Universidad Nacional de Tucumán
Facultad de Ciencias Económicas
Instituto de Administración
XIV Muestra Académica de Trabajos de Investigación de la Licenciatura en Administración

"Hacia un Sistema de Gestión de Seguridad de la Información (SGSI) en un grupo económico exportador de la provincia de Tucumán: GAP Analysis ISO 27001"

Autor: Inés Aceñolaza Chamorro
DNI: 43691424
Mail: Ineace12@gmail.com
Tutor: Marcelo Adrián García

Índice

Contenido

Resumen

El proyecto tiene como objetivo realizar un diagnóstico organizacional con un enfoque en el análisis de brecha (gap analysis) para evaluar la preparación de la empresa Tucumana y la factibilidad de implementación de un SGSI basado en la norma ISO 27001 en sus procesos administrativos.

El grupo utiliza gran cantidad de activos de información para su operación normal y carece de un panorama claro de las deficiencias y las áreas de riesgo en términos de seguridad de la información dentro de la organización. La ausencia de un análisis organizacional previo dificulta la toma de decisiones informadas sobre los recursos, los cambios operativos y las inversiones necesarias para establecer un SGSI eficaz. Esto podría resultar en la imposibilidad de abordar adecuadamente las vulnerabilidades de seguridad y las necesidades específicas de la empresa.

La investigación se enmarca en un enfoque cualitativo de tipo explicativo y descriptivo. Se busca profundizar en la comprensión de la implementación y evaluación de un SGSI, así como en la identificación de mejores prácticas en el proceso de auditorías internas en este contexto. El enfoque exploratorio permitirá la obtención de información detallada y rica en experiencias y perspectivas de los participantes.

Los datos cualitativos recopilados de las entrevistas y documentos serán sometidos a un análisis de contenido haciendo un análisis GAP para ver las brechas que se tiene entre lo que tiene la organización y lo que señala las normas ISO 27001.

Se ha demostrado que es factible la implementación de un SGSI en el grupo. El grupo cuenta con los recursos y el compromiso necesarios para cumplir con los requisitos de la norma ISO 27001. Sin embargo, se identificaron algunas áreas a mejorar.

Palabras Clave: Diagnóstico Organizacional – ISO 27001 – Sistema de Gestión de Seguridad de la Información

Introducción

En la era digital y altamente interconectada en la que vivimos, la seguridad de la información se ha convertido en un pilar fundamental para la supervivencia y éxito de las organizaciones en todo el mundo. La creciente amenaza de ciberataques, la fuga de datos confidenciales y las interrupciones en los servicios han subrayado la necesidad imperante de salvaguardar la integridad, la confidencialidad y la disponibilidad de la información. En este contexto, la norma internacional ISO/IEC 27001 emerge como un faro de guía, proporcionando un enfoque estructurado y sistemático para establecer, implementar, operar, supervisar, revisar, mantener y mejorar un Sistema de Gestión de Seguridad de la Información (SGSI).

La norma ISO/IEC 27001 no solo sirve como un marco para garantizar la seguridad de la información, sino que también insta a las organizaciones a adoptar un enfoque de mejora continua. Una parte integral de este enfoque es la realización de auditorías internas periódicas que evalúen la eficacia y el cumplimiento del SGSI implementado. Estas auditorías no solo identifican posibles brechas en la seguridad, sino que también permiten la identificación de oportunidades para la optimización de procesos y la mitigación proactiva de riesgos.

El propósito de este trabajo es explorar en profundidad el contexto en el que se encuentra la empresa estudiada para ver la posibilidad de implementación en de un SGSI basado en la norma ISO/IEC 27001:2022.

Situación Problemática

El grupo opera en los sectores Industrial y Agrícola, utilizando gran cantidad de activos de información para su operación normal. Aunque reconoce la importancia de proteger la seguridad de la información en sus procesos administrativos, aún no ha realizado un análisis exhaustivo de su situación actual. Carece de un panorama claro de las deficiencias y las áreas de riesgo en términos de seguridad de la información dentro de la organización. Esta falta de visión integral plantea la pregunta fundamental de si la empresa está verdaderamente preparada para la implementación de un Sistema de Gestión de Seguridad de la Información (SGSI) basado en la

norma ISO 27001.

La ausencia de un análisis organizacional previo dificulta la toma de decisiones informadas sobre los recursos, los cambios operativos y las inversiones necesarias para establecer un SGSI eficaz. Esto podría resultar en una implementación costosa y problemática, que podría no abordar adecuadamente las vulnerabilidades de seguridad y las necesidades específicas de la empresa.

Preguntas de Investigación

Se plantean las siguientes preguntas de Investigación:

¿Cuáles son los estándares y regulaciones pertinentes que deben ser considerados al identificar el marco de cumplimiento específico necesario para la implementación del Sistema de Gestión de Seguridad de la Información (SGSI) en la empresa?

¿Cómo se puede definir de manera precisa y exhaustiva el alcance del análisis de brecha para determinar qué procesos administrativos, áreas de la empresa y activos de información crítica deben ser incluidos en la evaluación, con el objetivo de garantizar una implementación efectiva del SGSI?

¿Qué debe incluir el diseño de un informe que contemple acciones y proyectos concretos para la implementación exitosa del Sistema de Gestión de Seguridad de la Información (SGSI) en la empresa?

Objetivo General

El objetivo general de este trabajo es realizar un diagnóstico organizacional con un enfoque en el análisis de brecha (gap analysis) para evaluar la preparación de la empresa Tucumana que opera en los sectores Industrial y Agrícola y la factibilidad de implementación de un Sistema de Gestión de Seguridad de la Información (SGSI) basado en la norma ISO 27001 en sus procesos administrativos.

Este diagnóstico permitirá identificar las deficiencias y áreas críticas de mejora, así como determinar los recursos necesarios para lograr una implementación exitosa del SGSI que

garantice la seguridad de la información en la organización.

Objetivos Específicos

Identificar el marco de cumplimiento específico requerido para la implementación del Sistema de Gestión de Seguridad de la Información (SGSI) en la empresa, en base a los estándares y regulaciones pertinentes, como la norma ISO 27001.

Definir claramente el alcance del análisis de brecha, identificando los procesos administrativos y las áreas de la empresa que serán objeto de evaluación, así como los activos de información crítica que deben ser protegidos.

Esta delimitación permitirá un enfoque preciso en la identificación de las diferencias entre la situación actual de seguridad de la información y los requisitos del Sistema de Gestión de Seguridad de la Información (SGSI) basado en la norma ISO 27001.

