UNIVERSIDAD INTERNACIONAL DE LA RIOJA

GOBIERNO DE LA CIBERSEGURIDAD

Actividad 1: Realizando una pre-auditoría de SGSI

Descripción breve

En esta actividad se busca aprender a trabajar con una herramienta de apoyo para realizar una pre-auditoría del nivel de cumplimiento de gestión de la seguridad de Industrias Vaine.

Daniel Barbeyto Torres

danibarbeytotorres@gmail.com

Contenido

1. Introducción

En la actualidad, la seguridad de la información se ha convertido en un pilar fundamental para la empresa, sobre todo a la hora de gestionar los activos más sensibles de una organización. Por eso mismo, la implementación de un Sistema de Gestión de Seguridad de la Información (SGSI) adaptado a la empresa proporcionara a esta los niveles de protección que necesita contra los posibles riesgos (tanto internos como externos).

Esta memoria recoge la pre-auditoría realizada para la empresa ficticia Industrias Vaine, dedicada a actividades de seguridad, defensa, inteligencia y comunicaciones. Su perfil requiere un enfoque sólido y avanzado de la seguridad de la información, más allá de una serie de medidas implantadas aisladamente.

A continuación, se describirá el proceso completo de pre-auditoría del SGSI siguiendo la norma ISO 27001/2:2022 con apoyo de la herramienta eMarisma para la documentación del proyecto. En este procedimiento se incluirán la definición de los activos, la evaluación de controles sobre los 4 grandes dominios y el análisis del SOA, entre otros.

El objetivo es ofrecer una visión clara del nivel de madurez de la empresa, identificando carencias significativas y proponiendo un plan real de mejoras alineado con las prácticas de seguridad de la información que la norma ISO 27001/2:2022 recomienda, y que deberían estar en un buen SGSI.

2. Estándares base

Para realizar esta pre-auditoría, se usará como estándar base la ISO 27001/2:2022. Guiándonos de este estándar tendremos el conocimiento para poder crear, integrar o mejorar un SGSI, asegurando la protección los activos sensibles de la empresa.

Para ello, el estándar cuenta con una guía de buenas prácticas donde los controles que la gestión de la seguridad de la información debe pasar se dividen en 4 grandes dominios: Organizativos [AO], Personas [AP], Infraestructuras [AI] y Tecnología [AT].

Gracias a este estándar base, se podrá realizar una evaluación del nivel de madurez de la empresa, a la vez que detectamos y medimos sus carencias y proporcionamos un plan de mejora.

3. Descripción de la empresa

Industrias Vaine es una empresa multinacional ficticia de tecnología avanzada, ubicada en Gotan City, conocida por sus desarrollos en tecnología de defensa, inteligencia y comunicación. Al ser uno de los objetivos favoritos de ataques por parte de organizaciones criminales, *hackers* y agentes hostiles, la seguridad de la información es una prioridad para mantener su integridad operativa y proteger los secretos industriales y tecnológicos.

Por esto mismo, la directiva de la empresa y el mismo propietario, Bruce Vaine, ha decidido certificarse un SGSI basado en el estándar base ISO 27001/2. Es por ello por lo que solicita una preauditoria para poder conocer la situación actual de seguridad.

4. Descripción del proyecto

En las siguiente captura, se puede ver la inicialización del proyecto en la herramienta eMarisma. En el apartado "Sector Empresarial", a falta de una opción más especifica para el caso de Industrias Vaine, se usará "6209 – Otros servicios relacionados con las tecnologías de la información y la informática".

El proyecto abarcará toda la organización a nivel corporativo, incluyendo la infraestructura tecnológica, los procesos críticos de negocio y tanto el personal propio como terceros con acceso a información.

La inicialización del proyecto establece el punto de partida para la implementación del SGSI y la formalización de políticas y procesos según el estándar base.

5. Categorización de activos

Para la creación de los activos, en eMarisma debemos que un subproyecto (únicamente por el modo de funcionamiento de la herramienta). El nombre del subproyecto será "Preauditoría SGSI". Una vez creado el subproyecto, ya podremos proceder a crear los 15 activos.

1. **Altavoces ambientales de zonas comunes**

- Tipo: [AUX] – Equipamiento auxiliar
- Subtipo: supply – Suministros esenciales
- Propietario: Departamento de comunicación
- Responsable: Técnico Audiovisual
- Valor estratégico: Muy bajo
- Descripción: Sistema de altavoces que reproduce avisos generales y música ambiental.

2. **Centro de Procesamiento de Datos de Industrias Vaine**

- Tipo: [L] – Instalaciones
- Subtipo: building – Edificio
- Propietario: Dirección General
- Responsable: Facilities Manager

- Valor estratégico: Muy Alto
- Descripción: Instalación física donde se concentran los servidores y almacenamientos que soportan los sistemas críticos de la organización.

3. Clúster de análisis criptográfico

- Tipo: [HW] – Equipos informáticos (hardware)
- Subtipo: host – Grandes equipos
- Propietario: Departamento de I+D
- Responsable: Administrador de Sistemas Críticos
- Valor estratégico: Alto
- Descripción: Conjunto de servidores dedicado a pruebas de algoritmos criptográficos y análisis de comunicaciones cifradas

4. Firewall perimetral

- Tipo: [HW] – Equipos informáticos (hardware)
- Subtipo: bp – Dispositivo de frontera
- Propietario: Dirección de tecnología
- Responsable: Administrador de red
- Valor estratégico: Alto
- Descripción: Dispositivo de seguridad perimetral que filtra el tráfico entre Internet y la red interna, mitigando ataques externos.

5. Iluminación automatizada de salas comunes

- Tipo: [L] – Instalaciones
- Subtipo: channel – Canalización
- Propietario: Mantenimiento
- Responsable: Responsable de instalaciones
- Valor estratégico: Muy Bajo
- Descripción: Sistema de encendido automático de luces en zonas compartidas.

