UNIVERSITAT POLITÈCNICA DE VALÈNCIA

DISCA
DEPARTAMENTO DE INFORMÁTICA DE SISTEMAS Y COMPUTADORES

TRABAJO DE FIN DE MÁSTER

MÁSTER UNIVERSITARIO EN INGENIERÍA DE COMPUTADORES

"Definición de una metodología ligera para la evaluación, implantación y gestión de la seguridad en sistemas informáticos"

Alumno: D. Francisco Mateu Sánchez

Directores: Dr. D. David De Andrés Martínez, Dr. D. Joaquín Gracia Morán

Valencia, Septiembre 2014

Agradecimientos

En primer lugar, quiero agradecer el apoyo y la paciencia a mis directores por ayudarme a buscar y a entender las preguntas y las respuestas.

Quiero también dar las gracias a los miembros de la empresa SCASSI Conseil, y especialmente a su CEO Laurent Pelud y a Laetitia Maynard Responsable de Marketing, por una gran acogida en su empresa donde he encontrado la orientación y las correcciones que necesitaba en el momento adecuado.

Y a mi familia por compartir las horas de esfuerzo.

Índice

Índice de tablas

Índice de figuras

1 Introducción

1.1 Sumario

Se presenta una metodología ligera y práctica, para evaluar los riesgos y el estado de protección de las pymes en el mercado español que permita definir y alcanzar el nivel adecuado de seguridad a cada organización.

1.2 Resumen

El propósito de este trabajo es crear un método práctico y útil para mejorar el nivel de seguridad en los sistemas informáticos y de sus datos en organizaciones y empresas dentro de un contexto particular como es el mercado español.

Se pretende reducir la distancia entre la realidad actual de las amenazas informáticas en las empresas y su nivel de seguridad.

Para ello se ha evaluado cómo es el entorno empresarial español y cuál es el nivel de preparación y protección de sus sistemas informáticos frente a las amenazas y riesgos actuales. Con ello se ha pretendido definir cuáles son las necesidades particulares de estas organizaciones.

Se ha realizado un estudio de las normas y estándares que permitan crear esta metodología dentro de un marco legal y de buenas prácticas aceptado universalmente. También se ha estudiado la existencia de guías y metodologías que pudieran dar solución al problema planteado.

Al no encontrar ninguna solución, se ha definido una metodología compuesta por varios métodos presentados en fases que permitan evaluar, corregir y mejorar los sistemas de seguridad de la información.

Las fases de la metodología son análisis, evaluación, presentación de resultados y propuesta de mejora. Para cada una de ellas se han estudiado las normas y estándares aplicables y se ha elegido el más adecuado adaptándolo a las particularidades del entorno y al proceso general de la metodología.

En la fase inicial de análisis se presentan unos cuestionarios que pretenden evaluar los riesgos y el estado de protección de la organización así como los niveles actual y adecuado de protección. En la segunda fase se presentan unos cuestionarios reducidos y parametrizados con los resultados de la fase anterior que evaluarán la seguridad de los sistemas de una forma más práctica. Los resultados de esta fase se evaluarán mediante una serie de fórmulas y plantillas definidas. En la fase 3 se presentarán los resultados obtenidos en dos tipos de informe, uno más técnico orientado a la corrección y mejora, y otro en forma de sumario orientado a concienciar a los órganos directivos del estado de su organización. En la cuarta fase se presenta una hoja de ruta con los objetivos a cumplir así como una serie de herramientas y soluciones previamente catalogadas entre las cuales se escogen las aplicables a la organización estudiadas.

Este trabajo está enfocado y limitado al mercado español y a las empresas pyme por sus características y situación actual.

1.3 Conceptos previos

Para la elaboración de este punto se han tomado como referencia las fuentes citadas en el apartado 8.1 Conceptos previos.

¿Qué es la seguridad?

Podemos entender la seguridad como una característica propia de cualquier sistema o cosa que nos indica el nivel en que se está libre de riesgo, peligro o amenaza.

Dado que la seguridad depende tanto de los factores externos como internos a un sistema, hablaremos de fiabilidad como el nivel de preparación de un sistema para soportar amenazas, daños o riesgos.

¿Cómo mantener un sistema seguro?

Hay tres aspectos que definen si un sistema es seguro y son confidencialidad, integridad y disponibilidad.

La confidencialidad nos indica que los objetos de un sistema son accesibles únicamente para los elementos autorizados a ello y que estos no pueden a su vez publicarlos a elementos no autorizados.

La integridad significa que los objetos solo serán modificados por elementos autorizados y de una forma controlada.

La disponibilidad indica que los objetos son accesibles a los elementos autorizados.

Para mantener un sistema seguro debemos mantener estos tres aspectos en el nivel adecuado a nuestra organización.

¿Qué debemos proteger?

