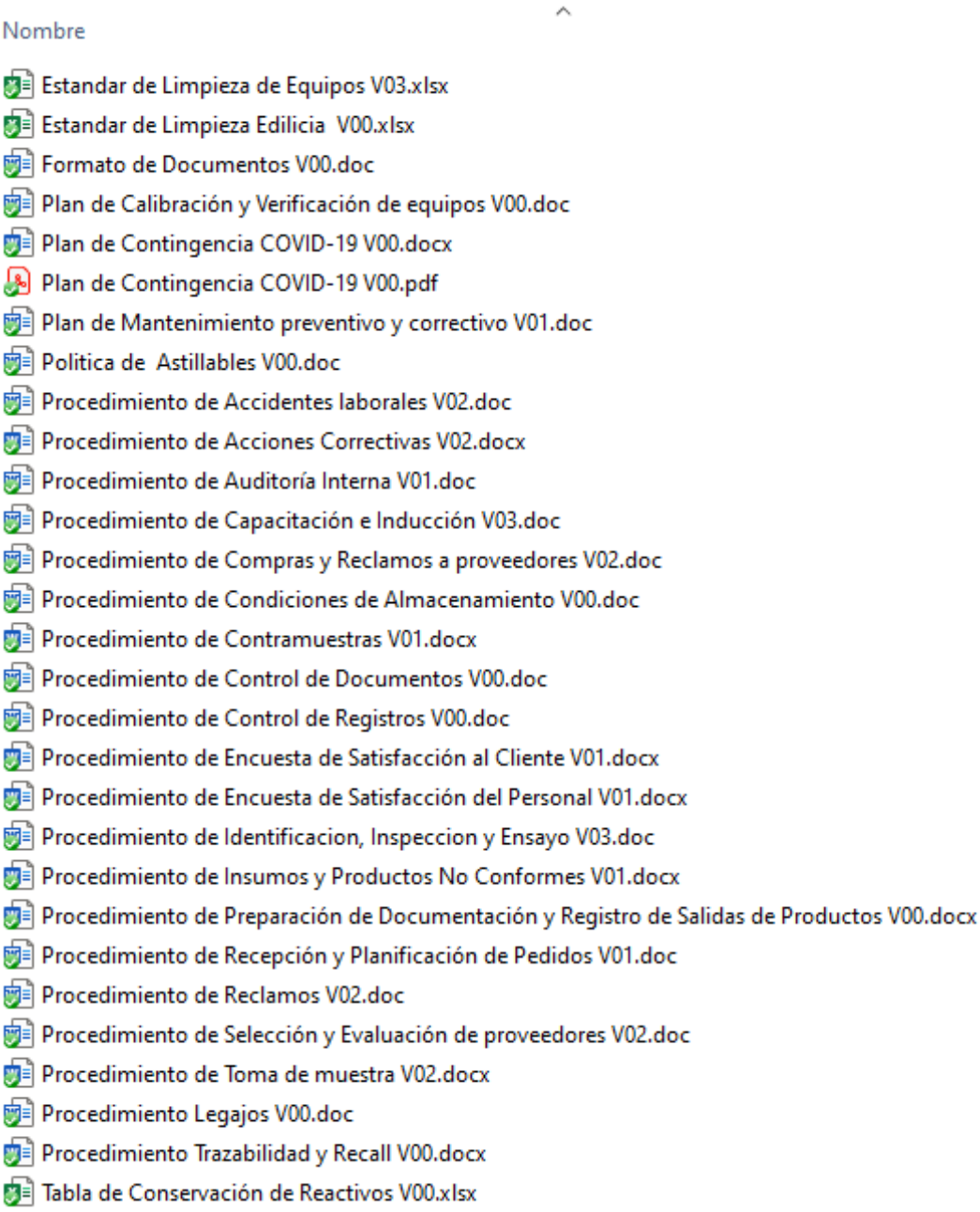
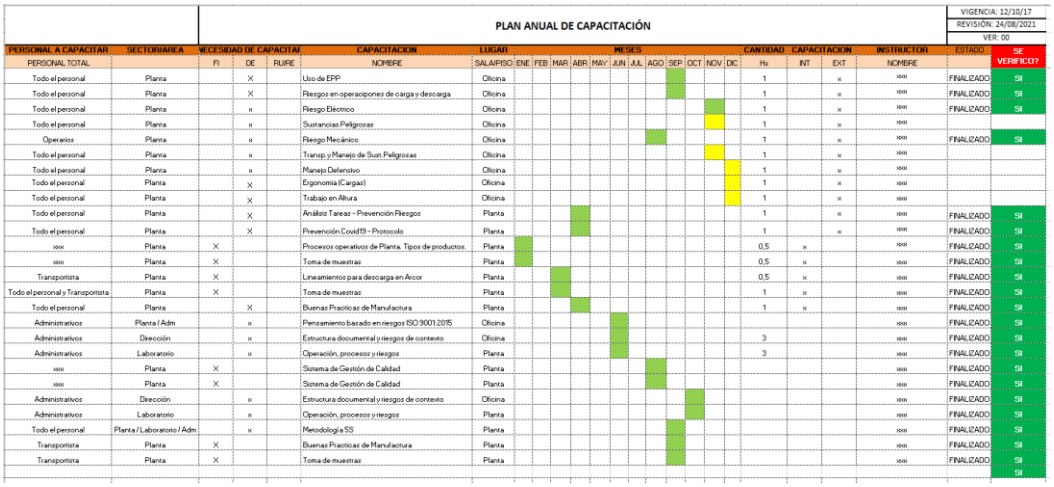



*Ilustración 13: Procedimientos de trabajo documentados*

También, se comprueba que la empresa cuenta con un “Plan Anual de Capacitaciones” y un “Procedimiento de Capacitación e Inducción”. Actualmente no se cuenta con actividades relacionadas a seguridad de la información. Las mismas están enfocadas a calidad y seguridad e higiene laboral. Sin embargo, puede utilizarse la misma herramienta para cumplimentar esta exigencia.