6. Inteligencia sobre amenazas internacionales

- Tipo: [D] – Datos / Información
- Subtipo: files – ficheros
- Propietario: Departamento de Inteligencia
- Responsable: Analista Principal de Inteligencia
- Valor estratégico: Muy Alto
- Descripción: Base de datos con perfiles de actores y técnicas hostiles conocidas. Esto es información fundamental para decisiones estratégicas de seguridad.

7. Programa de Desarrollo de Sistemas de Defensa "Aegis-V"

- Tipo: [D] – Datos / Información
- Subtipo: Int – Datos de gestión interna
- Propietario: Dirección General
- Responsable: CISO
- Valor estratégico: Muy Alto
- Descripción: Documentación clasificada que incluye, entre otros, especificaciones, algoritmos y

diseño de los sistemas Aegis-V. Su compromiso supondría un riesgo nacional y una pérdida total de ventaja estratégica.

8. Red cableada de la zona de descanso

- Tipo: [COM] – Redes de comunicaciones
- Subtipo: LAN – Red local
- Propietario: TIC
- Responsable: Administrador de redes
- Valor estratégico: Muy Bajo
- Descripción: Conexiones básicas disponibles en la zona de descanso para uso no crítico del personal. Está aislada del core de la red.

9. Red WiFi de invitados

- Tipo: [COM] – Redes de comunicaciones
- Subtipo: wifi – Red inalámbrica
- Propietario: TIC
- Responsable: Administrador de redes
- Valor estratégico: Bajo
- Descripción: Red inalámbrica aislada destinada a visitas y proveedores. No tiene acceso a la infraestructura interna.

10. Repositorio GitLab de proyectos clasificados

- Tipo: [SW] – Aplicaciones (software)
- Subtipo: prp – Desarrollo propio (in house)
- Propietario: Departamento de I+D
- Responsable: Líder DevOps
- Valor estratégico: Alto
- Descripción: Plataforma de control de versiones que almacena el código fuente de los proyectos de defensa, inteligencia y comunicaciones seguras.

11. Servicio interno de reserva de salas

- Tipo: [S] – Servicios
- Subtipo: int – Interno (a usuarios de la propia organización)
- Propietario: Administración
- Responsable: Técnico de sistemas
- Valor estratégico: Bajo
- Descripción: Servicio para gestionar reservas de salas de reuniones. No afecta a operaciones críticas.

12. Servidor de correo electrónico

- Tipo: [S] – Servicios
- Subtipo: email – Correo electrónico
- Propietario: Departamento TIC
- Responsable: Administrador de mensajería
- Valor estratégico: Medio
- Descripción: Servidor interno utilizado para el intercambio de correo electrónico de toda la organización, con uso mixto de información sensible y operativa.

13. Sistema biométrico de control de accesos a laboratorios

- Tipo: [AUX] – Equipamiento auxiliar
- Subtipo: supply – Suministros esenciales
- Propietario: Departamento de seguridad física
- Responsable: Responsable de Infraestructura
- Valor estratégico: Medio
- Descripción: Sistema de control de accesos basado en biometría que protege la entrada a laboratorios y áreas restringidas.

14. Sistema de copias de seguridad externas

- Tipo: [ARCH] – Arquitectura del sistema
- Subtipo: ext – Proporcionado por terceros
- Propietario: CTO
- Responsable: Administrador de Backup
- Valor estratégico: Medio
- Descripción: Solución de backup remoto que almacena copias cifradas de los sistemas clave para garantizar la continuidad ante desastres.

15. Sistema interno de encuestas al personal

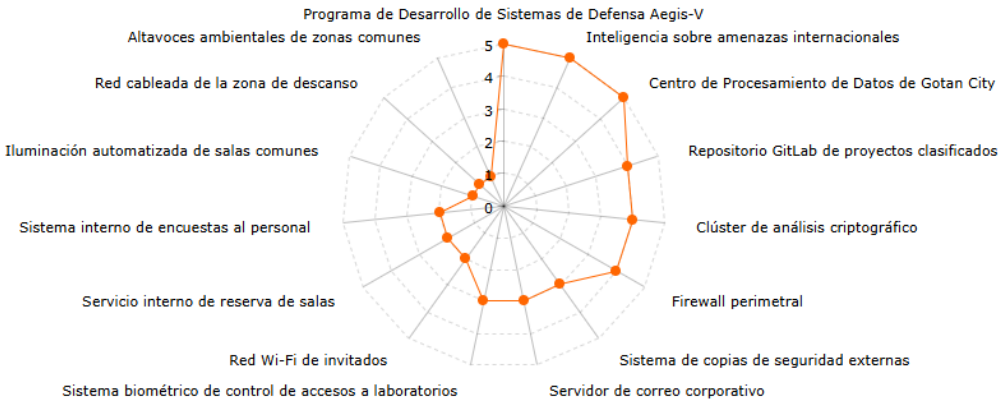
- Tipo: [S] – Servicios
- Subtipo: int – Interno (a usuarios de la propia organización)
- Propietario: Departamento de RRHH
- Responsable: Técnico de RRHH
- Valor estratégico: Bajo
- Descripción: Servicio externo contratado para realizar encuestas de satisfacción al personal. No gestiona información crítica y su interrupción tiene impacto mínimo en la operación.

En las siguientes capturas se muestra la correcta configuración de los activos en eMarisma.