3. Diseñar un plan informe que incluya acciones y proyectos específicos para la implementación efectiva del Sistema de Gestión de Seguridad de la Información (SGSI) en la empresa.

Marco Metodológico

Esta investigación se enmarca en un enfoque cualitativo de tipo explicativo y descriptivo. Se busca profundizar en la comprensión de la implementación y evaluación de un SGSI, así como en la identificación de mejores prácticas en el proceso de auditorías internas en este contexto. El enfoque exploratorio permitirá la obtención de información detallada y rica en experiencias y perspectivas de los participantes.

Para la recopilación de datos, se utilizarán principalmente dos métodos: entrevistas semiestructuradas y análisis documental. Las entrevistas permitirán obtener información detallada de profesionales involucrados en el proceso administrativo de la empresa. Además, se analizarán documentos como políticas, procedimientos y reportes de auditorías internas. Los datos cualitativos recopilados de las entrevistas y documentos serán sometidos a un análisis de contenido haciendo un análisis GAP para ver las brechas que se tiene entre lo que tiene la

organización y lo que señala las normas ISO 27001.

Marco Teórico

Para poner en contexto, se define el siguiente marco teórico.

Diagnostico organizacional

Según Elizabeth Vidal Arizabaleta (2004), autora del libro "Diagnóstico Organizacional," en términos sencillos, el diagnóstico se concibe como un proceso de comparación entre dos situaciones: la primera es la situación presente, que se ha llegado a conocer mediante un proceso de indagación exhaustiva; la segunda es una situación previamente definida y supuestamente conocida, que actúa como pauta o modelo de referencia. La brecha resultante de esta comparación o contraste es precisamente lo que se denomina diagnóstico.

Es importante destacar que el proceso diagnóstico no representa un fin en sí mismo, sino más bien un medio para potenciar los recursos y la capacidad estratégica de una organización. Este proceso se erige como un valioso insumo para la planificación estratégica de la entidad. En este contexto, el diagnóstico se integra como un componente esencial de la Dirección y la Planeación Estratégica, ya que desempeña un papel fundamental en la toma de decisiones que persiguen fines de productividad, competitividad, supervivencia y crecimiento en cualquier tipo de organización.

Esta comprensión del diagnóstico organizacional, basada en la obra de Vidal Arizabaleta, sienta las bases conceptuales esenciales para abordar la implementación de un Sistema de Gestión de Seguridad de la Información (SGSI) conforme a las normas ISO 27001 en los procesos administrativos de empresas que operan en los sectores Industrial y Agrícola. El análisis de brechas (Gap) entre la situación actual y los estándares ISO 27001 se convierte en una parte integral de este proceso de diagnóstico y mejora continua en busca de la excelencia operativa y estratégica

Activos de Información

Los "Activos de la Información" se definen como cualquier información o sistema

relacionado con su tratamiento que tenga valor para una organización, tales como procesos de negocio, datos, aplicaciones, equipos informáticos, personal, soportes de información, redes, equipamiento auxiliar o instalaciones. Estos activos son susceptibles de ser atacados deliberada o accidentalmente, lo que podría dar lugar a consecuencias económicas, legales o reputacionales para la organización (Instituto Nacional de Ciberseguridad [INCIBE], 2021).

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 definición es un concepto general que se puede desarrollar de forma mas amplia, Tipton y Krause (2009) definen la seguridad de la información como un conjunto de políticas, procedimientos y prácticas diseñadas para proteger la confidencialidad, integridad y disponibilidad de los activos de información de una organización. Esto implica la gestión de riesgos, la implementación de controles de seguridad y la respuesta a incidentes para mitigar las amenazas y los riesgos que puedan afectar a la información crítica de una organización.

Sistema de Gestión

En el glosario de términos de la norma ISO/IEC 27000:2018, cláusua 2.46, se define como Sistema de Gestión a un conjunto de elementos interrelacionados de una organización para establecer políticas y objetivos, y procesos para alcanzar dichos objetivos.

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. 70).

Norma ISO/IEC 27001

La norma ISO/IEC 27001, oficialmente titulada "Tecnología de la Información - Técnicas de seguridad - Sistemas de gestión de seguridad de la información - Requisitos," es una norma internacional que establece los requisitos y las directrices para la implementación de un Sistema de Gestión de Seguridad de la Información (SGSI) en una organización. Fue desarrollada conjuntamente por la Organización Internacional de Normalización (ISO) y la Comisión Electrotécnica Internacional (IEC).

En términos generales, la norma ISO/IEC 27001 tiene como objetivo ayudar a las organizaciones a proteger la confidencialidad, integridad y disponibilidad de la información que manejan. Para lograrlo, establece un marco de mejores prácticas que abarcan desde la identificación de riesgos y amenazas hasta la implementación de controles de seguridad y la gestión de incidentes.

Tabla 1: Estructura requisitos ISO 27001 y controles Anexo A

ESTRUCTURA
4 - Contexto de la Organización
5 - Liderazgo
6 - Planificación
7 - Apoyo
8 - Operación
9 - Evaluación de desempeño
10 - Mejora
ANEXO A
5- Controles Organizacionales
6 - Control de Personas
7 - Controles Físicos
8 - Controles Tecnológicos

Fuente: Elaboracion Propia

La norma se compone de una serie de secciones, incluyendo:

1. Alcance y objetivos: Define el alcance del SGSI y sus objetivos.
2. Referencias normativas: Enumera las normas y documentos de referencia relevantes.

3. Términos y definiciones: Proporciona una lista de términos y definiciones clave utilizados en la norma.
4. Contexto de la organización: Exige que la organización comprenda su contexto interno y externo, así como las necesidades y expectativas de las partes interesadas.
5. Liderazgo y compromiso: Establece los roles y responsabilidades de la alta dirección en relación con el SGSI.
6. Planificación: Aborda la identificación de riesgos, evaluación de riesgos y establecimiento de objetivos de seguridad de la información.
7. Apoyo: Se refiere a los recursos, competencia, toma de conciencia y comunicación necesarios para el SGSI.
8. Operación: Describe la implementación y operación de controles de seguridad.
9. Evaluación del desempeño: Establece la necesidad de monitorear, medir, analizar y evaluar el SGSI.
10. Mejora: Aborda la necesidad de tomar acciones para mejorar continuamente el SGSI.

ISO/IEC 27001 es una norma reconocida internacionalmente y se utiliza ampliamente como un marco de referencia para la gestión de la seguridad de la información en organizaciones de todos los tamaños y sectores. La certificación en ISO/IEC 27001 es una forma de demostrar el compromiso de una organización con la seguridad de la información a sus clientes, socios y partes interesadas.