PLAN ANUAL DE CAPACITACIÓN

VIGENCIA: 12/10/17
REVISIÓN: 24/08/2021
VER: 00

| PERSONAL A CAPACITAR | SECTOR/AREA | NECESIDAD DE CAPACITAR | | | CAPACITACION | LUGAR | MESES | | | | | | | | | | | CANTIDAD | CAPACITACION | | INSTRUCTOR | ESTADO | SE VERIFICO? |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| PERSONAL TOTAL | | FI | DE | RUIRE | NOMBRE | SALA/PISO | ENE | FEB | MAR | ABR | MAY | JUN | JUL | AGO | SEP | OCT | NOV | DIC | Hs | INT | EXT | NOMBRE | | |
| Todo el personal | Planta | | X | | Uso de EPP | Oficina | | | | | | | | | | | | | 1 | | x | xxx | FINALIZADO | SI |
| Todo el personal | Planta | | X | | Riesgos en operaciones de carga y descarga | Oficina | | | | | | | | | | | | | 1 | | x | xxx | FINALIZADO | SI |
| Todo el personal | Planta | | x | | Riesgo Eléctrico | Oficina | | | | | | | | | | | | | 1 | | x | xxx | FINALIZADO | SI |
| Todo el personal | Planta | | x | | Sustancias Peligrosas | Oficina | | | | | | | | | | | | | 1 | | x | xxx | | |
| Operarios | Planta | | x | | Riesgo Mecánico | Oficina | | | | | | | | | | | | | 1 | | x | xxx | FINALIZADO | SI |
| Todo el personal | Planta | | x | | Transp.y Manejo de Sust.Peligrosas | Oficina | | | | | | | | | | | | | 1 | | x | xxx | | |
| Todo el personal | Planta | | x | | Manejo Defensivo | Oficina | | | | | | | | | | | | | 1 | | x | xxx | | |
| Todo el personal | Planta | | X | | Ergonomía (Cargas) | Oficina | | | | | | | | | | | | | 1 | | x | xxx | | |
| Todo el personal | Planta | | X | | Trabajo en Altura | Oficina | | | | | | | | | | | | | 1 | | x | xxx | | |
| Todo el personal | Planta | | X | | Análisis Tareas - Prevención Riesgos | Planta | | | | | | | | | | | | | 1 | | x | xxx | FINALIZADO | SI |
| Todo el personal | Planta | | X | | Prevención Covid19 - Protocolo | Planta | | | | | | | | | | | | | 1 | | x | xxx | FINALIZADO | SI |
| xxx | Planta | X | | | Procesos operativos de Planta. Tipos de productos. | Planta | | | | | | | | | | | | | 0,5 | x | | xxx | FINALIZADO | SI |
| xxx | Planta | X | | | Toma de muestras | Planta | | | | | | | | | | | | | 0,5 | x | | xxx | FINALIZADO | SI |
| Transportista | Planta | X | | | Lineamientos para descarga en Arcor | Planta | | | | | | | | | | | | | 0,5 | x | | xxx | FINALIZADO | SI |
| Todo el personal y Transportista | Planta | X | | | Toma de muestras | Planta | | | | | | | | | | | | | 1 | x | | xxx | FINALIZADO | SI |
| Todo el personal | Planta | | X | | Buenas Practicas de Manufactura | Planta | | | | | | | | | | | | | 1 | x | | xxx | FINALIZADO | SI |
| Administrativos | Planta / Adm | | x | | Pensamiento basado en riesgos ISO 9001:2015 | Oficina | | | | | | | | | | | | | | | | xxx | FINALIZADO | SI |
| Administrativos | Dirección | | x | | Estructura documental y riesgos de contexto | Oficina | | | | | | | | | | | | | 3 | | | xxx | FINALIZADO | SI |
| Administrativos | Laboratorio | | x | | Operación, procesos y riesgos | Planta | | | | | | | | | | | | | 3 | | | xxx | FINALIZADO | SI |
| xxx | Planta | X | | | Sistema de Gestión de Calidad | Planta | | | | | | | | | | | | | | | | xxx | FINALIZADO | SI |
| xxx | Planta | X | | | Sistema de Gestión de Calidad | Planta | | | | | | | | | | | | | | | | xxx | FINALIZADO | SI |
| Administrativos | Dirección | | x | | Estructura documental y riesgos de contexto | Oficina | | | | | | | | | | | | | | | | xxx | FINALIZADO | SI |
| Administrativos | Laboratorio | | x | | Operación, procesos y riesgos | Planta | | | | | | | | | | | | | | | | xxx | FINALIZADO | SI |
| Todo el personal | Planta / Laboratorio / Adm | | x | | Metodología 5S | Planta | | | | | | | | | | | | | | | | xxx | FINALIZADO | SI |
| Transportista | Planta | X | | | Buenas Practicas de Manufactura | Planta | | | | | | | | | | | | | | | | xxx | FINALIZADO | SI |
| Transportista | Planta | X | | | Toma de muestras | Planta | | | | | | | | | | | | | | | | xxx | FINALIZADO | SI |
| | | | | | | | | | | | | | | | | | | | | | | | | SI |

*Ilustración 14: Registro de capacitaciones*

### *3.5.3 Concientización.*

El personal involucrado al SGSI debe ser consciente de la “Política de Seguridad de la Información”, su contribución a la eficiencia del sistema y a la mejora continua y las consecuencias del no cumplimiento de los requerimientos previstos.

Para dar cumplimiento al punto 7.3 de la norma, puede recurrirse a las siguientes actividades: dar a conocer roles y responsabilidades, comunicar los objetivos de seguridad, publicar las métricas de gestión, incentivar la participación de los miembros del SGSI para la generación de mejoras y el registro de desvíos, incidentes de seguridad y no conformidades, entre otros.

Este apartado está relacionado al concepto de cultura de seguridad de la información, concepto abordado anteriormente en el presente trabajo.

### *3.5.4 Comunicación.*

El apartado 7.4 de la norma indica que debe contarse con un plan de comunicación interna y externa que indique el momento oportuno para informar, destinatarios, remitentes y procedimientos adecuados para hacerlo.

Se verifica que, en la empresa abordada, se planifican reuniones quincenales, en donde se tratan temas relacionados al funcionamiento del sistema de gestión. En el orden del día, podrían incluirse cuestiones relacionadas a la seguridad de la información. Se evidencia que se lleva registro, a través de minutas de reunión, de los temas abordados en cada una de ellas.

Además, se observa que en la empresa está expuesta la “Política de Calidad” y los procedimientos están accesibles para el personal. Lo mismo debería efectuarse para los documentos del SGSI.

### *3.5.5 Información documentada.*

En el punto 7.5 del marco analizado, se establece que el SGSI debe documentar la información requerida por la norma y toda aquella que sea considerada necesaria por el ente, para el logro de los objetivos propuestos. La misma debe estar identificada correctamente y disponible para su consulta y utilización. Debe tenerse un control de revisión y aprobación y estar adecuadamente protegida.

También es importante que se defina, entre otras cuestiones, la distribución, acceso, recuperación, uso, almacenamiento y preservación, conservación y disposición final de la información documentada.

Se verifica que la empresa analizada cuenta con los siguientes elementos relacionados a este requerimiento:

- Procedimiento de formato de documentos V00
- Procedimiento de control de documentos V00
- Procedimiento de control de Registros V00
- Listado de documentos y registros V00
- Repositorio compartido y colaborativo en “Dropbox”, que permite mantener los controles requeridos en la norma

| (LOGO DE LA EMPRESA) | NOMBRE DEL DOCUMENTO | (SECTOR) |
|---|---|---|
| Vigencia | Versión | Revision |
| 22/10/2017 | V:00 | 23/8/2021 |

*Ilustración 15: Encabezado de documentos del Sistema de Gestión en empresa analizada*

## 3.6 Operación

En este capítulo de la norma, se establece que la organización debe planificar, implementar y controlar los procesos necesarios para cumplir con los requerimientos de seguridad de la información, las acciones para tratar los riesgos y las oportunidades. Además, deben planificarse las actividades

necesarias para alcanzar los objetivos de seguridad propuestos. Todo esto debe estar adecuadamente documentado, para evidenciar las acciones efectuadas a tal fin.

Asimismo, la organización debe realizar un control de los desvíos respecto a la planificación anual efectuada, ejecutando las acciones correctivas que sean necesarias para evitar cualquier resultado negativo. También deben controlarse los procesos tercerizados.

Por otro lado, debe definirse la periodicidad de las evaluaciones de riesgo e implementar un plan para tratar aquellos que se hayan identificado.

Lo solicitado en este apartado debe ser completamente abordado por la organización objeto de estudio, en lo que respecta a seguridad de la información. Cabe destacar, como se mencionó anteriormente, que la empresa efectúa evaluaciones de riesgo de cuestiones relativas a calidad, contexto, partes interesadas y riesgo de proceso. Además, lleva un registro y efectúa un seguimiento de los desvíos detectados.

## 3.7 Evaluación de Desempeño

En el apartado 9 de la norma, se solicita evaluar el desempeño de la seguridad de la información y del SGSI. Encontramos aquí cuestiones de análisis y evaluación, revisión por la dirección y auditorías internas.

### *3.7.1 Seguimiento, medición y evaluación.*

La organización debe planificar la forma de monitorear, medir, analizar y evaluar el SGSI. Dentro de este requerimiento deben tenerse en cuenta los aspectos a tratar, metodología, oportunidad de realización y evaluación, responsable de ejecución, entre otros. Además, deben evidenciarse los resultados obtenidos, conservando documentación probatoria.