Tipo	Nombre	Propietario	Resp.	Coste	Valor	Descripción
Equipamiento auxiliar	Altavoces ambientales de zonas comunes	Comunicación Interna	Técnico Audiovisual	0.00€	Muy Bajo	Sistema de altavoces que reproduce avisos generale...
Instalaciones	Centro de Procesamiento de Datos de Gotan City	Dirección General	Facilities Manager	0.00€	Muy Alto	Instalación física donde se concentran los servido...
Equipos informáticos (hardware)	Clúster de análisis criptográfico	Departamento de I+D	Administrador de Sistemas Críticos	0.00€	Alto	Conjunto de servidores dedicado a pruebas de algor...
Equipos informáticos (hardware)	Firewall perimetral	Dirección de tecnología	Administrador de red	0.00€	Alto	Dispositivo de seguridad perimetral que filtra el ...
Instalaciones	Iluminación automatizada de salas comunes	Mantenimiento	Responsable de instalaciones	0.00€	Muy Bajo	Sistema de encendido automático de luces en zonas ...
Datos / Información	Inteligencia sobre amenazas internacionales	Departamento de Inteligencia	Analista Principal de Inteligencia	0.00€	Muy Alto	Base de datos con perfiles de actores y técnicas h...
Datos / Información	Programa de Desarrollo de Sistemas de Defensa "Aegis-V"	Dirección General	CISO	0.00€	Muy Alto	Documentación clasificada que incluye, entre otros...
Redes de comunicaciones	Red cableada de la zona de descanso	TIC	Administrador de redes	0.00€	Muy Bajo	Conexiones básicas disponibles en la zona de desca...
Redes de comunicaciones	Red Wi-Fi de invitados	TIC	Administrador de redes	0.00€	Bajo	Red inalámbrica aislada destinada a visitas y prov...
Aplicaciones (software)	Repositorio GitLab de proyectos clasificados	Departamento I+D	Líder DevOps	0.00€	Alto	Plataforma de control de versiones que almacena el...

Tipo	Nombre	Propietario	Resp.	Coste	Valor	Descripción
Servicios	Servicio interno de reserva de salas	Administración	Técnico de sistemas	0.00€	Bajo	Servicio para gestionar reservas de salas de reuni...
Servicios	Servidor de correo corporativo	Departamento TIC	Administrador de mensajería	0.00€	Medio	Servidor interno utilizado para el intercambio de ...
Equipamiento auxiliar	Sistema biométrico de control de accesos a laboratorios	Departamento de seguridad física	Responsable de Infraestructura	0.00€	Medio	Sistema de control de accesos basado en biometría ...
Arquitectura del sistema	Sistema de copias de seguridad externas	CTO	Administrador de Backup	0.00€	Medio	Solución de backup remoto que almacena copias cifr...
Servicios	Sistema interno de encuestas al personal	Departamento de RRHH	Técnico de RRHH	0.00€	Bajo	Servicio externo contratado para realizar encuesta...

La siguiente figura muestra un gráfico donde se muestra el valor estratégico de cada uno de los activos.



6. Análisis de controles

Para el análisis de los controles, se ha realizado una agrupación que acoge a todos los activos que hemos creado, y se le ha llamado “Preauditoría Checklist”. A continuación, mediante una serie de controles, podremos comprobar el nivel de madurez de la empresa según el estándar ISO 27001/2:2022 en cada uno de los 4 grandes dominios. Los controles han sido analizados en base a las preguntas que pertenecen a cada control, dando respuesta en todos los casos detalladamente a cada una de ellas (asumiendo que dichos enunciados de las preguntas se conoce).

Controles del Dominio Organizativo [AO]

Control A.05.04 – Responsabilidades de gestión

Bruno Vaine (el director de Industrias Vaine) ha declarado claramente su intención de implantar un SGSI conforme a la ISO 27001/2, sobre todo debido a la gran sensibilidad de varios de sus activos. Aunque existe una intención clara y real expresada por su director, la empresa todavía no ha formalizado oficialmente las políticas y procedimientos apropiados. Entre otros elementos a destacar señalamos:

- No se ha planteado una política de seguridad de forma oficial
- No se ha planteado una política de protección para los activos tecnológicos.
- Una gran parte del personal no conoce la intención de la directiva de establecer dicho SGSI.

Por otro lado, Industrias Vaine cuenta con una serie de prácticas internas de seguridad para proteger activos especialmente sensibles (por ejemplo, el firewall perimetral), pero de momento la asignación

de roles en la empresa sugiere estar más basado en la experiencia del personal técnico que en un proceso directivo basado en un documento formalizado de roles y responsabilidades.

Porcentaje de control: 25% (NO CUMPLE)

Control A.05.11 – Devolución de activos

Industrias Vaine cuenta con una serie de prácticas internas que pertenecen a un procedimiento formalizado de desvinculación gestionado por el departamento de RRHH que, efectivamente, incluye la devolución de todos los activos físicos y electrónicos bajo custodia de la organización, como tarjetas de acceso o equipo especializado asignado.

No obstante, este procedimiento aún no está alineado con los requisitos de documentación que exige el SGSI que la directiva de Industrias Vaine busca, motivo por el cual su alcance no está completamente integrado con el marco de gestión formal a desarrollar.

Por otro lado, no existe un procedimiento formal que regule la gestión de información almacenada en dispositivos o propios de la organización durante el ejercicio laboral. Tampoco se realizan de forma oficial verificaciones sistemáticas que aseguren la eliminación o devolución de datos sensibles.

Asimismo, en algunas áreas de la organización como I+D y ciberseguridad si se realiza cierta documentación técnica y memoria de los conocimientos críticos (almacenada en repositorios de Github, informes operativos, etc.) pero la transferencia de dicho conocimiento no está formalizada. No hay un proceso formal definido para garantizar la retención de la información en caso de una desvinculación.

A pesar de que no se cuenta con un proceso formalizado por la ISO 27001/2, Industrias Vaine dispone de medidas eficaces que impiden la copia no autorizada de información sensible mediante firewall perimetral, revocación rápida de privilegios y restricciones en sistemas críticos bien controladas y monitorizadas. La empresa realiza un control realista de este riesgo durante el periodo previo a la desvinculación del personal.