Ciclo metodológico para la implantación de la norma ISO 27001

Para Gómez Vietes, A. (2014) en su libro de Auditoría de Seguridad Informática, el éxito en la implantación de un SGSI desde cualquier perspectiva empresarial depende del compromiso y la mentalidad de cambio de los niveles ejecutivos y directivos en las organizaciones, por tanto, el alcance del sistema requiere de un nivel Implantación de un sistema de gestión de seguridad

de información bajo la ISO 27001: Análisis del riesgo de la información de concientización de las esferas estratégicas y tácticas de la estructura empresarial. En consecuencia, es necesario que la decisión en la implantación del modelo involucre a todas las instancias de la empresa desde una óptica democrática y participativa; más aún se hace apremiante que el líder del proceso haga parte de la alta gerencia, lo que garantiza el nivel de responsabilidad y evita la obstrucción del proceso.

Aplicación

En el contexto de la empresa objeto de estudio, se llevó a cabo exhaustiva recolección de datos y análisis de información, con el propósito de entender a profundidad la situación actual y áreas donde puede haber mejora. Esta información abarca una amplia gama de aspectos, centrándose en los procesos administrativos pero con una mirada puesta en el área de TI, para explorar los procesos de seguridad de la información y el cumplimiento basado en la norma ISO/IEC 27001.

El proyecto se divide en dos partes fundamentales, cada una de ellas con un propósito específico. En primer lugar, se llevará a cabo una minuciosa identificación del marco normativo aplicable, centrado en la norma ISO 27001. Esta fase no solo busca comprender en detalle los requisitos de la norma, sino también adaptarlos al contexto particular de la empresa y definir su alcance en los procesos administrativos. Esto sentará las bases para la segunda parte del proyecto.

La segunda parte del proyecto consiste en el análisis Gap ISO 27001, donde se evaluará exhaustivamente la diferencia entre las prácticas y medidas de seguridad de la información existentes en la empresa y los requisitos establecidos por la norma ISO 27001. Este análisis permitirá identificar las brechas críticas que deben abordarse para cumplir con los estándares de seguridad de la información. Como resultado, se desarrollarán planes de mejora propuestos, que serán entregables clave para la empresa.

Para el análisis Gap ISO 27001, se utilizó una metodología de trabajo se estructuró en diversas fases para llevar a cabo la evaluación exhaustiva de la Seguridad de la Información:

- **Fase I: Revisión de las funciones organizativas:** En esta etapa, se examinó el organigrama y las funciones de los puestos que se relacionan con la Seguridad de la Información.

- **Fase II: Revisión de política y marco normativo:** Se procedió a examinar la presencia de una política de seguridad de la información y el conjunto de normativas que rigen en la organización.

- **Fase III: Revisión de la existencia de planes de concientización:** Se examinó la existencia de planes de concientización enfocados en la seguridad y la protección de los datos personales.

- **Fase IV: Revisión de seguimiento y control:** Se revisaron las prácticas de seguimiento y control adoptadas para supervisar el desempeño organizacional. Se enfocó en la mejora continua de las iniciativas de seguridad en la organización.

- **Fase V: análisis de Gap de Seguridad:** Se ejecutó un análisis detallado para identificar las discrepancias entre las medidas de seguridad de la organización y los requisitos de seguridad definidos. Utilización de herramienta de diagnóstico en Excel.

- **Fase VI: plan de acción:** Se diseñaron planes de acción que establecerán estrategias de mejora en seguridad, abordando objetivos a corto, mediano y largo plazo.

Para el análisis de los datos, se emplea una metodología Capability Maturity Model Integration (CMMi®), que se ha convertido en una herramienta fundamental para evaluar de manera cuantitativa la implementación y despliegue de los requisitos establecidos por la Norma ISO/IEC 27001. Este enfoque proporciona un marco estructurado para medir la madurez de los procesos dentro de la organización en relación con la gestión de la seguridad de la información.

Tabla 2: Modelo de Madurez de Procesos CMMI

Madurez	Grado	Valor	Descripción	Clave	Aspectos
N/A - No Aplica	N/A	NA	No aplica al ámbito de estudio / Organización	N/A	Implantación
0 - Inexistente	0	0%	No se realiza ningún aspecto de la actividad.	Sin Acciones	
1 - Inicial	1	5%	Estado donde el éxito de las actividades se basa, la mayoría de las veces, en el esfuerzo personal. Los procesos son desorganizados, totalmente reactivos y los roles y responsabilidades están mal o poco definidos.	Esfuerzo Personal	
2 - Gestionado	2	15%	Se normalizan las buenas prácticas en base a la experiencia y el método. Están definidos los productos a realizar, y los hitos para su revisión. Las definiciones no aplican a nivel corporativo, ni existe normalización.	Buenas Prácticas	
3 - Definido	3	60%	La Organización entera participa en el proceso. Existen métodos y templates bien definidos y documentados. Existen normativas y procedimientos aprobados que regulan la actividad. Los correspondientes actores han sido formados.	Procedimientos	Formalización
4 - Cuantitativo	4	85%	Se puede seguir con indicadores numéricos y estadísticos la evolución de los procesos.	Indicadores	
5 - Optimizado	5	100%	En base a criterios cuantitativos, se pueden determinar las desviaciones más comunes y optimizar los procesos. En lo sucesivo, se reducirán costos gracias a la reducción de problemas y a la continua revisión de los procesos.	Mejora Continua	

Fuente: Elaboración propia en Excel

Empresa Objeto Estudio

La empresa en cuestión es un conglomerado que engloba diversas empresas con un enfoque en las actividades industriales y agrícolas. Su sede principal se encuentra en Yerba Buena, Tucumán, Argentina. Este grupo empresarial se destaca por su diversidad de operaciones en dos sectores distintos pero complementarios: la producción de materiales de construcción y la agricultura.

En el ámbito de la actividad industrial, la empresa se dedica a la fabricación de productos clave como ladrillos huecos, cerramientos y aberturas especiales. Estos productos son esenciales en la construcción y son utilizados en una variedad de proyectos, desde viviendas residenciales hasta estructuras industriales y comerciales. La calidad y la versatilidad de estos materiales contribuyen al éxito en la industria de la construcción.

Por otro lado, en el campo de la actividad agrícola, el grupo se involucra en la producción, el empaque y la comercialización de productos agrícolas, específicamente arándanos y limones. Estos cultivos son altamente demandados en los mercados nacionales e internacionales debido a su calidad y sabor. La empresa se esfuerza por mantener altos estándares de calidad en la producción y el empaque de estas frutas para satisfacer las

necesidades de sus clientes.