Cabe destacar que las mediciones son necesarias por los siguientes motivos:

- Permiten adoptar acciones de mejora continua
- Son un mecanismo que permiten validar acciones correctivas y oportunidades de mejora adoptadas con anterioridad
- Posibilitan asignar mayores o diferentes recursos a áreas con necesidades

➢ Evidencian objetivamente las decisiones tomadas y los resultados asociados

Se observa en la empresa analizada, que cuentan con un archivo denominado “Plan Operativo Anual”, en donde se exponen los indicadores de gestión de cada uno de los aspectos solicitados para su Sistema de Gestión.

Además, cuentan con un documento llamado “Indicadores de Gestión V00”, en donde se muestran los resultados de cada una de las métricas, su composición y gráficos ilustrativos. Sin embargo, se evidencia que no se llevan indicadores relacionados a seguridad de la información, por lo que se deberían diseñar métricas específicas.

| ACTIVIDADES | PROGRAMA OPERATIVO ANUAL= POA | NOMBRE DEL INDICADOR | | OBJETIVO | | | | | | | | TIPO DE INDICADOR | FRECUENCIA DE MEDICIÓN |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | OBJETIVO PLANTEADO | INDICADOR ASOCIADO | RATIO | OBJ. PERIODO 2018 | V.R AL CIERRE | OBJ. PERIODO 2019 | V.R AL CIERRE | OBJ. PERIODO 2020 | V.R AL CIERRE | OBJ. PERIODO 2021 | V.R AL CIERRE al 30/10/21 | ESTADÍSTICO / GESTIÓN | |
| Nº | ENFOQUE EN CALIDAD | A | | | | | | | | | | | |
| OBJETIVO Nº 1 | | INDICADOR 01 | Explicación del ratio 01 | 80% | 95% | 85% | 85% | 87% | 90% | 89% | 89,2% | Gestión | Anual |
| | | INDICADOR 02 | Explicación del ratio 02 | | | | | 80% | 100% | 85% | 100% | Gestión | Mensual |
| | | INDICADOR 03 | Explicación del ratio 03 | | | | | | | 69,69% | VER EN PLANILLA | Gestión | Anual |
| 1 | ACTIVIDAD Nº 1 | | | | | | | | | | | | |
| 2 | ACTIVIDAD Nº 2 | | | | | | | | | | | | |
| 3 | ACTIVIDAD Nº 3 | | | | | | | | | | | | |
| OBJETIVO Nº 2 | | INDICADOR 04 | Explicación del ratio 04 | 5 | 1 | 3 | 0 | 2 | 6 | 5% | 0,2% | Gestión | Mensual |
| | | INDICADOR 05 | Explicación del ratio 05 | 10% | 0% | 5% | 0% | 3% | 0% | 2% | 0% | Gestión | Mensual |
| 1 | ACTIVIDAD Nº 1 | | | | | | | | | | | | |
| 2 | ACTIVIDAD Nº 2 | | | | | | | | | | | | |
| 3 | ACTIVIDAD Nº 3 | | | | | | | | | | | | |
| Nº | ENFOQUE EN CAPITAL HUMANO | B | | | | | | | | | | | |
| Nº | ENFOQUE EN COMPRAS | C | | | | | | | | | | | |
| Nº | ENFOQUE EN RENTABILIDAD | D | | | | | | | | | | | |
| Nº | ENFOQUE EN PROCESO | E | | | | | | | | | | | |

*Ilustración 16: Programa Operativo Anual*

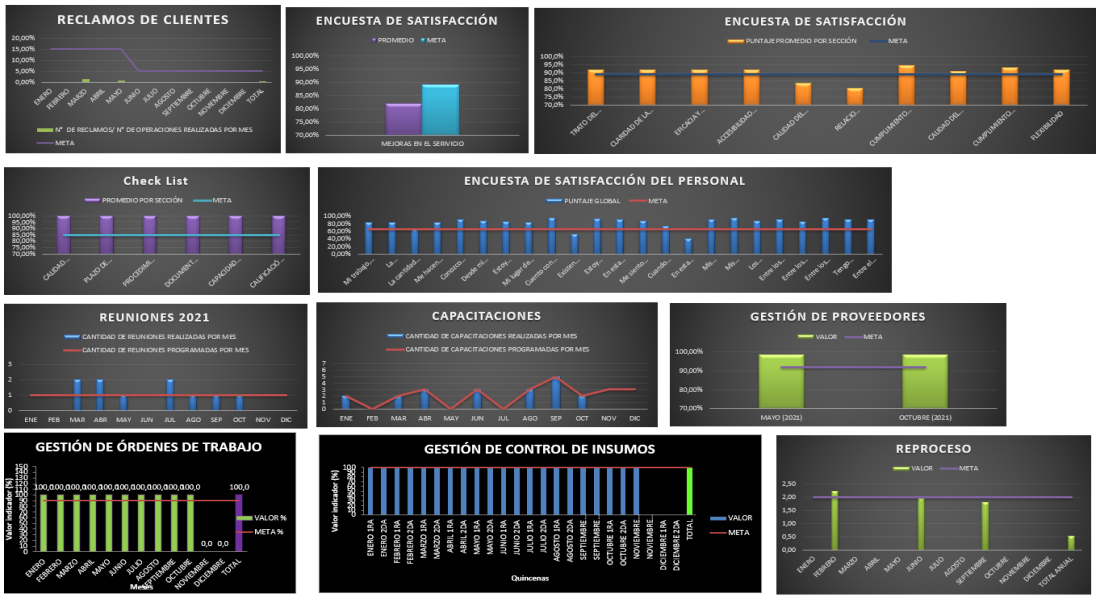



*Ilustración 17: Indicadores de Gestión de la empresa analizada*

### *3.7.2 Auditoría interna.*

En el punto 9.3 se indica que la organización debe realizar periódicamente auditorías internas para informar acerca del nivel de cumplimiento de los requisitos propios y los de la norma, especificándose cuales son los aspectos que deben corregirse o mejorarse.

El proceso de auditoría es una de las herramientas más importantes para la mejora continua de los sistemas de gestión. El éxito de la misma, depende en gran medida de los auditores, por lo que su formación es de fundamental importancia para la organización.

Una auditoría se define como una “revisión sistemática de una actividad o de una situación para evaluar el cumplimiento de las reglas o criterios objetivos a que aquellas deben someterse” (Real Academia Española, s.f.). Para efectuarla se toman en cuenta los requisitos de ISO 27001 y normas relacionadas, políticas, procedimientos, legislación aplicable, códigos de ética y de conducta, entre otros.

Para el cumplimiento de este apartado la organización debería:

- Definir un programa de auditoría que contenga la frecuencia, métodos, responsabilidades y los requisitos de la planificación y presentación de los respectivos informes
- Establecer criterios y alcance de la actividad
- Escoger auditores y efectuar auditorías de manera objetiva e imparcial
- Determinar un mecanismo que asegure que los resultados sean informados a la dirección
- Archivar información documentada como evidencia de la realización y respaldo de los resultados de auditoría

Se observa que la organización estudiada efectúa auditorías internas periódicas y cuenta con los siguientes archivos para dar cumplimiento a este requerimiento:

- Procedimiento de Auditoría Interna V01
- Cronograma de Auditoría Interna V00
- Plan de Auditoría – Año 20XX
- Informe de Auditoría – Período XX

Podrían utilizarse las herramientas que ya se encuentran implementadas, incluyéndose actividades relacionadas a los requisitos de la ISO 27001.