Por último, sí que se realiza un registro de inventario básico de los activos sensibles delegados al personal (como tarjetas de acceso, dispositivos portátiles y equipamiento especializado), pero el inventario no es totalmente completo ni uniforme (sobre todo en activos de uso común), lo que impide asegurar la notificación exhaustiva de absolutamente todos los elementos a devolver en un proceso formal de desvinculación.

Porcentaje de control: 60% (CUMPLE PARCIALMENTE)

Control A.05.25 – Evalución y decisión sobre eventos de seguridad de la información

Industrias Vaine cuenta con mecanismos y técnicas de clasificación y detección de eventos de seguridad (por ejemplo, alertas en el firewall perimetral o actividades anómalas en las redes internas, entre otros), pero no hay un esquema formalizado de categorización y priorización completamente documentado dentro de un marco SGSI basado en la ISO 27001/2. Es decir, se cuentan con las capacidades prácticas internas y hay un procedimiento dictado a seguir, pero dicho proceso no está aún correctamente estandarizado.

Por otro lado, la empresa dispone de un equipo técnico con experiencia y dotado que realiza evaluaciones operativas completas de los eventos que han sido detectados. Cuando se diagnostica

una actividad anómala en las redes internas, el personal especializado investiga y toma decisiones de contención o escalado según la gravedad e impacto de esta, de forma que dicha evaluación práctica de eventos si se realiza de forma efectiva.

Por último, añadir que no existe un procedimiento de documentación formal y estructurado para la evaluación de los eventos de seguridad. Existen una serie de registros técnicos para tomar decisiones almacenados en un repositorio de datos común, pero la mayoría son logs realizados por herramientas de seguridad.

Porcentaje de control: 50% (CUMPLE PARCIALMENTE)

Control A.05.26 – Respuesta a incidentes de seguridad de la información

Industrias Vaine dispone de prácticas internas para responder a los incidentes de seguridad, pero no cuentan todavía con un procedimiento formalizado como parte del SGSI. Es decir, el equipo técnico sabe cómo actuar de forma informal sin un procedimiento oficial o un plan de respuesta documentado bajo la ISO 27001/2.

Por otro lado, aún dada la ausencia de un SGSI formal, los incidentes de seguridad son respondidos por equipos técnicos de alta especialización, especialmente en las areas de comunicación y ciberseguridad. El proceso no está documentado bajo la ISO 27001/2, pero la respuesta es efectiva y realizada bajo un personal cualificado.

Industrias Vaine cumple varios de los puntos planteados gracias a sus capacidades internas, entre ellos la contención de los sistemas afectados por el incidente (a), la recogida de evidencias tan pronto como sea posible (b), el escalado del incidente si asi requiere (c), la comunicación de la existencia del incidente a las partes interesadas (e) y la coordinación puntual con los proveedores para la mejora de la efectividad de la respuesta (f).

El resto de puntos no se cubre correctamente por la falta de la estandarización de los puntos d, g, h, i y j, resultando en que la empresa tiene una respuesta operativa efectiva, pero no alineada con un proceso ISO completo.

Porcentaje de control: 66.66% (CUMPLE PARCIALMENTE)

Control A.05.27 – Aprendizaje de los incidentes de seguridad de la información

En la empresa no existe un marco estructurado y estandarizado que permita evaluar los costes de incidentes de seguridad de la información formalmente, impidiendo una medición consistente o un análisis comparativo de incidentes.

Por otro lado, la información obtenida de incidentes permite introducir ciertos ajustes operativos, especialmente en incidentes relacionados con los activos más sensibles de la compañía. El equipo técnico aprende de los incidentes más recurrentes y aplica correcciones basadas en la experiencia directa, pero el dicho conocimiento no está integrado en un marco formal de mejora del SGSI, de forma que si hay un aprendizaje práctico, pero no está sistematizado ni documentado según la ISO 27001/2.

Porcentaje de control: 25% (NO CUMPLE)

Controles del Dominio Personas [AP]

Control A.06.02 – Términos y condiciones de empleo

Industrias Vaine incorpora en sus contratos la casi totalidad de los puntos señalados en esta parte del control. El personal firma contratos donde estos conocen las obligaciones básicas de seguridad debido a la naturaleza sensible de la actividad. No obstante, no se cuenta aún con las políticas de seguridad formalizadas y estandarizadas que el marco de un SGSI en base a la ISO 27001/2 indica.

Sin embargo, la empresa no cuenta ni con una definición formal de los roles y responsabilidades en materia de seguridad ni con un proceso de comunicación previo a la contratación donde dichos roles y responsabilidades se transmitan de manera formal tal y como describiría el marco de un SGSI.

Por otro lado, el personal firma contratos donde se comunican los términos de seguridad básicos y las obligaciones y condiciones de la empresa relativas a la seguridad de la información, pero estas cláusulas no están vinculadas a una política formal de seguridad ni a un procedimiento de revisión periódica estandarizado.

Por último, los acuerdos y NDAs firmados por el personal durante su ejercicio laboral incluyen correctamente una serie de obligaciones posteriores referidos a la confidencialidad, una vez su contrato finaliza. La empresa es cautelosa en este punto debido a la naturaleza sensible de sus activos, y dichas obligaciones se mantienen vigentes tras una desvinculación con el personal.

Porcentaje de control: 50% (CUMPLE PARCIALMENTE)

Control A.06.04 – Proceso Disciplinario

La empresa realiza una serie de comprobaciones técnicas básicas antes de aplicar medidas disciplinarias, sobre todo cuando el proceso está relacionado con un activo sensible, pero el procedimiento no está formalizado o estandarizado, de forma que no hay una política de seguridad comunicada al personal todavía implementada.

Sin embargo, Industrias Vaine no ha implementado ningún procedimiento relacionado específico sobre conductas disciplinarias relacionadas con la seguridad de la información. Este tipo de infracciones es gestionado de forma puntual y eficiente, pero no está vinculada a un marco formal de SGSI.