El compromiso con la calidad y la atención al detalle es un pilar fundamental en todas las operaciones de este grupo empresarial. Su capacidad para diversificar sus actividades en dos sectores estratégicos, la construcción y la agricultura, refleja una visión empresarial sólida y una adaptación inteligente a las oportunidades del mercado.

Por último, la empresa reconoce la relevancia de la información como un activo crítico, y este proceso de recolección y análisis nos proporciona una base sólida para avanzar hacia una gestión más eficiente y segura de nuestros recursos y operaciones. En las secciones siguientes, se explorará en detalle los resultados de la investigación y las acciones que se plantean.

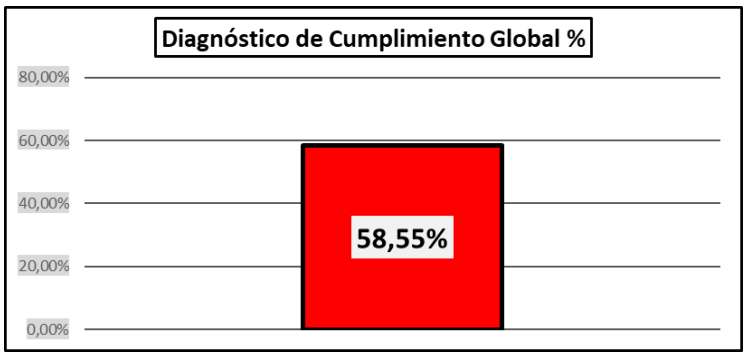
Resultados

En este apartado se exponen los valores de las métricas relevadas teniendo en cuenta las entrevistas realizadas, la documentación aportada, cuestionarios de entrevistas, así como los conocimientos y el criterio profesional.

El número de métricas o controles evaluados de acuerdo a lo definido por la norma ISO/IEC 27001:2022 es de cuarenta y nueve (49). Sobre dichas métricas se han identificado hallazgos y observaciones destinadas a la mejora continua de la organización con respecto a la seguridad de la información.

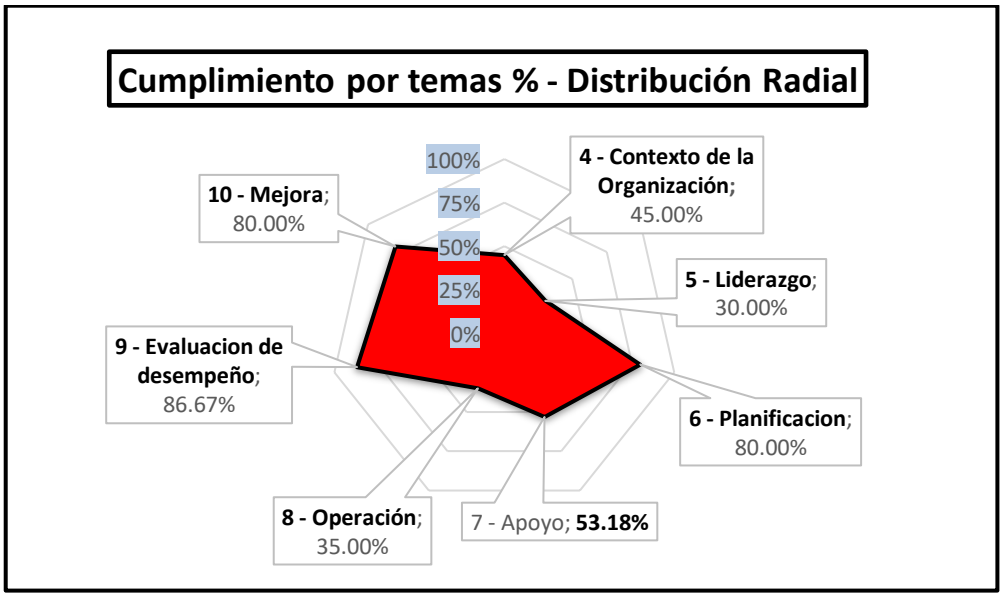
Se obtuvo un cumplimiento general de 58.55%. Si bien este valor es bastante razonable, se considera que existen aspectos a mejorar para la implementación exitosa del SGSI por lo que se procederá a diseñar un plan de acción más adelante.

Tabla 3: Diagnóstico de Cumplimiento Global



Fuente: Elaboración propia

Tabla 4: Cumplimiento por temas – Distribución radial



Fuente: Elaboración Propia

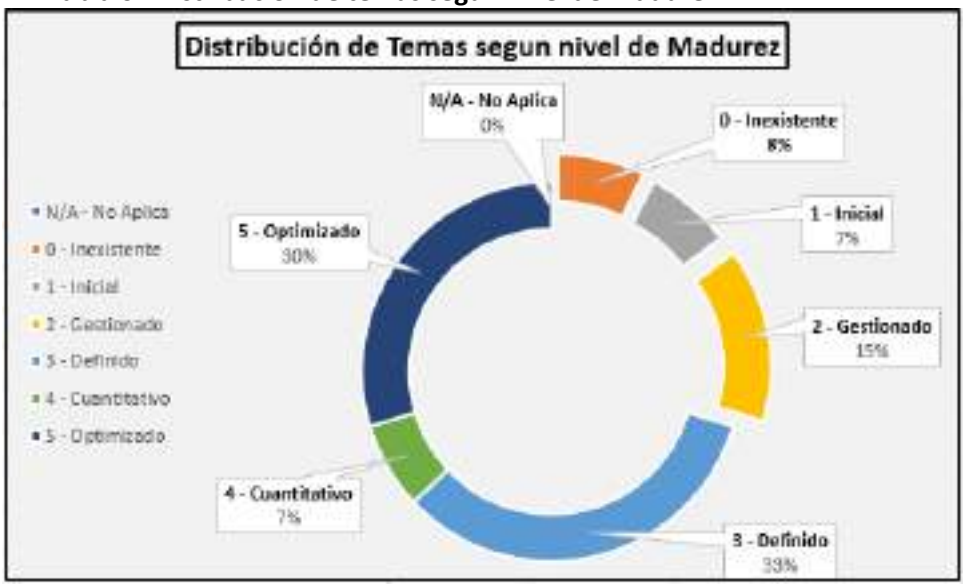
Se muestra el detalle de las métricas obtenidas, en donde se puede observar que los principales aspectos a mejorar son en cuanto al requisito 8 de Operación y 5 de Liderazgo.