El objetivo es proteger activos de las empresas que puedan ser especialmente valiosos para su funcionamiento.

En la actualidad los sistemas informáticos constituyen unos bienes preciados en sí mismos además de formar parte de todos los procesos internos de las organizaciones. Es por esto que las amenazas propias de este sistema se extienden a la totalidad de la empresa.

Dentro de los sistemas informáticos deberemos proteger los elementos físicos (Hardware) los procesos y aplicaciones (Software) y los datos.

¿De quién tenemos que protegernos?

Las amenazas son muchas y muy variadas y suelen agruparse de diferentes maneras (catástrofes, personas, amenazas lógicas, externas, internas).

Las amenazas han evolucionado con el tiempo y han pasado de ser hechos aislados propios de hackers a una industria especializada presente en todos los medios y con gran cantidad de recursos.

¿Cómo debemos protegernos?

Con la gran evolución de los sistemas informáticos así como de sus amenazas se ha producido una evolución similar de las herramientas y los métodos de protección existiendo un catálogo casi infinito de herramientas, productos, empresas, normativas y estándares.

Es aquí donde empieza a percibirse la dificultad que supone establecer un nivel adecuado de seguridad para las empresas de menos recursos. Estas empresas no disponen de personal especializado ni de la posibilidad de invertir en un gran proyecto externo que les permita escoger las mejores herramientas y métodos para ellos.

2 Planteamiento del problema

2.1 Introducción

2.1.1 Motivación

Durante el tiempo que me ha llevado a definirme como Administrador de Sistemas Informáticos me he encontrado con muchos obstáculos técnicos para los cuales he tenido que aprender, investigar, implantar o desarrollar todo tipo de herramientas, métodos o soluciones técnicas.

Esto me ha llevado a tener una visión concreta, desde mi experiencia, de las necesidades de las organizaciones en las cuales he podido trabajar.

2.1.2 Recorrido personal

Desde niño supe que mi pasión eran la informática y la tecnología.

Realicé un módulo de informática de empresas una vez acabado el bachillerato con la intención de entrar en la universidad con conocimientos más sólidos.

Esto me permitió trabajar de Técnico de Campo durante cuatro años mientras estudiaba una Ingeniería. En este tiempo trabajé en muchos tipos de empresas y organizaciones (fábricas, hospitales, colegios e institutos, Pymes) aprendiendo de trabajadores, directivos o gerentes que lo importante para ellos era el negocio, y que la tecnología era una herramienta que debía producir sinergias con su negocio pero que en muchas ocasiones los lastraba con costes elevados de donde no se veían beneficios claros.

Al acabar la carrera trabajé dos años en un organismo público dentro de un proyecto de implantación de metodología ITIL para la implantación y optimización del proceso de atención a 600 usuarios consiguiendo una reducción del 90% de incidencias.

Posteriormente cambié a una Consultora de Sistemas, filial de una Factoría de Software, donde durante 4 años formé parte y en algunas ocasiones lideré diferentes proyectos como el montaje e instalación de infraestructuras (racks, servidores, cabinas, redes), sistemas operativos, bases de datos, servidores de aplicaciones (Red Hat, Windows, Oracle, OAS, Tomcat, etc.), consolidación de centros de datos a entornos virtuales, mantenimiento y outsourcing de los sistemas en todas las empresas clientes del grupo.

En esta empresa tuve que realizar proyectos de implantación y/o auditoría de seguridad para lo cual tuve que aprender de forma autónoma tanto normas, métodos, mejores prácticas o tecnologías aplicables.

Actualmente he acabado el Máster en Ingeniería y Computadores a falta de TFM (del cual este informe forma parte) y trabajo en la Universidad Internacional Valenciana como Administrador de Sistemas y Seguridad donde he diseñado, establecido y mantengo tanto la infraestructura tecnológica de 4 sedes como la plataforma de aplicaciones online compuesta de 36 servidores virtuales sobre hipervisores VMware con tecnologías Red Hat, Tomcat y Oracle.

2.1.3 Habilidades y herramientas

Viendo mi recorrido profesional en perspectiva, he entendido que lo que me ha hecho avanzar ha sido el adquirir las habilidades necesarias para resolver las necesidades de las empresas.

Para esto he aprendido a utilizar las herramientas que iba necesitando apoyándome en la formación y en lo que me aportaba el mercado o la comunidad.

En todas las empresas con las que he trabajado han tenido necesidades de seguridad pero no he encontrado nunca una solución que les sirviera a nivel global y que fuera atractiva para estas.

Siempre he encontrado rechazo a los proyectos de seguridad tanto por la dirección como por usuarios o administradores y las razones que se repetían eran costes elevados, elevados tiempos de implantación y gestión, poca experiencia en seguridad, complejidad, ROI difícil de percibir o calcular, falta de una regulación clara entre otras.