**CRONOGRAMA DE AUDITORIA**

| Vigencia | | Revision |
|---|---|---|
| 12/10/2017 | Version: 00 | 20/5/2021 |

| MES AUDITORIA | xxx | AUDITOR | xxx | SISTEMA AUDITADO | ISO 9001:2015 | NEGRO | FERIADO-DESCANSO |
|---|---|---|---|---|---|---|---|
| | | | | | | GRIS | PLANIFICADO |
| | | | | | | VERDE | AUDITADO |

| | ago-21 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | sep-21 | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | DOM | LUN. | MAR. | MIÉ. | JUE. | VIE. | SÁB. | DOM. | LUN. | MAR. | MIÉ. | JUE. | VIE. | SÁB. | DOM. | LUN. | MAR. | MIÉ. | JUE. | VIE. | SÁB. | DOM. | LUN. | MAR. | MIÉ. | JUE. | VIE. | SÁB. | DOM. | LUN | MAR | LUN | | | | |
| SECTOR AUDITADO | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 | 26 | 27 | 28 | 29 | 30 | 31 | 1 | | | | |
| DIRECCION | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| ADMINISTRACION | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| LABORATORIO | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| TALLER | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| CARGA Y DESCARGA | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |

*Ilustración 18: Cronograma de Auditoría*

### *3.7.3 Revisión por parte de la Dirección.*

La dirección de la organización debe revisar periódicamente el SGSI para asegurar que el mismo esté actualizado, es decir, que sea pertinente, adecuado y eficaz. Debe conservarse la documentación que evidencie su resultado.

Este requerimiento de la norma, muestra la necesidad del compromiso de la alta dirección con el SGSI. Es decir, que debe involucrarse con los resultados y tomar las decisiones necesarias para el nuevo período que incluye la adecuación de recursos, objetivos y mejoras.

En el punto 9.3 de la norma se establece que este documento debe contener por lo menos los siguientes elementos:

- Acciones correctivas detectadas con anterioridad por parte del órgano director
- Cambios efectuados relacionados al SGSI
- Información relacionada al desempeño de la seguridad de la información, como ser: no conformidades, acciones correctivas, métricas, resultados de auditorías internas y el nivel de cumplimientos de los objetivos de seguridad de la información
- Retroalimentación de las partes interesadas
- Efectos de la evaluación de riesgo y situación de respectivo tratamiento
- Oportunidades de mejora

Finalmente, deben presentarse conclusiones o salidas, que incluyan las decisiones que se tomaron para aprovechar oportunidades de mejora y corregir los desvíos que se hayan oportunamente detectado.

Se observa que la empresa analizada confecciona anualmente un documento que aborda la “revisión por parte de la dirección”. Hasta el momento no se incluyeron cuestiones relacionadas a seguridad de la información, por lo que debería considerárselo.

Sin embargo, se evidencia que, en el último informe presentado, se propone como actividad para el año en curso “identificar riesgos y amenazas informáticas”, lo que se considera un punto de partida para la implementación de un “sistema integrado de gestión” que cumpla con requisitos de seguridad de la información.

## 3.8 Mejora

Tomando como referencia el Ciclo de Deming, el último capítulo normativo de ISO 27001, es el que tiene una mayor vinculación con la última etapa de esta metodología, el “actuar”. En este apartado se abordarán los requisitos de las no conformidades y acciones correctivas, los cuales están relacionados con la mejora continua.

### *3.8.1 No conformidad y acción correctiva.*

Una no conformidad es un incumplimiento a un requisito de la norma o de seguridad de la información. Por su parte, una acción correctiva es aquella que se efectúa para corregir un producto no conforme y eliminar las causas de las no conformidades, evitando que se repitan. Debe evaluarse posteriormente la eficacia de todas las acciones correctivas, conservando toda la información documental como evidencia.

Se observa que la empresa objeto de análisis, confecciona una “Planilla de Seguimiento de Reclamos, Desvíos y Acciones Correctivas V01”, en donde se efectúa un control y seguimiento de todos estos aspectos. En la misma se identifica el desvío y se efectúa su correspondiente tratamiento, seguimiento, evaluación de eficacia y riesgo. Esta misma herramienta podría utilizarse para el registro de los desvíos relacionados a ISO 27001.

### *3.8.2 Mejora continua.*

El punto 10.2 del *framework* reza que “la organización debe mejorar continuamente la pertinencia, la adecuación y la eficiencia del SGSI” (ISO/IEC 27001, 2013, pág. 18).

Esto involucra integrar sistemáticamente los procesos de mejora del SGSI dentro los habituales de revisión y control de la compañía. En este aspecto, están implicadas cuestiones relacionadas a la comunicación y la madurez de la cultura de seguridad de la información, para lograr de este modo, la participación activa de todo el personal (NormaISO27001.es, s.f.).

Para alcanzar este requisito, puede recurrirse a alguna de las siguientes herramientas:

- Detección de nuevas necesidades de las partes interesadas, como por ejemplo: protección de datos personales, privacidad, entre otros
- Acciones correctivas sobre desvíos
- Revisión por parte de la Dirección
- Adecuación de los objetivos de Seguridad de la Información
- Resultados de las auditorías internas y externas
- Seguimiento y medición de indicadores
- Evaluaciones periódicas de riesgos
- Informes sobre incidentes de seguridad
- Valoraciones respecto al nivel de cumplimiento por parte de los proveedores de servicios

# 4 Controles de Seguridad a implementarse

## 4.1 Objetivos de control y controles de referencia (Anexo A)

En el presente capítulo se presentan los controles del "Anexo A" del marco ISO 27001 (ISO/IEC, 2021) según el texto revisado en octubre de 2021 que enmienda[8] la versión del año 2013, indicando aquellos que son aplicables a la organización objeto de estudio.

Cabe destacar que es factible, en casos particulares, excluir algunos de los controles del anexo de la norma, pero esta situación debe ser debidamente justificada, teniendo en cuenta la "evaluación de riesgos" efectuada[9].

### *4.1.1 Controles organizacionales.*

| Nº | DETALLE | CONTROL | APLICABLE |
|---|---|---|---|
| A.5.1 | Política de seguridad de la información | La política de seguridad de la información y otras de aspectos específicos deben ser definidas y aprobadas por la Dirección. Además, deben ser publicadas, comunicadas y darse a conocer al personal y partes interesadas.<br>Deben revisarse a intervalos de tiempo planificados y verificar si se produjeron cambios significativos. | SI |
| A.5.2 | Roles y responsabilidades de seguridad de la información | Los roles y responsabilidades de seguridad de la información deben definirse y asignarse de acuerdo con las necesidades de la organización. | SI |
| A.5.3 | Segregación de funciones | Deberán segregarse las funciones y las áreas de responsabilidad por oposición. | Si |

[8] Con el objetivo de alinear "Anexo A" de la norma con los controles definidos en la tercera edición de ISO / IEC 27002

[9] Véase apartado "3.4.4 - Acciones para tratar el riesgo"

| | | | |
|---|---|---|---|
| A.5.4 | Responsabilidades de gestión | La dirección debe exigir a todo el personal que aplique la seguridad de la información de acuerdo con la política de seguridad establecida, las políticas y los procedimientos específicos. | Si |
| A.5.5 | Contacto con autoridades | La organización debe establecer y mantener contacto con las autoridades pertinentes. | Si |
| A.5.6 | Contacto con grupos de interés especial | La organización deberá establecer y mantener contacto con grupos de intereses especiales u otros foros especializados en seguridad y asociaciones profesionales. | Si |
| A.5.7 | Inteligencia de amenazas | La información relacionada con las amenazas a la seguridad de la información se recopilará y analizará para producir inteligencia al respecto. | Si |
| A.5.8 | Seguridad de la información en la gestión de proyectos | La seguridad de la información se integrará en la gestión de proyectos. | Si |
| A.5.9 | Inventario de activos de información y otros activos asociados | Se debe desarrollar y mantener un inventario de activos de información y otros activos asociados, incluyendo a sus propietarios. | Si |
| A.5.10 | Uso aceptable de los activos de la información y otros activos asociados | Se deben identificar, documentar e implementar las reglas para el uso aceptable y los procedimientos para el manejo de la información y otros activos asociados. | Si |