Tabla5: Nivel de Madurez respecto a los Capítulos

Capítulo	Nivel de Madurez						
	N/A - No Aplica	0 - Inexistente	1 - Inicial	2 - Gestionado	3 - Definido	4 - Cuantitativo	5 - Optimizado
4 - Contexto de la Organización	0	0	0	1	2	0	0
5 - Liderazgo	0	0	0	1	2	0	0
6 - Planificacion	0	0	0	0	0	0	2
7 - Apoyo	0	2	1	1	3	1	3
8 - Operación	0	0	1	1	0	1	0
9 - Evaluacion de desempeño	0	0	0	0	1	0	2
10 - Mejora	0	0	0	0	1	0	1
	0	**2**	**2**	**4**	**9**	**2**	**8**

Fuente: Elaboración Propia

Tabla 6: Distribución de temas según nivel de Madurez



Fuente: Elaboración Propia

Requisitos para la implementación de un SGSI

Luego de haber realizado un diagnóstico global, se analiza detalladamente cada punto de los requerimientos del marco ISO 27001, para ver la factibilidad de implementación del Sistema de Gestión de Seguridad de la Información.

1. Contexto de La Organización. Apartado 4 de ISO 27001

La organización deberá determinar los asuntos externos e internos que sean relevantes para su propósito y que afecten su capacidad, por lo que es de suma importancia comprender y conocer a la organización en su contexto interno y externo.

1.1. Contexto y Comprensión de las necesidades y las expectativas de las partes interesadas: En contexto estratégico existe un FODA que se hizo al momento de hacer la misión y Visión hace 4 o 5 años. En ese documento de Misión, Visión y valores está la parte de los stakeholders o sea los implicados en las operaciones. Se verifica que la empresa hace un análisis para la comprensión de necesidades y expectativas de las partes interesadas pero no se encuentran actualizados.

1.2. Determinación del alcance del SGSI: La organización deberá determinar los límites , en los cuales deben indicarse los activos críticos a proteger.

La empresa bajo estudio releva con un inventario de los activos que son los bienes de

uso y de capital. Dentro de cada área como los procesos principales de cobrar, pagar, comprar y vender están definidos y documentados.

Se verifica que existen algunas definiciones, pero faltan puntos para cumplir adecuadamente con los requisitos de la norma.

2. Liderazgo. Apartado 5 de ISO 27001

La alta dirección deberá demostrar liderazgo y compromiso con respecto al Sistema de Gestión de Seguridad de la Información al integrar los requisitos del sistema de gestión de seguridad de la información en los procesos de la organización y Comunicar la importancia de la gestión efectiva.

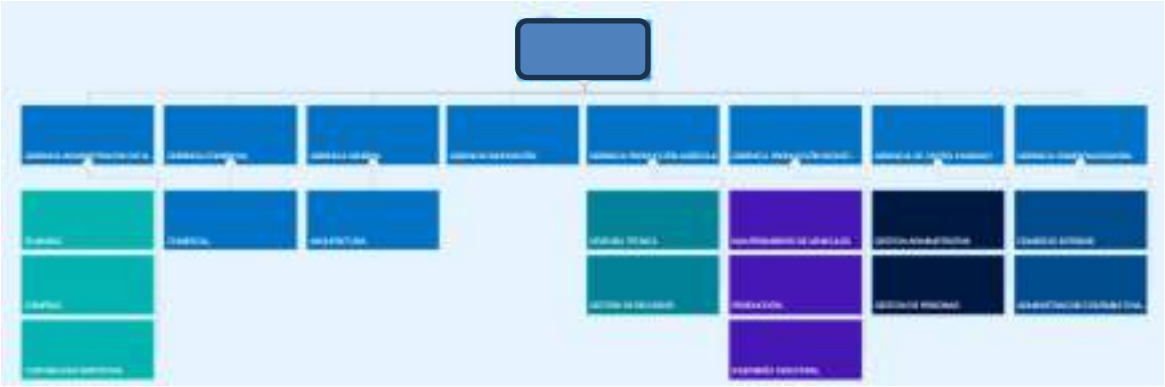
2.1. Liderazgo y Compromiso: Se debe tener en consideración la cultura organizacional y los recursos disponibles

2.2. Política : 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. Se verifica que la empresa tiene una política general que maneja recursos humanos sobre distintos aspectos de las distintas áreas. Pero no cuenta con una PSI, por lo que deberá establecer una política especifica.

2.3. Roles, responsabilidades y autoridades en la organización: La alta dirección debe asegurar que las responsabilidades y los roles relacionados a la seguridad de la información se determinen y se comuniquen.

La empresa no tiene designado un representante en el área de seguridad. Existe un área nueva de innovación y tecnología que se encargaría de los aspectos relacionados con TI y data. Por esta parte vemos que se debería incluir las responsabilidades de seguridad de la información al área y los roles pertinentes.

Tabla 7: Organigrama



Fuente: Área de Innovación y tecnología de la empresa

3. Planificacion. Apartado 6 de ISO 27001

La organización deberá establecer objetivos de seguridad de la información en funciones y niveles pertinentes. La organización deberá conservar información documentada sobre los objetivos de seguridad de la información.

3.1. Metodología de evaluación y tratamiento de riesgos: La organización deberá definir y aplicar un proceso de evaluación de riesgos de seguridad de la información. La organización deberá conservar información documentada sobre el proceso de evaluación de riesgos de seguridad de la información.

Se verifica que la empresa tiene un proceso de evaluación de riesgos para los distintos circuitos del funcionamiento del negocio. Tiene identificados los riesgos y planea el tratamiento de riesgos priorizando según la criticidad. Podrían agregar Riesgos de SI para cumplimentar lo requerido en ISO 27001.

Tabla 8: Mapa de riesgos y detalle

Fuente: Área de Innovación y tecnología de la empresa

4. Apoyo. Apartado 7 de ISO 27001

La organización debe determinar la competencia necesaria de las personas bajo su control y asegurarse que sean competentes en función a sus antecedentes documentados de educación, capacitación y experiencia previa.

4.1. Competencia: La empresa tiene un organigrama definido, perfiles de puesto, legajos del personal adecuadamente resguardados, en copia digital y física. Sin embargo, se debería incluir procedimientos específicos de SI para dar cumplimiento a los requisitos que plantea ISO 27001.

4.2. Concientización: No se cuenta con un "Plan Anual de Capacitaciones", si bien la empresa tiene capacitaciones cubiertas que están consideradas dentro del esquema de beneficios, no hay nada específico. Se tiene proyectado un taller inicial de ciberseguridad.

Tabla 9: Imagen de la Portada del Taller de concientización

Fuente: Área de Innovación y tecnología de la empresa

4.3. Comunicación: Se encuentran armando el departamento de comunicación. De todas formas, si existe un plan de comunicación interna y externa.