Para seguir avanzando en mi desarrollo profesional he sentido la necesidad de adquirir la capacidad de dar a las empresas un método para implantar y gestionar la seguridad de forma sencilla, ligera y a bajo coste.

2.2 Objetivos

El objetivo principal es proporcionar a las empresas y organizaciones un método fiable y robusto con el cual mantener sus sistemas seguros y que les permita ser conscientes del nivel de protección.

Para ello se deberán superar las barreras a la adopción dotando de las herramientas necesarias para evaluar tanto en detalle como en conjunto los sistemas de seguridad. Esto permitirá concienciar tanto a la dirección como a los diferentes actores.

El sistema deberá ser ligero pero tendrá que poder evaluar dentro del modelo las tecnologías ya implantadas así como las posibilidades que ofrece el mercado o la comunidad. También deberá evaluarse las interrelaciones entre ellas para evitar gastos innecesarios y conseguir optimizar la inversión.

Esta metodología pretende ser un nexo de unión entre las definiciones teóricas y otras más prácticas, suprimiendo las deficiencias y carencias de los diferentes modelos.

Una solución global debería ajustarse a normas y estándares como ISO 27001 debiendo abarcar la cobertura de la norma.

Utilidad, debería plasmar el marco de la normativa mediante una formalización y una estructuración de las reglas de seguridad alineado a los procesos de negocio.

Práctica/Pragmática, debería incluir soluciones concretas para la implantación de los proyectos de seguridad de una empresa.

Se pretende dotar a las empresas de un medio para auditar y formalizar los procesos de securización que permita implantar y controlar diferentes soluciones prácticas. Esta incluirá

métodos de control, análisis periódicos de los cambios, nuevas necesidades y corrección de los métodos implantados sin olvidar el testeo y análisis práctico de la robustez de los sistemas.

2.3 Cómo abordar el problema

En primer lugar será necesario adquirir los conocimientos de base necesarios para entender correctamente el problema. Para ello se realizará un proceso de investigación de seguridad informática orientada a empresas.

En segundo lugar será necesario comprobar si el problema ya ha sido planteado y si existe algún tipo de solución.

Se ha realizado un trabajo de investigación de las normativas, metodologías y proyectos de securización más extendidas y aceptadas por la comunidad o el mercado.

Se construirá una metodología práctica que recoja las diferentes soluciones y proyectos de seguridad ordenados dentro de una definición estructurada que permita, de forma sencilla controlar, evaluar o priorizar los diferentes proyectos.

Sobre una base sólida como es la definición de SANS de los 20 controles de seguridad críticos, se establecerá una metodología que sirva como referencia para implementar sistemas de seguridad en entornos informáticos.

Se separará de forma modular los diferentes contextos prácticos de aplicación a partir de la definición de puntos críticos de control de SANS.

Esta solución práctica deberá cumplir lo especificado en la normativa ISO 27001.

SANS ordena los puntos de control por prioridad en la mitigación de ataques.

Se desarrollará unas plantillas que recojan en cada uno de los puntos de control una tabla de métodos de cómo implementarlo.

En cada uno de los métodos se evaluarán las diferentes soluciones que ofrece el mercado y se definirán una serie de pesos (tiempo de implantación, calidad, precio, coste de administración…) que permitirán establecer métricas.

Estos métodos se presentarán ordenados en las plantillas por la ganancia adquirida.

Con esto se pretende obtener una metodología ligera y modular que sirva como herramienta para definir y evaluar la seguridad en las organizaciones tanto en las fases de diseño o implementación como en las fases de mantenimiento.

La definición de parámetros como inversión o tiempo permitirá a su vez obtener el nivel de seguridad alcanzado pudiendo minimizar los costes sin penalizar la seguridad del sistema.

El carácter modular de esta solución permite añadir cualquier solución nueva, ajustar las calidades, evolucionar el modelo en el tiempo o ajustarlo a nuevas necesidades.

La jerarquización y priorización de los controles y soluciones aporta una etapa inicial de implantación marcada por una ganancia rápida a un coste muy reducido. Esto supone un valor añadido a la hora de conseguir la implicación y concienciación de los órganos directivos y reducir las barreras tradicionales.

2.4 Justificación. Estudio del entorno

2.4.1 Introducción

En el mercado español y valenciano hay poca demanda de sistemas de seguridad informática. Pocas empresas se dedican exclusivamente a este sector. La poca demanda la cubren asesorías jurídicas y consultoras generalistas.

Mi pregunta: ¿Por qué?

Para justificar el planteamiento del problema se ha realizado un estudio del contexto empresarial español. Se han escogido gráficos y tablas del *Estudio sobre seguridad de la información y continuidad de negocio en las pymes española,* Inteco (2012) *[2],* porque representa con exactitud el ámbito de estudio del problema.