Por otro lado, Las violaciones de la seguridad de la información provocan consecuencias correctamente por las obligaciones contractuales de la empresa, pero no hay implementado todavía un procedimiento formalizado por un marco ISO como exige el SGSI.

Porcentaje de control: 16.66% (NO CUMPLE)

Control A.06.06 – Acuerdos de confidencialidad o no revelación

Industrias Vaine usa recurrentemente acuerdos de confidencialidad para todo el personas y partes interesadas debido a la naturaleza sensible de la información que se trata, pero no existe un modelo estandarizado alineado con las especificaciones de un SGSI. Es decir, los NDA cumplen la mayoría de los puntos descritos en esta parte del control, pero no están desarrollados con el nivel de formalización que la ISO 27001/2 especifica.

Sin embargo, la empresa garantiza que todos los NDAs se ajusten a la normativa jurisdiccional actual. Dichos acuerdos son redactados por el área jurídica de la empresa, lo que garantiza su validez a nivel jurisdiccional.

Por otro lado, no hay implementado en la empresa un procedimiento formal de revisión periódica que actualice dichos documentos según sus necesidades. Esto limita la capacidad del SGSI para mantener los acuerdos alineados con las necesidades actuales de seguridad.

Porcentaje de control: 50% (CUMPLE PARCIALMENTE)

Control A.06.07 – Teletrabajo

Una vez revisados los puntos que se declaran en esta parte del control, se concluye que, aunque la empresa permite el teletrabajo de forma limitada en puestos no críticos, no existen reglas ni políticas formales de teletrabajo que cubran los requisitos de la ISO 27001/2.

Debido a la gran limitación de los puestos de teletrabajo en la empresa, esta no cuenta con unas políticas oficiales sobre la información que puede manejarse en remoto, los puestos que si están autorizados, las medidas a tomar, etc. Una vez revisados los puntos se concluye que bajo la ISO 27001/2, no hay un marco que cubra las medidas necesarias para el teletrabajo seguro.

Porcentaje de control: 0% (NO CUMPLE)

Control A.06.08 – Notificación de eventos de seguridad de la información

La naturaleza de la empresa fomenta que todo el personal (sobre todo en áreas como ciberseguridad e I+D) reporte actividades anómalas, pero no hay una política formalizada que defina esta obligación, por lo que el conocimiento de como realizar dichas notificaciones o del deber de minimizar el efecto de los incidentes de seguridad de la información no es homogéneo en toda la plantilla.

Por otro lado, la empresa no dispone de un procedimiento formal o de un punto de contacto documentado para notificar incidentes o vulnerabilidades. Estas notificaciones de eventos de seguridad son realizadas de forma informal al equipo técnico necesario sin una regulación por un marco SGSI.

Además, no hay una política formal que identifique los tipos de eventos que deben ser notificados de forma que solamente se notifican los eventos de forma informal. Tampoco se notifican todos los casos previstos por la ISO 27001/2.

No obstante, el equipo técnico sí conoce de manera formal mediante una política estructurada y formal los riesgos tanto legales como técnicos de realizar pruebas por su cuenta, y son conocedores de ello.

Porcentaje de control: 37.5% (NO CUMPLE)

Controles del Dominio Infraestructuras [AI]

Control A.07.01 – Perímetro de seguridad física

Debido a la naturaleza sensible de los activos, Industrias Vaine cuenta con perímetros físicos bien definidos y robustos con control biométrico de accesos o sistemas de alarma, entre otros. Estas medidas proporcionan un nivel elevado de protección para dichos puntos críticos, pero no hay una

definición formalizada bajo el SGSI por la ISO 27001/2 que documenta cada uno de los perímetros correctamente.

Porcentaje de control: 50% (CUMPLE PARCIALMENTE)

Control A.07.03 – Seguridad de oficinas, despachos y recursos

La protección de las oficinas, despachos y recursos es realizada de forma adecuada y correcta, usando mecanismo tanto físicos como tecnológicos para evitar la exposición de actividades y activos sensibles. No obstante, están formalizadas ni documentadas como parte de un SGSI en su totalidad, aunque se conoce el interés de la directiva en realizarlo.

Porcentaje de control: 50% (CUMPLE PARCIALMENTE)

Control A.07.06 – Trabajo en áreas seguras

La empresa aplica controles operativos estrictos en las áreas seguras de la empresa para proteger los activos sensibles, entre ellos accesos restringidos o un control del uso de dispositivos, pero las políticas que formalicen las medidas de seguridad a tomar aún están en proceso de ser formalizadas.

Por otro lado, Industrias Vaine aplica varias de las directrices, como la restricción de la información sobre áreas seguras o la prohibición de ciertos trabajos sensibles sin una supervisión adecuada, pero no hay ni una documentación ni políticas formales que cubran completamente todos los puntos indicados en esta parte del control en especial las revisiones periódicas sobre áreas desocupadas (c). La mayoría de las prácticas se realizan correctamente en su totalidad, pero muchas no cuentan con la estandarización de un SGSI formal.

Porcentaje de control: 50% (CUMPLE PARCIALMENTE)

Control A.07.08 – Emplazamiento y protección de equipos

La protección de equipos y su emplazamiento es realizada correctamente en la empresa. Industrias Vaine limita el acceso físico a los activos sensibles aplicando determinados controles contra amenazas físicas. Tanto la realización de dichos controles, la protección de datos sensibles para reducir el riesgo de la exposición visual no autorizada, como la separación entre instalaciones gestionadas y no gestionadas está correctamente implementada y documentada, pero no en su totalidad como indicaría un marco SGSI bajo la norma ISO 27001/2.

Porcentaje de control: 50% (CUMPLE PARCIALMENTE)

Control A.07.13 – Mantenimiento de los equipos

La empresa aplica un programa de mantenimiento de los equipos controlado y formalizado que abarca todos los puntos planteados en el control, siguiendo estrictamente las especificaciones de los proveedores y realizada únicamente por el personal técnico cualificado y autorizado. Estas prácticas están reguladas correctamente como lo indica el marco SGSI, y son coherentes con la ISO 27001/2, permitiendo cumplir adecuadamente los requisitos del control.