5. Operación. Apartado 8 de ISO 27001

5.1. Planificación y control operativos: a organización deberá planificar, implementar y

controlar los procesos necesarios para cumplir con los requisitos y llevar a cabo las acciones determinadas en la Cláusula 6, mediante criterios para los procesos.

No se han identificado y documentado los procesos críticos para los procesos operativos, pero si se tiene definido los propietarios responsables de cada activo y de su propia información.

5.2. Evaluación del riesgo a la Seguridad e la Información: La organización deberá realizar evaluaciones de riesgos de seguridad de la información en intervalos planificados o cuando se propongan o produzcan cambios significativos.

La empresa no ha realizado una revisión exhaustiva de sus activos de información críticos y de los riesgos asociados a su pérdida, pero si efectúan una evaluación del riesgo de los circuitos de negocios.

5.3. Tratamiento del riesgo a la Seguridad de la Información: Se deberá implementar el plan de tratamiento de riesgos de seguridad de la información. La organización deberá conservar información documentada de los resultados del tratamiento de riesgos de seguridad de la información.

Tabla 10: Gantt de proyecto de tratamiento de riesgos

Fuente: Área de Innovación y tecnología de la empresa

6. Evaluacion de Desempeño. Apartado 9 de ISO 27001

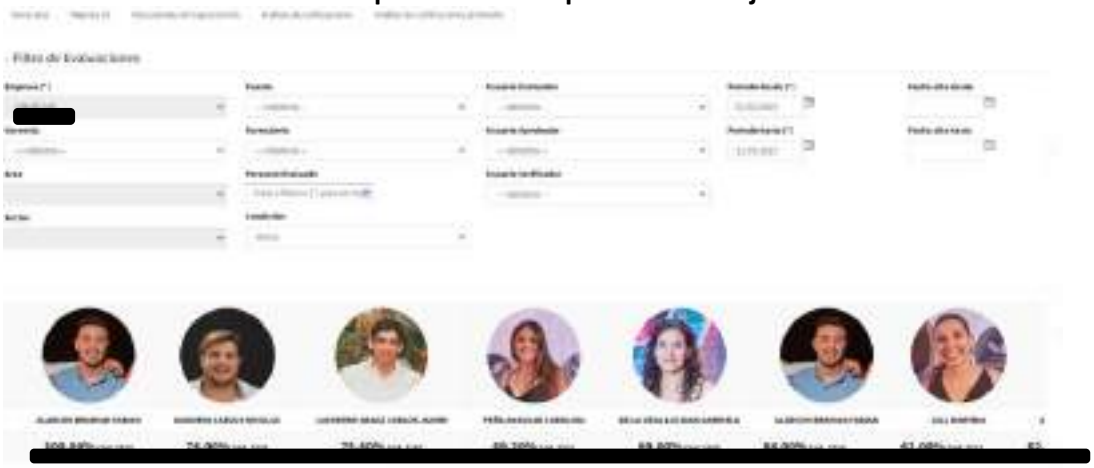
La Alta Dirección debe revisar el SGSI de la organización a intervalos planificados para asegurar que continúa siento pertinente, adecuado y eficaz

6.1. Seguimiento, medición, análisis y evaluación: La organización debe evaluar el

desempeño de la Seguridad de la Información y la eficacia del SGSI.

La empresa utiliza un sistema para para gestionar desempeño del personal. No se utiliza para evaluar el desempeño en cuanto a requisitos de Seguridad, pero puede ser incluido fácilmente en el sistema existente.

Tabla 11: Reporte de desempeño de los mejores 10



Fuente: Área de Innovación y tecnología de la empresa

6.2. Auditoría Interna: La organización debe realizar auditorías internas a intervalos planificados para proporcionar información acerca del funcionamiento del SGSI

En la empresa, se encuentra el área de auditoría interna que definen un plan anual de auditoría interna, que se va actualizando a medida que transcurre el tiempo.

A partir de estas, se redactan los reportes de auditoría interna para impulsar proyectos de equipos interáreas que se ponen en la tarea de la gestión del proyecto. Los resultados son presentados a la alta dirección. Debería efectuarse una adecuación a los requisitos de la Norma ISO 27001, en cuanto a los objetivos de Seguridad de la Información.

7. Mejora. Apartado 10 de ISO 27001

Cuando ocurra una no conformidad, la organización debe reaccionar ante ella y evaluar la necesidad de acciones para eliminar sus causas y evitar que se repita. Además, debe revisar su respectiva eficacia y conservar información documentada como evidencia

La organización debe mejorar continuamente la pertinencia, adecuación y eficacia del SGSI

7.1. No conformidad y acción correctiva: La empresa no lleva una evaluación de no conformidad y por consiguiente tampoco toma acciones correctivas. Deberá implementarse una evaluación y seguimiento de las no conformidades para

7.2. Mejora continua: La organización deberá mejorar continuamente la idoneidad, la suficiencia y la eficacia del sistema de gestión de seguridad de la información.

A partir del criterio profesional se puede concluir que la empresa tiene un principio de mejora continua, optimizado y actualizado en cuanto a los temas para su funcionamiento y continuidad de negocio.

Conclusiones

Este El análisis realizado ha demostrado que es factible la implementación de un Sistema de Gestión de Seguridad de la Información (SGSI) en el grupo económico exportador de la provincia de Tucumán. El grupo cuenta con una estructura sólida y un equipo de profesionales calificados, lo que le permite cumplir con los requisitos de la norma ISO 27001.

Sin embargo, también se han identificado algunas áreas a mejorar. Estas áreas se centran principalmente en los puntos de liderazgo, operación y apoyo.

Con el compromiso de la dirección y la implementación de las acciones correctivas necesarias, el grupo podrá implementar un SGSI exitoso que le permita proteger sus activos de información y cumplir con los requisitos legales y reglamentarios e impulsar el crecimiento en cuanto a su seguridad de la información.

Recomendaciones

Para garantizar el éxito de la implementación del SGSI, se recomienda que el grupo adopte las siguientes medidas:

- Definir una política de seguridad de la información que establezca los objetivos y principios del SGSI.

- Desarrollar procedimientos para apoyar la política de seguridad de la información.
- Formar al personal en las políticas y procedimientos de seguridad de la información.

El grupo también puede considerar la posibilidad de contratar a un consultor externo para que lo apoye en la implementación del SGSI. Un consultor externo puede proporcionar experiencia y conocimientos que pueden ser valiosos para el grupo.

La implementación de un SGSI es una inversión importante que puede proporcionar al grupo muchos beneficios. Un SGSI bien implementado puede ayudar al grupo a proteger sus activos de información, cumplir con los requisitos legales y reglamentarios, y mejorar su reputación.