| | | | |
|---|---|---|---|
| A.5.11 | Devolución de activos | El personal y otras partes interesadas, según corresponda, devolverán todos los activos de la organización que estén en su poder al cambiar o terminar su empleo, contrato o acuerdo. | Si |
| A.5.12 | Clasificación de la información | La información se clasificará de acuerdo con las necesidades de seguridad de la información de la organización en base a la confidencialidad, integridad, disponibilidad y otros requisitos pertinentes de las partes interesadas. | Si |
| A.5.13 | Etiquetado de información | Se debe desarrollar e implementar un conjunto apropiado de procedimientos para el etiquetado de la información de acuerdo con el esquema de clasificación de la información adoptado por la organización. | Si |
| A.5.14 | Transferencia de información | Deben existir reglas, procedimientos o acuerdos de transferencia de información dentro de la organización y entre la organización y otras partes. | Si |
| A.5.15 | Control de acceso | Se deben establecer e implementar reglas para controlar el acceso físico y lógico a la información y otros activos asociados en base a los requisitos de seguridad de la información y del negocio. | Si |

| | | | |
|---|---|---|---|
| A.5.16 | Gestión de identidad | Se gestionará el ciclo de vida completo de las identidades. | Si |
| A.5.17 | Información de autenticación | La asignación y la gestión de la información de autenticación deben estar controladas por un proceso de gestión, que incluye asesorar al personal sobre el manejo adecuado de la información de autenticación. | Si |
| A.5.18 | Derechos de acceso | Los derechos de acceso a la información y otros activos asociados deben ser aprovisionados, revisados, modificados y eliminados de acuerdo con una política específica y reglas para el control de acceso. | Si |
| A.5.19 | Seguridad de la información en las relaciones con los proveedores. | Se deben definir e implementar procesos y procedimientos para gestionar los riesgos de seguridad de la información asociados con el uso de los productos o servicios del proveedor. | Si |
| A.5.20 | Abordar la seguridad de la información dentro de los acuerdos con proveedores | Los requisitos de seguridad de la información relevantes deben establecerse y acordarse con cada proveedor en función del tipo de relación con el proveedor. | Si |
| A.5.21 | Gestión de la seguridad de la información en la cadena de suministro de las TIC | Se deben definir e implementar procesos y procedimientos para gestionar los riesgos de seguridad de la información asociados con la cadena de suministro de productos y servicios de TIC. | No |

| | | | |
|---|---|---|---|
| A.5.22 | Seguimiento, revisión y gestión de cambios de los servicios de proveedores | La organización debe monitorear, revisar, evaluar y gestionar regularmente los cambios en las prácticas de seguridad de la información del proveedor y la prestación de servicios. | Si |
| A.5.23 | Seguridad de la información para el uso de servicios en la nube | Los procesos de adquisición, uso, gestión y salida de los servicios en la nube deben establecerse de acuerdo con los requisitos de seguridad de la información de la organización. | Si |
| A.5.24 | Planificación y preparación de la gestión de incidentes de seguridad de la información | La organización debe planificar y prepararse para la gestión de incidentes de seguridad de la información definiendo, estableciendo y comunicando procesos, roles y responsabilidades de gestión de incidentes de seguridad de la información. | Si |
| A.5.25 | Evaluación y decisión sobre eventos de seguridad de la información | La organización debe evaluar los eventos de seguridad de la información y decidir si deben categorizarse como incidentes. | Si |
| A.5.26 | Respuesta a incidentes de seguridad de la información | Los incidentes de seguridad de la información se responderán de acuerdo con procedimientos documentados. | Si |
| A.5.27 | Aprendizaje de los incidentes de seguridad de la información | El conocimiento obtenido de los incidentes de seguridad de la información se utilizará para fortalecer y mejorar los controles de seguridad de la información. | Si |

| | | | |
|---|---|---|---|
| A.5.28 | Recolección de evidencia | La organización debe establecer e implementar procedimientos para la identificación, recopilación, adquisición y preservación de evidencia relacionada con eventos de seguridad de la información. | Si |
| A.5.29 | Seguridad de la información durante la interrupción | La organización debe planificar cómo mantener la seguridad de la información a un nivel apropiado durante la interrupción. | Si |
| A.5.30 | Preparación de las TIC para la continuidad empresarial | La preparación para las TIC se planificará, implementará, mantendrá y probará en función de los objetivos de continuidad del negocio y los requisitos de continuidad de las TIC. | Si |
| A.5.31 | Requisitos legales, estatutarios, reglamentarios y contractuales | Los requisitos legales, estatutarios, reglamentarios y contractuales relevantes para la seguridad de la información y el enfoque de la organización para cumplir con estos requisitos deben identificarse, documentarse y mantenerse actualizados. | Si |
| A.5.32 | Derechos de propiedad intelectual | La organización debe implementar procedimientos apropiados para proteger los derechos de propiedad intelectual. | No |
| A.5.33 | Protección de registros | Los registros estarán protegidos contra pérdida, destrucción, falsificación, acceso no autorizado y divulgación no autorizada. | Si |

| | | | |
|---|---|---|---|
| A.5.34 | Privacidad y protección la información personal de identificación (PII) | La organización debe identificar y cumplir con los requisitos relacionados con la preservación de la privacidad y la protección de la PII de acuerdo con las leyes y regulaciones aplicables y los requisitos contractuales. | Si |
| A.5.35 | Revisión independiente de la seguridad de la información | El enfoque de la organización para gestionar la seguridad de la información y su implementación, incluidas las personas, los procesos y las tecnologías, debe revisarse de forma independiente a intervalos planificados o cuando se produzcan cambios significativos. | Si |
| A.5.36 | Cumplimiento de políticas, reglas y estándares de seguridad de la información. | Se debe revisar periódicamente el cumplimiento de la política de seguridad de la información de la organización, las políticas, las reglas y los estándares específicos del tema. | Si |
| A.5.37 | Procedimientos operativos documentados | Los procedimientos operativos para las instalaciones de procesamiento de información deben documentarse y ponerse a disposición del personal que los necesite. | Si |

*Ilustración 19: Controles Organizacionales. "Anexo A" - ISO 27001, enmienda N° 1 (2021)*

*4.1.2 Controles de personas.*

| Nº | DETALLE | CONTROL | APLICABLE |
|---|---|---|---|
| A.6.1 | Revisión de antecedentes | La verificación de los antecedentes de todos los candidatos se realizará antes de incorporarse a la organización y de forma continua teniendo en cuenta las leyes aplicables, reglamentos y la ética. La clasificación de la información a la que se va a acceder y los riesgos percibidos serán proporcionales a los requisitos de la empresa. | Si |
| A.6.2 | Términos y condiciones de empleo | Los acuerdos contractuales de empleo deben establecer las responsabilidades del personal y de la organización en materia de seguridad de la información. | Si |
| A.6.3 | Sensibilización, educación y formación en seguridad de la información | El personal de la organización y las partes interesadas relevantes deben recibir concientización, educación y capacitación adecuada sobre seguridad de la información y actualizaciones periódicas de la política de seguridad de la información de la organización, las políticas y los procedimientos específicos del tema, según sea relevante para su función laboral. | Si |
| A.6.4 | Proceso Disciplinario | Se debe formalizar y comunicar un proceso disciplinario para tomar acciones contra el personal y otras partes interesadas relevantes que hayan cometido una violación a la política de seguridad de la información. | Si |

| | | | |
|---|---|---|---|
| A.6.5 | Responsabilidades después del cese o cambio de empleo | Las responsabilidades y deberes de seguridad de la información que sigan siendo válidos después de la terminación o el cambio de empleo se definirán, se harán cumplir y se comunicarán al personal pertinente y a otras partes interesadas. | Si |
| A.6.6 | Acuerdos de confidencialidad o no divulgación | Los acuerdos de confidencialidad o no divulgación que reflejen las necesidades de la organización para la protección de la información deben ser identificados, documentados, revisados y firmados periódicamente por el personal y otras partes interesadas relevantes. | Si |
| A.6.7 | Trabajo remoto | Se deben implementar medidas de seguridad cuando el personal esté trabajando de forma remota, para proteger la información a la que se accede, procesa o almacena fuera de las instalaciones de la organización. | Si |
| A.6.8 | Informes de eventos de seguridad de la información | La organización debe proporcionar un mecanismo para que el personal informe los eventos de seguridad de la información observados o considerados sospechosos a través de los canales apropiados de manera oportuna. | Si |