Porcentaje de control: 100% (SÍ CUMPLE)

Controles Dominio Tecnología [AT]

Control A.08.07 – Protección contra el código dañino

Industrias Vaine cuenta con medidas operativas y técnicas correctas y sólidas para protegerse contra el código dañino. Entre otros dispone de antivirus actualizado en los *endpoints* de la empresa, un filtrado en las pasarelas de correo y controles básicos para impedir la instalación de software no autorizado. Es verdad que hay un proceso técnico definido formalmente de gestión de vulnerabilidades y define entornos aislados para actividades críticas, pero todavía faltan algunas políticas formalizadas dentro del SGSI conforme a la ISO 27001/2 que regulen aspectos como la verificación oficial de las fuentes de inteligencia sobre amenazas y la actualización periódica de la concienciación del personal, entre otros.

Porcentaje de control: 50% (CUMPLE PARCIALMENTE)

Control A.08.18 – Uso de programas de utilidad privilegiada

Industrias Vaine controla de forma solida el uso de las herramientas privilegiadas y con ello, los permisos asignados al personal técnico. Entre otros, se realiza una autenticación individual reforzada, limitando el acceso a unas tareas determinadas. Aun así, faltan algunas políticas y procedimientos formales bien definidos en el marco del sistema de gestión de seguridad de la información para documentar correctamente los niveles de autorización, entre otros.

Porcentaje de control: 50% (CUMPLE PARCIALMENTE)

Control A.08.20 – Seguridad de las redes

La empresa cuenta con unos controles muy sólidos para la red, siendo considerada bien protegida a nivel operativo. Hay control de dispositivos, un firewall perimetral muy complejo, filtrado de conexiones y bastionado de equipos de red sensibles, entre muchos otros. Sin embargo, las políticas implementadas son insuficientes como para poder cubrir todos los puntos que se sugieren en esta parte del control (por ejemplo, no hay políticas para regular el aislamiento de subredes durante ataques). Sugiere una gran protección técnica, pero falta una estandarización de los procedimientos y políticas referidos a los controles.

Además, Industrias Vaine usa controles operativos correctos y completos en sus virtualizaciones de red, pero no dispone de un marco formal que regule la seguridad en SDN, SD-WAN para, entre otros, su segmentación lógica.

Porcentaje de control: 50% (CUMPLE PARCIALMENTE)

Control A.08.30 – Externalización del Desarrollo

Industrias Vaine mantiene acuerdos básicos con proveedores externos, sin una política formalizada del SGSI para gestionar de forma completa y solida la cadena de suministro cuando se subcontrata y el desarrollo es externo. Para puntos definidos en este control como os requisitos contractuales de prácticas seguras o evidencias formales de pruebas de seguridad en el desarrollo, no hay una estandarización según la norma ISO 27001/2.

Porcentaje de control: 50% (CUMPLE PARCIALMENTE)

Control A.08.34 – Protección de los sistemas de información durante la auditoría pruebas

La empresa controla bien el acceso a los sistemas de información durante las auditorías, acordando con la directiva claramente el alcance de las pruebas y limitando las actividades que se pueden realizar sobre los sistemas sensibles de la organización. El acceso directo lo ejecuta personal con privilegios cuando no es posible un acceso de solo lectura, y las pruebas que pueden afectar se ejecutan fuera del horario operativo para no afectar a la disponibilidad del personal. Aun cumpliendo con los puntos propuestos en el control de manera práctica, las políticas aún no están plenamente formalizadas, y no definen de manera estándar aspectos como la verificación previa de seguridad de los equipos de auditoría cuando esta es externa, o como se realiza la gestión de copias aisladas.

Porcentaje de control: 50% (CUMPLE PARCIALMENTE)

7. Análisis del SOA

A continuación, se cumplimentan los niveles del documento de aplicabilidad (SoA). Para cada control, se ha definido un plan de implantación con fechas e instrucciones para poder cumplir con cada uno de los objetivos citados en dicho control. Además, se ha indicado el último responsable de que dicho plan de implementación se llevase a cabo.

SoA del Dominio Organizativo [AO]

A.05.04 - Responsabilidades de gestión

1. Redacción y aprobación de las políticas de seguridad de información.
- Fecha: Nov-Dic 2025

2. Formación de roles y responsabilidades de seguridad en la empresa
- Fecha: Dic 2025

3. Aprobación e implantación de mecanismo de comunicación al personal de las políticas, mediante sesiones informativas y entregas de los documentos pertinentes.
- Fecha: Dic 2025

4. Creación e implantación del canal de denuncias anónimas (*whistleblowing*)
- Fecha: Ene - Feb 2026

5. Inicio del plan de formación sobre responsabilidades y del sistema de gestión de la seguridad de la información.
- Fecha: Ene 2026 (será planificado como anual, para mantener la concienciación de la importancia de la seguridad en el personal).

Responsable: Director General y propietario (Bruno Vaine), con apoyo del Responsable de Seguridad de la Información (una vez sea designado como rol, previsto en la implantación del SGSI).

A.05.11 - Devolución de activos

1. Revisión, corrección y formalización del procedimiento de desvinculación.
- Fecha: Dic 2025

2. Creación de un procedimiento formalizado de checklist de devolución de activos mediante una base de datos sólida.
- Fecha: Ene 2026

3. Formalización de procedimiento de eliminación segura de información en dispositivos personales o prestados para mantener segura la información sensible.
- Fecha: Feb 2026

4. Formalización de proceso de revocación inmediata de accesos en procesos de devolución
- Fecha: Mar 2026

Responsable: Responsable de Activos e IT (para garantizar la devolución de activos) y Responsable de RRHH (para la coordinación en la gestión de bajas/ cambios de puesto).