Referencias

- *Instituto Nacional de Ciberseguridad. (2021). Glosario de términos de ciberseguridad: Una guía de aproximación para el empresario.*
- *Arizabaleta, E. (2004) Diagnóstico Organizacional. Ecoe Ediciones.*
- *Hernández Samieri, A. (2018). Metodología de la Investigación. Mc Graw Hill educación.*
- *Gómez Vietes, A. (2014) . Auditoría de seguridad Informática. Starbook*
- *Arévalo Ascanio, J. G., Bayona Trillos, R. A., & Rico Bautista, D. W. (2015). Implantación de un sistema de gestión de seguridad de información bajo la ISO 27001: Análisis del riesgo de la información. Revista Tecnura.*
- *ISO/IEC 27000:2018, cláusua 2.46*

Anexo

ANEXOS

Empresa:	Grupo MP
Lugar(es) / Instalación(es):	Sede Central, ubicada en Yerba Buena Tucumán.
Alcance:	Área Administrativa, con mirada en el Área de TI
Norma aplicable, Criterios de auditoría:	ISO/IEC 27001:2022 Documentación del sistema de gestión de la organización Condiciones de certificación
Tipo de auditoría:	Análisis de Brecha para Implementación de SGSI
Representante de la empresa:	Gerente General (C.E.O)
Objetivo de la entrevista Inicial:	Recabar información
Lengua(s) de auditoría:	Español
Auditor: Aceñolaza Chamorro Inés	
☐ externo, empresa:	☐
Ciudad, fecha de elaboración del plan de auditoría:	Tucumán, 08/09/23

Día 1				
Tiempo desde	**hasta**	**Requisitos**	**Entrevistado**	**Procesos**
14:30	15:00	Reunión de apertura, Entrevista con la dirección	**Todos, Gestión**	**Introducción y coordinación del plan de auditoría** **Presentación de los procesos empresariales relevantes para la seguridad de la información en la empresa**
15:00	15:30	4.Contexto. 4.1 FODA 4.2 Partes Interesadas 4.3 Alcance SGSI 5. Liderazgo 6.2	Gerente C.E.O	**Contexto de la organización** **Comprender la organización y su contexto** **Comprender las necesidades y expectativas de las partes interesadas. Determinar el alcance del sistema de gestión de la seguridad de la información** **Liderazgo. La Política de SI Objetivos de Seguridad de la**

				Información. Roles y Responsabilidades
		Reunión de cierre		

Día 2				
Tiempo desde hasta		**Unidad organizativa y procesos**	**Entrevistado**	**Capítulo estándar**
09:00	11:00	6. Planificación, Gestión de riesgos 6.1.2 - Metodología de evaluación y tratamiento de riesgos 6.1.3.e Plan de tratamiento de riesgos 8 Operación	**Area de TI**	**Acciones para hacer frente a los riesgos y oportunidades (6.1.1, 6.1.2, 6.1.3)** **Objetivos de seguridad de la información y planificación para alcanzarlos** **Informe de evaluación de riesgos Inventario**

		8.1 Planificación y control operativos 8.2 Evaluación de los riesgos para la seguridad de la información 8.3 Tratamiento de los riesgos para la seguridad de la información Anexo A		**de activos** **Política de control de acceso** **Procedimientos operativos para la gestión de TI**
11:00	12:30	7 Apoyo 7.1 Recursos 7.2 Competencias 7.3 Sensibilización 7.4 Comunicación 7.5 Información documentada 9 Evaluación de resultados 9.1 Seguimiento, medición, análisis y evaluación 9.2 Auditoría interna 9.3 Revisión por la	Gerente de Area: Administracion Area de TI	**Registros de formación, habilidades, experiencia y cualificaciones - RRHH** Sensibilización, información documentada, etc. Indicadores clave de rendimiento, Auditoría interna, Mejora continua Resultados de las acciones correctivas - Administracion.

		dirección 10 Mejoras 10.1 Mejora continua 10.2 No conformidad y medidas correctoras		Registros de actividades de usuarios, excepciones y eventos de seguridad - TI
15:30	16:30	Política de seguridad de la información		
16:30	17:30	Documentación del auditor	Sólo auditores	

Los objetivos de la entrevista inicial/ auditoria:

a) revisar la información documentada

b) evaluar las condiciones específicas de la empresa y entablar conversaciones con el personal.

c) revisar el estado y la comprensión de la empresa en relación con los

requisitos de la norma, en particular con respecto a la identificación de los aspectos claves de la Seguridad de la Información.

d) obtener la información necesaria sobre el alcance del sistema de gestión, incluyendo:

- las instalaciones del cliente,
- procesos y equipos utilizados,
- niveles de control establecidos,

El objetivo de la auditoría es confirmar la aplicabilidad del SGSI para el alcance propuesto.

ANEXO 2

Redaccion de las preguntas para usuarios diferentes: CEO, Gerentes y Area de TI

REQUISITO	PREGUNTA	CRITERIO DE AUDITORÍA	REQUISITO
Contexto de la Organización	¿Se evalúan los riesgos y oportunidades del contexto para asegurar que el SGSI pueda lograr los resultados previstos, reducir los efectos no deseados y lograr la mejora continua? (FODA, PEST, Fuerzas de Porter)	4.1 - Comprensión de la Organización y su contexto 6.1 - acciones para tratar el riesgo y las oportunidades	La organización debe determinar las cuestiones internas y externas que son pertinentes a su propósito y afectan su capacidad para alcanzar los resultados previstos en su SGS
	¿Tienen identificadas y documentadas las necesidades de las "partes interesadas" del negocio?	4.2 - Comprensión de las necesidades y las expectativas de las partes interesadas	La organización debe determinar las partes interesadas pertinentes al SGSI y sus requisitos de seguridad de la información
	¿Cómo identifica los activos críticos y la información sensible que deberían quedar sujetos a las medidas de seguridad en el alcance de un SGSI?	4.3 - Determinación del alcance del SGSI	La organización debe determinar los límites y la aplicabilidad del SGS para establecer su alcance
Liderazgo	¿Se ha designado un representante de la alta dirección con responsabilidades específicas para la seguridad de la información? ¿Cuáles son sus funciones ? ¿Se ha planeado un intervalo de revisión para las políticas de S. de la Inf. de comprobar su pertinencia, adecuación y eficacia?	5.1 - Liderazgo y Compromiso	La alta dirección debe asegurar la integración de los requisitos del SGS con los procesos de la organización
	¿Poseen una "política de seguridad de la información" definida y documentada? ¿La misma es comunicada a las partes interesadas?	5.2 - Política	La alta dirección debe establecer una política de seguridad de la información documentada. La misma debe ser comunicada y estar disponible para las partes interesadas
	¿Qué roles y responsabilidades específicos se han asignado en su organización para la gestión de la seguridad de la información? ¿Quiénes son los responsables de supervisar y garantizar el cumplimiento de las políticas y procedimientos de seguridad?	5.3 - Roles, responsabilidades y autoridades en la organización	La alta dirección debe asegurar que las responsabilidades y autoridades para los roles pertinentes a la Seguridad de la información se asignen y se comuniquen
Planificación y Gestión de Riesgos	¿Tienen definidos y documentados "objetivos" y "métricas"? Hay alguno relacionado con la SI? Hay necesidad o actualizaciones de estos objetivos?	6.2 - Objetivos de SI y planificación para lograrlos	La organización debe establecer y documentar objetivos de Seguridad de la información para las funciones y niveles pertinentes
	¿Cómo identifica y evalúa su organización los riesgos y oportunidades que pueden afectar a la seguridad de la información? ¿Qué acciones específicas ha tomado su organización para abordar los riesgos identificados en relación con la seguridad de la información?	6.1 Acciones para abordar riesgos y oportunidades	
	¿Se han establecido procedimientos de mitigación de riesgos? ¿Cómo se comunica la política de seguridad de la información a los empleados y partes interesadas, y cómo se asegura de que entienden y se cumplan?	6.1.2 - Valoración de evaluación y tratamiento de riesgos	La organización debe implementar el plan de tratamiento del riesgo a la Seguridad de la información y mantener información documentada a respecto