*Ilustración 20: Controles de Personas. "Anexo A" - ISO 27001, enmienda N° 1 (2021)*

*4.1.3 Controles Físicos.*

| Nº | DETALLE | CONTROL | APLICABLE |
|---|---|---|---|
| A.7.1 | Seguridad física perimetral | Se definirán y utilizarán perímetros de seguridad para proteger las áreas que contienen información y otros activos asociados. | Si |
| A.7.2 | Entrada física | Las áreas seguras deben estar protegidas por controles de entrada y puntos de acceso adecuados. | Si |
| A.7.3 | Asegurar oficinas, salas e instalaciones | Se diseñará e implementará la seguridad física de las oficinas, salas e instalaciones. | Si |
| A.7.4 | Monitoreo de seguridad física | Las instalaciones deben ser monitoreadas continuamente para detectar accesos físicos no autorizados. | Si |
| A.7.5 | Protección contra amenazas físicas y ambientales | Se debe diseñar e implementar protección contra amenazas físicas y ambientales, como desastres naturales y otras amenazas físicas intencionales o no intencionales a la infraestructura. | Si |
| A.7.6 | Trabajo en áreas seguras | Se diseñarán e implementarán medidas de seguridad para trabajar en áreas seguras. | Si |
| A.7.7 | Escritorios limpios y pantallas despejadas | Deben definirse y aplicarse adecuadamente reglas de "escritorios limpios" para documentos, medios de almacenamiento extraíbles e instalaciones de procesamiento de información. | Si |
| A.7.8 | Ubicación y protección de equipos | El equipamiento debe estar ubicado de forma segura y protegida. | Si |

| | | | |
|---|---|---|---|
| A.7.9 | Seguridad de los activos fuera de las instalaciones | Se protegerán los activos fuera de los espacios físicos de la organización. | Si |
| A.7.10 | Medios de almacenamiento | Los medios de almacenamiento deben gestionarse a lo largo de su ciclo de vida de adquisición, uso, transporte y eliminación de acuerdo con el esquema de clasificación de la organización y los requisitos de manipulación. | Si |
| A.7.11 | Servicios de apoyo | Las instalaciones de procesamiento de información deben estar protegidas contra cortes de energía y otras interrupciones causadas por fallas en los servicios públicos de apoyo. | Si |
| A.7.12 | Seguridad del cableado | Los cables que transporten energía, datos o servicios de información de apoyo estarán protegidos contra intercepciones, interferencias o daños. | Si |
| A.7.13 | Mantenimiento de equipamiento | El equipamiento se mantendrá correctamente para garantizar la disponibilidad, integridad y confidencialidad de la información. | Si |
| A.7.14 | Eliminación o reutilización segura de equipos | Los elementos del equipamiento tecnológico que contengan medios de almacenamiento deben verificarse para garantizar que los datos confidenciales y el software con licencia se hayan eliminado o sobrescrito de forma segura antes de su eliminación o reutilización. | Si |

*Ilustración 21: Controles Físicos. "Anexo A" - ISO 27001, enmienda N° 1 (2021)*

*4.1.4 Controles Tecnológicos.*

| Nº | DETALLE | CONTROL | APLICABLE |
|---|---|---|---|
| A.8.1 | Dispositivos de usuarios finales | Se protegerá la información almacenada, procesada o accesible a través de dispositivos de usuario. | Si |
| A.8.2 | Derechos de acceso privilegiado | La asignación y el uso de derechos de acceso privilegiado se restringirán y gestionarán. | Si |
| A.8.3 | Restricción de acceso a la información | El acceso a la información y otros activos asociados se restringirá de acuerdo con la política específica sobre control de acceso. | Si |
| A.8.4 | Acceso al código fuente | El acceso de lectura y escritura al código fuente, las herramientas de desarrollo y las bibliotecas de software se gestionarán de forma adecuada. | No |
| A.8.5 | Autenticación segura | Se implementarán tecnologías y procedimientos de autenticación seguros en función de las restricciones de acceso a la información y la política específica del tema sobre control de acceso. | Si |
| A.8.6 | Capacidad de gestión | El uso de recursos se supervisará y ajustará de acuerdo con las necesidades actuales y previstas. | Si |
| A.8.7 | Protección contra malware | La protección contra el malware se implementará y apoyará mediante la concientización adecuada del usuario. | Si |

| | | | |
|---|---|---|---|
| A.8.8 | Gestión de vulnerabilidades técnicas | Se debe obtener información sobre las vulnerabilidades técnicas de los sistemas de información en uso.<br>Se debe evaluar la exposición de la organización a tales vulnerabilidades y tomar las medidas apropiadas. | Si |
| A.8.9 | Gestión de la configuración | Se deben establecer, documentar, implementar, monitorear y revisar las configuraciones, incluidas las de seguridad, de *hardware*, *software*, servicios y redes. | Si |
| A.8.10 | Eliminación de información | La información almacenada en sistemas de información, dispositivos o cualquier otro medio de almacenamiento se eliminará cuando ya no sea necesaria. | Si |
| A.8.11 | Enmascaramiento de datos | El enmascaramiento de datos se debe realizar de acuerdo con la política específica sobre control de acceso y otros requisitos del tema y del negocio relacionados, teniendo en cuenta la legislación aplicable. | Si |
| A.8.12 | Prevención ante la fuga de datos | Se aplicarán medidas de prevención de fuga de datos de los sistemas, redes y cualquier otro dispositivo que procese, almacene o transmita información sensible. | Si |
| A.8.13 | Respaldo de información | Las copias de seguridad de la información, el *software* y los sistemas deben mantenerse y probarse periódicamente de acuerdo con la política de copias de seguridad acordada. | SI |

| | | | |
|---|---|---|---|
| A.8.14 | Redundancia de instalaciones de procesamiento de información | Las instalaciones de procesamiento de información se implementarán con suficiente redundancia para cumplir con los requisitos de disponibilidad. | Si |
| A.8.15 | Inicio sesión | Los registros de actividades, excepciones, fallas y otros eventos relevantes deben ser generados, almacenados, protegidos y analizados. | Si |
| A.8.16 | Actividades de seguimiento | Las redes, los sistemas y las aplicaciones deben ser monitoreados para detectar comportamientos anómalos y tomar las acciones apropiadas para evaluar los posibles incidentes de seguridad de la información. | Si |
| A.8.17 | Sincronización de reloj | Los relojes de los sistemas de procesamiento de información utilizados por la organización deben estar sincronizados con las fuentes de tiempo aprobadas. | Si |
| A.8.18 | Uso de programas de utilidad privilegiados | El uso de programas de utilidad que pueden anular los controles del sistema y de las aplicaciones deben ser restringidos y controlados estrictamente. | Si |
| A.8.19 | Instalación de software en sistemas operativos | Se deben implementar procedimientos y medidas para gestionar de forma segura la instalación de software en los sistemas operativos. | Si |

| | | | |
|---|---|---|---|
| A.8.20 | Seguridad de las redes | Las redes y los dispositivos de red deben estar asegurados, administrados y controlados para proteger la información en los sistemas y las aplicaciones. | Si |
| A.8.21 | Seguridad de los servicios de red | Los mecanismos de seguridad, los niveles de disponibilidad y los requisitos de los servicios de red deben identificarse, implementarse y monitorearse. | Si |
| A.8.22 | Segregación de redes | Los grupos de servicios, usuarios y sistemas de información deben estar separados en las redes de la organización. | Si |
| A.8.23 | Filtrado web | El acceso a sitios web externos se gestionará para reducir la exposición a contenido malicioso. | Si |
| A.8.24 | Uso de criptografía | Se definirán e implementarán reglas para el uso efectivo de criptografía, incluyendo gestión de claves criptográficas. | Si |
| A.8.25 | Ciclo de vida de desarrollo seguro | Se establecerán y aplicarán reglas para el desarrollo seguro de *software* y sistemas. | No |
| A.8.26 | Requisitos de seguridad de la aplicación | Los requisitos de seguridad de las informaciones deben identificarse, especificarse y aprobarse al desarrollar o adquirir aplicaciones. | Si |
| A.8.27 | Principios de ingeniería y arquitectura de sistemas seguros | Los principios para la ingeniería de sistemas seguros deben establecerse, documentarse, mantenerse y aplicarse a cualquier actividad de desarrollo de sistemas de información. | No |