A.05.25 - Evaluación y decisión sobre eventos de seguridad de la información

1. Formalización e Integración de un esquema de categorización de eventos en base a la gravedad y probabilidad del posible incidente.
- Fecha: Q1 2026

2. Formalización del proceso de evaluación inicial de eventos
- Fecha: Q1-2 2026

3. Integración del esquema de categorización de eventos en el sistema de seguridad y herramientas existentes
- Fecha: Q2-3 2026

4. Formalización de plantilla de registro de evaluaciones de eventos
- Fecha: Q3 2026

5. Formación interna a personal sobre el nuevo esquema de categorización de eventos.
- Fecha: Desde Ene 2026 (periódica y obligatoria).

Responsable: Responsable de Seguridad de la Información y Equipo de Ciberseguridad.

A.05.26 - Respuesta a incidentes de seguridad de la información

1. Formalización de un procedimiento de respuesta a incidentes, desde la detección de los eventos de seguridad hasta la erradicación de los incidentes.
- Fecha: Dic 2025

2. Formalización de plantillas para el registro de incidentes y análisis a posteriori.
- Fecha: Ene 2026

3. Formalización del procedimiento de escalado del incidente
- Fecha: Ene 2026

4. Formalización de revisiones anuales periódicas tanto técnicas y prácticas del procedimiento de respuesta a incidentes.
- Fecha: Feb 2026

Responsable: Responsable de Seguridad de la Información y Equipo de Respuesta a Incidentes

A.05.27 - Aprendizaje de los incidentes de seguridad de la información

1. Formalización del procedimiento de creación de conocimiento post-incidentes y del registro que almacene dicho conocimiento.
- Fecha: Dic 2025

2. Integración del aprendizaje en la evaluación de riesgos
- Fecha: Q1 2026 (o una vez se haya formalizado el proceso de evaluación de riesgos correctamente)

3. Formalización del procedimiento de modificación de los controles afectados por los incidentes para reducir la probabilidad de que vuelvan a ocurrir
- Fecha: Q1 2026

4. Uso del conocimiento adquirido post-incidentes como material formativo en sesiones internas en la empresa de forma periódica.
- Fecha: Q1-2 2026

Responsable: Responsable de Seguridad de la Información y Equipo de Respuesta a Incidentes

SoA del Dominio Personas [AP]

A.06.02 - Términos y condiciones de empleo

1. Revisión y registro de carencias de los contratos actuales
- Fecha: Dic 2025

2. Formalizar e integrar un anexo contractual de seguridad donde se definan, entre otros, los roles y responsabilidades asignados.
- Fecha: Q1 2026

3. Formalización de procedimiento de revisión de los contratos y de anexos de seguridad periódica.
- Fecha: Q1-2 2026

Responsable: Departamento de RRHH, en colaboración con el área Jurídica y el Responsable de Seguridad de la Información.

A.06.04 - Proceso Disciplinario

1. Formalización de los procedimientos disciplinarios necesarios de seguridad según políticas de la empresa.
- Fecha: Dic 2025

2. Integración y comunicación de los procesos disciplinarios al personal y partes interesadas relevantes
- Fecha: Q1 2026

Responsable: Departamento de RRHH, en colaboración con el área jurídica y el Responsable de Seguridad de la Información.

A.06.06 - Acuerdos de confidencialidad o no revelación

1. Recopilación y formalización en base a la norma ISO 27001/2 de los NDAs actuales
- Fecha: Q1 2026

2. Actualización progresiva de los NDAs antiguos
- Fecha: Q1-4 2026

3. Revisión anual del formato y de los NDAs
- Fecha: Dec 2026

Responsable: Área Jurídica, con colaboración de RRHH (para la relación con el personal) y con el Departamento de Contratación (para terceros/ subcontratos).

A.06.07 - Teletrabajo

1. Formalización de las políticas relacionadas con el teletrabajo seguro
- Fecha: Q1 2026

2. Definición formal de procedimientos de alta y baja del personal en el teletrabajo.
- Fecha: Q1-2 2026

3. Formación del personal necesario en las especificaciones y requisitos de trabajar por remoto
- Fecha: Q2 2026

Responsable: Responsable de la Seguridad de la Información, Departamento de Recursos Humanos y Departamento de IT.

A.06.08 - Notificación de eventos de seguridad de la información

1. Formalización de un procedimiento de comunicación de notificaciones de seguridad, tanto de su formato como de su proceso de realización.
- Fecha: Dec 2025

2. Creación e integración de un único punto de contacto para la transmisión de notificaciones
- Fecha: Q1 2026

3. Comunicación del punto de contacto de transmisión de notificaciones en el personal, y inclusión del procedimiento formal de comunicación de notificaciones en la formación laboral antes de ejercer el oficio
- Fecha: Q2 2026

Responsable: Responsable de la Seguridad de la Información y los Departamentos de IT, Ciberseguridad y RRHH (para el correcto establecimiento de la comunicación dentro de la empresa).

SoA del Dominio Infraestructura [AI]

A.07.01 - Perímetro de seguridad física

1. Documentación formalizada y estandarizada de los perímetros existentes
- Fecha: Dec 2025

2. Creación y formalización de las políticas necesarias para los perímetros de seguridad e integración de dichas políticas en la empresa.
- Fecha: Q1-2 2026

3. Publicación y comunicación al personal de las nuevas políticas de perímetros de seguridad.
- Fecha: Q3 2026

Responsable: Responsable de Infraestructuras y Responsable de Seguridad de la Información

A.07.03 – Seguridad de oficinas, despachos y recursos

1. Documentación y registro formal de oficinas, despachos y recursos críticos
- Fecha: Q1 2026

2. Creación y formalización de políticas de seguridad relacionadas con la seguridad física de dichos activos
- Fecha: Q2 2026