	¿Cuáles son los recursos disponibles actualmente para la implementación de un SGSI, como presupuesto, personal o tecnología?	6.1.3 c) Recursos necesarios	
Operación	¿Se han identificado y documentado los procesos críticos para los procesos operativos? ¿Se han definido los propietarios responsables de cada una de los activos comprendidos en el inventario?	8.1 Planificación y control operativos	
	¿Los empleados y usuarios de partes externas devuelven todos los activos de la organización en su poder tras la terminación de su empleo, contrato o acuerdo?		
	¿Ha realizado la organización una revisión exhaustiva de sus activos de información críticos y de los riesgos asociados a su custodia o compromiso? ¿Revisan una evaluación del riesgo a la seguridad de la información de manera periódica? (anexo "A")	8.2 - Evaluación del riesgo a la Seguridad de la Información	La organización debe realizar evaluaciones de riesgo a la seguridad de la información a intervalos planificados o cuando ocurren cambios significativos. Se debe conservar información documentada al respecto
	¿Planifican el adecuado tratamiento del riesgo de Seguridad de la información sobre los activos de información identificados? ¿Se cuenta documentación al respecto? ¿Está la información debidamente clasificada de acuerdo con los requisitos legales, su valor, su sensibilidad y su criticidad?	8.3 - Tratamiento del riesgo a la Seguridad de la Información	La organización debe implementar el plan de tratamiento del riesgo a la Seguridad de la información y mantener información documentada a respecto

Soporte	¿Existe en la compañía un organigrama definido y documentado?	7.1 - Recursos	La organización debe determinar y proporcionar los recursos necesarios para el establecimiento, la implementación, el mantenimiento y la mejora continua del SGSI
	¿Se realiza una verificación de antecedentes de todos los candidatos al empleo según las leyes, regulaciones y ética relevantes, y debe verificarse en proporcionalidad con los requisitos del negocio, con la clasificación de la información a ser accedida y con los riesgos percibidos? ¿Poseen un legajo físico del personal?	7.1. antes del empleo, durante	
	¿La organización cuenta con "Perfiles de Puesto" documentados que provean las habilidades que debe tener cada colaborador, teniendo en cuenta su rol y función desempeñada? Tienen responsabilidades para y con la ley	7.2 - Competencia	La organización debe determinar la competencia necesaria de las personas bajo su control y asegurarse que sean competentes en función a sus antecedentes documentados de educación, capacitación y experiencia previa
	¿Existe un proceso disciplinario formal y comunicado a todos los empleados, para tomar acciones ante fallas en el incidente relacionado a la seguridad?	7.2 - Competencia	La organización debe determinar la competencia necesaria de las personas bajo su control y asegurarse que sean competentes en función a sus antecedentes documentados de educación, capacitación y experiencia previa
	¿Efectúan evaluaciones periódicas desempeño al personal?	7.2 - Competencia	La organización debe determinar la competencia necesaria de las personas bajo su control y asegurarse que sean competentes en función a sus antecedentes documentados de educación, capacitación y experiencia previa
	¿Los procedimientos de negocio relevantes o críticos están documentados?	7.2 - Competencia	La organización debe determinar la competencia necesaria de las personas bajo su control y asegurarse que sean competentes en función a sus antecedentes documentados de educación, capacitación y experiencia previa

	¿Tienen definido un cronograma anual de capacitación y concientización de Seguridad de la Información?	7.3 - Concientización	Las personas que realizan trabajos para la organización deben ser conscientes de la Política de Seguridad de la Información, su contribución a la eficacia del SGSI y las implicancias de su incumplimiento
	¿Los miembros de la organización tienen acceso y conocen todos los aspectos que atiende la Política de Seguridad de la Información?	7.3 - Concientización	Las personas que realizan trabajos para la organización deben ser conscientes de la Política de seguridad de la información, su contribución a la eficacia del SGSI y las implicancias de su incumplimiento.
	¿Se definen, comunican y se hacen cumplir a los empleados o contratistas, las responsabilidades y las obligaciones relativas a la SI que continúan estando vigentes luego de la desvinculación o cambio de puesto?	7.3 - Concientización	Las personas que realizan trabajos para la organización deben ser conscientes de la Política de seguridad de la información, su contribución a la eficacia del SGSI y las implicancias de su incumplimiento.
	¿La organización cuenta con un "Plan de Comunicación Interna y Externa" respecto al SGSI?	7.4 - Comunicación	La organización debe determinar la necesidad de comunicaciones internas y externas pertinentes al SGSI
	¿Los empleados y, cuando sea pertinente los contratistas, reciben concientización, educación y capacitación actualizadas, y actualizaciones regulares de las políticas y procedimientos organizacionales, que sean pertinentes a su labor?	7.5.1 - Generalidades de la información documentada	El SGSI de la organización debe incluir la información documentada requerida por ISO 27001 y aquella considerada necesaria para la eficacia del SGSI

Ver normas APA de: https://normas-apa.org/wp-content/uploads/Guia-Normas-APA-7ma-edicion.pdf