| | | | |
|---|---|---|---|
| A.8.28 | Codificación segura | Los principios de codificación segura se aplicarán al desarrollo de software. | No |
| A.8.29 | Pruebas de seguridad en desarrollo y aceptación | Los procesos de prueba de seguridad deben definirse e implementarse en el ciclo de vida del desarrollo. | No |
| A.8.30 | Desarrollo subcontratado | La organización debe dirigir, monitorear y revisar las actividades relacionadas con el desarrollo subcontratado de sistemas. | No |
| A.8.31 | Separación de entornos de desarrollo, prueba y producción | Los entornos de desarrollo, prueba y producción deben estar separados y protegidos. | No |
| A.8.32 | Gestión de cambios | Los cambios en las instalaciones de procesamiento y los sistemas de información estarán sujetos a los procedimientos de gestión de cambios. | Si |
| A.8.33 | Información de pruebas | La información de las pruebas se seleccionará, protegerá y gestionará de forma adecuada. | No |
| A.8.34 | Protección de los sistemas de información durante las pruebas de auditoría | Las pruebas de auditoría y otras actividades de garantía que impliquen la evaluación de los sistemas operativos deben planificarse y acordarse entre el auditor y la dirección correspondiente. | Si |

*Ilustración 22: Controles Tecnológicos. "Anexo A" - ISO 27001, enmienda N° 1 (2021)*

# 5 Conclusiones

En el presente trabajo se desarrolló un marco teórico sobre los principales postulados que plantea la gestión de la seguridad de la Información, con el objetivo de entender las implicancias que conlleva la implementación, seguimiento y control de un SGSI. Esto permitió evidenciar la relevancia de la seguridad informática en las organizaciones actuales y determinar la relación de esta disciplina con la ciencia de la administración.

Posteriormente, se efectuó una observación del estado actual del Sistema de Gestión, certificado por IRAM – ISO 9001 en calidad, de una empresa dedicada a la comercialización de productos químicos para la industria, ubicada en la provincia de Tucumán, Argentina. A partir de esta primera evaluación, se realizó un estudio de tipo explicativo y descriptivo, analizando los requerimientos que adicionalmente debería cumplir la organización para certificar su sistema de gestión, teniendo en cuenta exigencias de seguridad de la información.

Se realizó un relevamiento de los requisitos que actualmente se cumplen, debido a que el SGC cuenta con una estructura común de alto nivel compatible con un SGSI. Luego se identificaron las acciones y controles de seguridad que deberían implementarse, para dar cumplimiento a lo indicado en ISO 27001. En este sentido, se observa que un número considerable de requerimientos actualmente están siendo cumplimentados y otros podrían ser llevadas a cabo sin realizar demasiado esfuerzo de recursos, reutilizando herramientas implementadas como, por ejemplo: análisis de contexto, capacitaciones, auditorías, entre otros. Si existiesen variaciones en un mismo procedimiento a fin de dar cumplimiento a ambos *framework*, deberá indicarse la situación en el documento destinado a tal fin.

Por lo anteriormente expresado, se pudo corroborar que existen puntos en común entre los dos estándares analizados, por lo que se presenta una oportunidad de integración. Sin embargo, se evidencian diferencias que deben tenerse en cuenta, especificándose las cláusulas que se están cumpliendo de cada estándar.

Se hace hincapié en la importancia de la evaluación y gestión del riesgo para una adecuada dirección estratégica del negocio, lo que contribuiría a

evitar incidentes que comprometan la confidencialidad, integridad y/o disponibilidad de la información y otorgaría confianza a los *stakeholders*, demostrando que los peligros identificados se gestionan apropiadamente.

También, se recomienda la aplicación de los controles organizacionales, de personas, físicos y tecnológicos que propone el “Anexo A” de la norma ISO 27001 y se planifiquen auditorías internas periódicas que monitoreen su adecuado cumplimiento y el de los pertinentes controles por oposición que deberían estar previstos en el diseño de los procedimientos de trabajo.

Se considera que la puesta en marcha de un sistema de gestión integrado que cumpla con requisitos de calidad y seguridad de la información, es una propuesta factible de aplicar en la entidad analizada, agregando valor y contribuyendo a la mejora continua de sus procesos de negocio. Para ello, se requerirá la asignación de mayores recursos económicos y humanos para su sostenimiento en el tiempo.

Asimismo, es aconsejable que se designe un responsable idóneo para liderar el sistema de gestión integrado; se incorporen a este todas las operaciones de la empresa y se fomenten actividades para lograr el compromiso de sus miembros y de la dirección de la compañía.

Finalmente se hace énfasis en que aquellas personas que tienen a su cargo la gestión del ente deben considerar a la seguridad de la información en el diseño de los procesos de negocios, sistemas de información y controles.

# 6 Referencias Bibliográficas

- **Bibliografía Específica**


Arrarte, R. (20 de junio de 2019). *La tecnología y el buen gobierno corporativo*. Obtenido de Diligent.com: https://www.diligent.com/es/importancia-tecnologia-buen-gobierno-corporativo/

Baca Urbina, G. (2016). *Introducción a la Seguridad Informática.* México: Grupo Editorial Patria.

Bravo, R. (Año 22, N° 252). *Doble Virus. Update trending*. Info Tecnology, 20.

Cano M., J. J. (2013). *Inseguridad de la Información: Una visión estratégica*. Bogotá: Alfaomega.

Coraminas, J. (1961). *Breve diccionario epistomológico de la lengua castellana.* Madrid, España: Gredos.

Deloitte. (s.f.). *¿Qué es el gobierno corporativo? Transparencia y confianza*. Obtenido de Deloitte: https://www2.deloitte.com/es/es/pages/governance-risk-and-compliance/articles/que-es-el-gobierno-corporativo.html

Dirección Nacional de Ciberseguridad. Jefatura de Gabinete de Ministros. (14 de febrero de 2022). Modelo Referencial de Política de Seguridad de la Información. *Disposición 01/2022*. Ciudad de Buenos Aires.

Escuela Europea de Excelencia. (11 de octubre de 2016). *¿Cómo integrar las normas ISO 9001 e ISO 27001?* Obtenido de Nuevas Normas ISO: https://www.nueva-iso-9001-2015.com/2016/10/integrar-normas-iso-9001-e-iso-27001/

FACPCE. (2002). *RT 16: Marco conceptual de las normas contables profesionales.* Capital Federal, Argentina: CECYT. Obtenido de http://www.cgcetucuman.org.ar/wp-content/uploads/RT_16.pdf

Gestion.org. (s.f.). *¿Qué es la Administración? Descubre sus orígenes y cómo se aplica en las empresas del siglo XXI*. Obtenido de gestion.org: https://www.gestion.org/que-es-la-administracion/

INCIBE. (18 de mayo de 2021). *Glosario de términos de Ciberseguridad: una guía de aproximación para el empresario.* Obtenido de Protege tu empresa: https://www.incibe.es/protege-tu-empresa/guias/glosario-terminos-ciberseguridad-guia-aproximacion-el-empresario

IRAM. (s.f.). *Diplomado en sistemas de gestión integrados*. Obtenido de IRAM Formación: https://iram.org.ar/curso/1901-diplomado-en-sistemas-de-gestion-integrados/

ISO / IEC. (2018). *Tecnología de la información - Gestión de servicios - Parte 7: Orientación sobre la integración y correlación de ISO / IEC 20000-1: 2018 a ISO 9001:2015 e ISO / IEC 27001: 2013.* Suiza: ISO.