3. Publicación y comunicación al personal de las nuevas políticas sobre ubicaciones seguras en la empresa. Integración de la política en el aprendizaje previo a la entrada de personal en la empresa.
- Fecha: Q3 2026

Responsable: Responsable de Infraestructuras

A.07.06 – Trabajo en áreas seguras

1. Documentación y registro formal de las áreas seguras de la empresa en la actualidad.
- Fecha: Dec 2025

2. Formalización y estandarización de procedimiento de trabajo seguro en las zonas seguras de la empresa.
- Fecha: Q1 2026

3. Inclusión de revisiones, controles y normas para evitar daños e interferencias en las áreas seguras de la empresa.
- Fecha: Q2 2026

4. Publicación y comunicación al personal de las nuevas políticas sobre áreas seguras en la empresa. Integración de la política en el aprendizaje previo a la entrada de personal en la empresa.
- Fecha: Q3 2026

Responsable: Responsable de Infraestructuras y Responsable de Seguridad de la Información

A.07.08 – Emplazamiento y protección de equipos

1. Auditoría y registro del estado actual de los equipos y de los peligros ambientales actuales.
- Fecha: Dec 2025

2. Documentación formalizada de directrices para reducir los riesgos y amenazas provocados por las amenazas ambientales y accesos no restringidos, entre otros.
- Fecha: Q1 2026

3. Implementación en la empresa de los ajustes necesarios en los procedimientos para asegurar la protección de los equipos
- Fecha: Q2 2026

Responsable: Responsable de Infraestructuras y Responsable de Seguridad de la Información

A.07.13 – Mantenimiento de los equipos

1. Formalización del plan de mantenimiento periódico de los equipos ya existente
- Fecha: Dec 2025

2. Creación de un registro de los errores y problemas encontrados durante el mantenimiento.
- Fecha: Q1 2026

Responsable: Departamento de IT.

SoA del Dominio Tecnología [AT]

A.08.07 – Protección contra el código dañino

1. Creación y formalización de políticas contra el malware
- Fecha: Q1 2026

2. Integración de las políticas en las herramientas y software de la empresa
- Fecha: Q2 2026

3. Establecer un procedimiento formalizado de revisión periódica de las políticas para ajustarlas si fuese necesario
- Fecha: Q2 2026

4. Publicación y comunicación de las políticas al personal de la empresa. Propuesta de sesiones informativas periódicas para la concienciación contra el malware del personal.
- Fecha: Q3 2026

Responsable: Responsable de Sistemas de Información

A.08.18 – Uso de programas de utilidad privilegiada

1. Formalización de una documentación sobre todas las utilidades privilegiadas de la empresa y de los niveles de autorización permitidos en cada una de ellas.
- Fecha: Dec 2025

2. Formalización del procedimiento de otorgación de permisos y privilegios para el uso de dichas utilidades acompañado de un control estricto.
- Fecha: Q1 2026

3. Publicación y publicación de la política al personal. Integración de la política en las sesiones de aprendizaje previas a la entrada del personal en la organización.
- Fecha: Q2 2026

Responsable: Responsable de Sistemas de Información.

A.08.20 – Seguridad de las redes

1. Formalización de todos los documentos de configuraciones y topologías de red en la empresa.
- Fecha: Q1-2 2026

2. Creación y formalización de todas las políticas relacionadas con la seguridad de las redes en la empresa.
- Fecha: Q1-3 2026

3. Creación de los procedimientos necesarios para poder garantizar la protección de la red en caso de ataque.
- Fecha: Q3 2026

4. Publicación y comunicación de todas las políticas, documentos y procedimientos al personal. Inclusión de ellos en el proceso de aprendizaje previo a la entrada del personal en la empresa.
- Fecha: Q4 2026

Responsable: Departamento de Redes en coordinación con el Responsable de Sistemas de la Información.

A.08.30 – Externalización del desarrollo

1. Formalización de las políticas de seguridad necesarias para el desarrollo de sistemas subcontratados.
- Fecha: Dic 2025

2. Creación de plantillas estandarizadas que incluyan pruebas, modelos de amenazas, evidencias de seguridad, etc. para asegurar el correcto desarrollo.
- Fecha: Q1 2026

3. Establecer un procedimiento formal de auditorías a los entregables proporcionados durante el desarrollo y a los proveedores subcontratados de forma periódica.
- Fecha: Q1-2 2026

Responsable: Responsable de Sistemas de Información y Departamento de RRHH

A.08.34 – Protección de sistemas durante auditorías y pruebas

1. Creación y formalización de un procedimiento de auditorías técnicas de forma bien detallada.
- Fecha: Q1 2026

2. Creación de políticas formalizadas que definan las condiciones de horarios, registros, copias aisladas, etc.
- Fecha: Q1 2026

3. Publicación y comunicación al personal de las nuevas políticas de auditorías de la empresa. Integración de este conocimiento al aprendizaje realizado por el personal antes de la entrada a la empresa.
- Fecha: Q2 2026

Responsable: Responsable de Sistemas de Información.

8. Conclusiones

El nivel de madurez que presenta Industrias Vaine es parcialmente insuficiente: A nivel técnico e infraestructural, presenta controles y defensas muy sólidos, pero no son aplicados con una formalización y estandarización adecuada en la mayoría de los casos. No hay en la mayoría de los casos un procedimiento, política o documentación que establezca como se debe de actuar o defina la política de la empresa ante un hecho.

Pese a ello, afortunadamente la directiva de Industrias Vaine muestra una intención clara de certificarse en la ISO 27001/2, por lo que si se sigue el SOA propuesto y se realiza en los plazos propuestos, la organización contaría con una base muy buena para poder implementar un sistema de gestión de la seguridad de la información con un nivel de madurez y apto para su posterior certificación.

9. Bibliografía

"Norma ISO 27001" - https://www.normaiso27001.es/

"Manual de eMarisma" - https://es.scribd.com/document/651489180/Manual-Emarisma-v2022ç