ISO/IEC. (2021). *Tecnología de la Información. Técnicas de seguridad. Sistemas de gestión de la seguridad de la información. Requisitos. Enmienda 1 .* JTC 1/SC 27/WG 1 N° 3025.

ISO/IEC 27000. (2014). *Tecnología de la información. Técnicas de seguridad. Sistemas de gestión de seguridad de la información. Descripción general y vocabulario.* Vernier, Geneva, Switzerland: ISO.

ISO/IEC 27001. (2013). *Tecnología de la Información. Técnicas de seguridad. Sistemas de gestión de la seguridad de la información. Requisitos.* Capital Federal, Argentina: Subcomité de Seguridad de la Información, Ciberseguridad y Protección de la Privacidad (IRAM).

ISO/IEC 27005. (2012). *Tecnología de la información. Gestión del riesgo de seguridad de la Información.* Subcomité de Seguridad de la Información.

Itgovernance. (s.f.). *ISO 38500*. Obtenido de Itgovernance.eu: https://www.itgovernance.eu/es-es/iso-38500-es#:~:text=ISO%2FIEC%2038500%20es%20el,comunicaci%C3%B3n%20IT%20de%20una%20organizaci%C3%B3n.

IT-Insecurity. (23 de agosto de 2009). *Cultura de Seguridad de la Información: Entendiendo una percepción*. Obtenido de IT-Insecurity: https://insecurityit.blogspot.com/2009/08/cultura-de-seguridad-de-la-informacion.html

Lardent, A. R. (2001). *Sistemas de Información para la gestión empresaria: procedimientos, seguridad y auditoría.* Buenos Aires, Argentina: Pearson.

Laudon, K. C. (2016). *Sistemas de Información Gerencial, 14º edición.* México: Pearson.

NormaISO27001.es. (s.f.). *Norma ISO 27001*. Obtenido de NormaISO27001: https://normaiso27001.es/mejora-en-iso-27001/

Real Academia Española. (s.f.). *Auditoría*. Obtenido de Real Academia Española: https://dle.rae.es/auditor%C3%ADa

Real Academia Española. (s.f.). *Riesgo*. Obtenido de Real Academia Española: https://dle.rae.es/riesgo

Significados.com. (s.f.). *Significado de Vulnerable*. Obtenido de Significados.com.

Significados.com. (s.f.). *Significado de Vulnerable*. Obtenido de Significados.com: https://www.significados.com/vulnerable/

Wikipedia. (07 de octubre de 2021). *Ciclo de Deming*. Obtenido de Wikipedia: https://es.wikipedia.org/wiki/Ciclo_de_Deming

- **Bibliografía General**


Áudea (15 de febrero de 2016*). Diferencias entre Ciberseguridad y Seguridad de la Información*. Obtenido de audea.com: https://www.audea.com/diferencias-ciberseguridad-seguridad-la-informacion/

Cobos M. (2020). *8 problemas de integrar Normas ISO*. ISOTools Excellence. España. Obtenido de ISOTools.org: https://info.isotools.org/integrar-sistemas-gestion

Collazo J., Saroka R. (2010). *Informática en las organizaciones: todo lo que el profesional en ciencias económicas debe conocer para la aplicación eficiente de los recursos informáticos en la organización*. EDICON (Fondo Editorial Consejo). Buenos Aires

García M. A. (2021). *Conocimientos en Seguridad de la Información requeridos por profesionales en Ciencias Económicas para la Gestión Estratégica de Negocios*. Facultad de Ciencias Económicas (UNT), Tucumán

INCIBE (20 de marzo de 2017). *Amenaza vs Vulnerabilidad, ¿sabes en qué se diferencian?* Obtenido del Instituto Nacional de Ciberseguridad: https://www.incibe.es/protege-tu-empresa/blog/amenaza-vs-vulnerabilidad-sabes-se-diferencian

INCIBE (30 de noviembre de 2016). *CEO, CISO, CIO… ¿Roles en ciberseguridad?* Obtenido del Instituto Nacional de Ciberseguridad: https://www.incibe.es/protege-tu-empresa/blog/ceo-ciso-cio-roles-ciberseguridad

INCIBE (s.f). *Políticas de seguridad para la pyme.* Obtenido del Instituto Nacional de Ciberseguridad: https://www.incibe.es/protege-tu-empresa/herramientas/politicas

INTECO (s.f.). *Implementación de un SGSI en la empresa*. Obtenido de INCIBE: https://www.incibe.es/extfrontinteco/img/File/intecocert/sgsi/img/Guia_apoyo_SGSI.pdf

IRAM, Instituto Argentino de Normalización y Certificación (2015). *Norma ISO 9001: Sistemas de Gestión de Calidad.* Subcomité de Sistemas de Gestión de Calidad.

IRAM, Instituto Argentino de Normalización y Certificación (2021). *Norma ISO 27002: Tecnología de la información. Técnicas de seguridad. Código de buenas prácticas para los controles de la seguridad de la información.*

IRAM, Instituto Argentino de Normalización y Certificación (2019). *La norma IRAM-ISO/IEC 27001. Requisitos para los Sistemas de Gestión de Seguridad de la Información*. Material de estudio de curso a distancia. Obtenido de IRAM.org: https://iram.org.ar/curso/2037-la-norma-iram-iso-iec-27001-requisitos-para-los-sistemas-de-gestion-de-seguridad-de-la-informacion/

ISBL (31 de enero de 2021). *¿Qué es un sistema de gestión y para qué sirve?* Obtenido de Instituto de Seguridad y Bienestar Laboral: https://isbl.eu/2021/01/que-es-un-sistema-de-gestion-y-para-que-sirve/

ISO / IEC (2021*). Directivas ISO/IEC, Parte 1. Procedimientos para el trabajo técnico. Suplemento ISO consolidado - Procedimientos específicos de ISO*. Comisión Electrotécnica Internacional de ISO, Suiza. Obtenido de iso.org: https://www.iso.org/sites/directives/current/consolidated/index.xhtml

ISO27000.es (s.f.). *Términos relacionados con la serie ISO 27000 y la seguridad de la información*. Obtenido de ISO27000.es: https://www.iso27000.es/glosario.html

ISOTools Excellence (23 de mayo de 2017). *Sistemas Integrados de Gestión ISO 9001, ISO 14001 y OHSAS 18001: Costes y beneficios*. Obtenido de ISOTools.org: https://www.isotools.cl/sistemas-integrados-gestion-iso-9001-iso-14001-ohsas-18001-costes-beneficios/

ISOTools Excellence (28 de febrero de 2019). *Sistemas Integrados de Gestión, ¿Cuáles son sus beneficios?* Obtenido de ISOTools.org: https://www.isotools.org/2019/02/28/sistemas-integrados-gestion-beneficios/

ISOTools Excellence (28 de junio de 2015) *¿Qué es SGSI?* Obtenido de Seguridad de la Información, blog especializado en Seguridad de la Información y Ciberseguridad: https://www.pmg-ssi.com/2015/07/que-es-sgsi/

Mendoza M. A. (9 de enero de 2019) *¿Cómo definir el alcance del SGSI?* Obtenido de Welivesecurity: https://www.welivesecurity.com/la-es/2018/01/09/definir-alcance-sgsi/

Palomino W. (11 de noviembre de 2019). *Alcances sobre la norma internacional ISO 37001*. Obtenido de Estudio Oré Guardia: https://oreguardia.com.pe/alcances-sobre-la-norma-internacional-iso-37001/

Saroka R. H. (2002). *Sistemas de información en la era digital*. Fundación OSDE. Argentina.

Scolnik, H. D. (2014) *¿Qué es la Seguridad Informática?* 1° edición. Editorial Paidós. Argentina.

Wikipedia (s.f.) *Administración*. Obtenido de Wikipedia: https://es.wikipedia.org/wiki/Administraci%C3%B3n