2.4.2 Presentación de datos e interpretación

Población sobre la que se ha realizado el estudio.

Tabla 1: Universo del estudio

Número de empleados	Total empresas[7]	Total empresas con conexión a Internet[8]	%
Microempresas *(menos de 10 empleados)*	3.094.721	1.983.716	93,1%
Pequeñas empresas *(10-49 empleados)*	130.994	127.064	6,0%
Medianas empresas *(50-249 empleados)*	19.864	19.745	0,9%
Total	**3.245.579**	**2.130.525**	**100%**
Sector de actividad	**Total empresas**	**Total empresas con conexión a Internet**	**%**
Industria y construcción	706.643	s/d[9]	21,8%
Comercio y hostelería	1.068.649	s/d	32,9%
Transporte	216.802	s/d	6,7%
Nuevas Tecnologías	60.032	s/d	1,8%
Servicios empresariales	739.664	s/d	22,8%
Otros servicios	453.789	s/d	14,0%
Total	**3.245.579**	**2.130.525**	**100%**
Zona geográfica[10]	**Total empresas**	**Total empresas con conexión a Internet**	**%**
Zona Sur	631.586	s/d	19,5%
Zona Centro	452.184	s/d	13,9%
Cataluña	600.698	s/d	18,5%
Zona Este	526.669	s/d	16,2%
Zona Norte	534.352	s/d	16,5%
Comunidad de Madrid	500.090	s/d	15,4%
Total	**3.245.579**	**2.130.525**	**100%**

Fuente: Directorio Central de Empresas. Instituto Nacional de Estadística (INE). 2011

Tabla 1. Universo del estudio. Fuente: Inteco, (2012, p. 16).

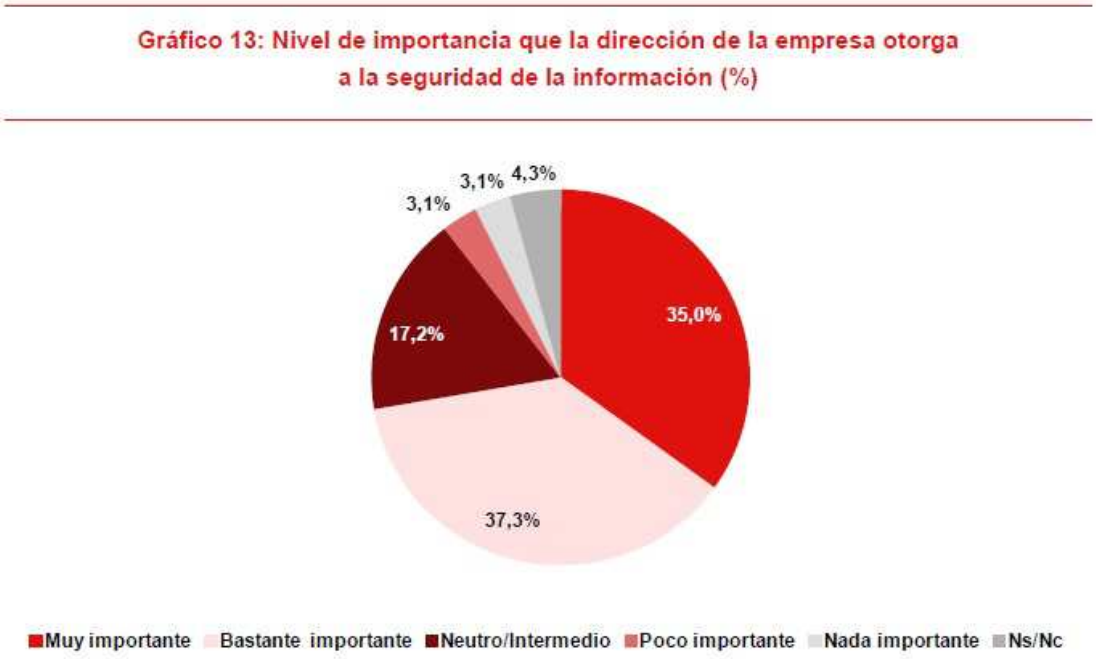


Figura 1. Nivel de importancia otorgado a la seguridad. Fuente: Inteco, (2012, p. 37).

Las empresas sobre las que se ha realizado el estudio afirman ser conscientes del alto nivel de importancia que tiene la seguridad de la información para sus organizaciones. 72.3%

Figura 2. Reconocimiento de incidentes de seguridad. Fuente: Inteco, (2012, p. 68).

A pesar del dato anterior, un 26,1% de las empresas afirman haber sufrido incidentes de seguridad.

Gráfico 46: Incidentes de seguridad declarados que hayan impactado en la continuidad de los procesos u operaciones de negocio (%)

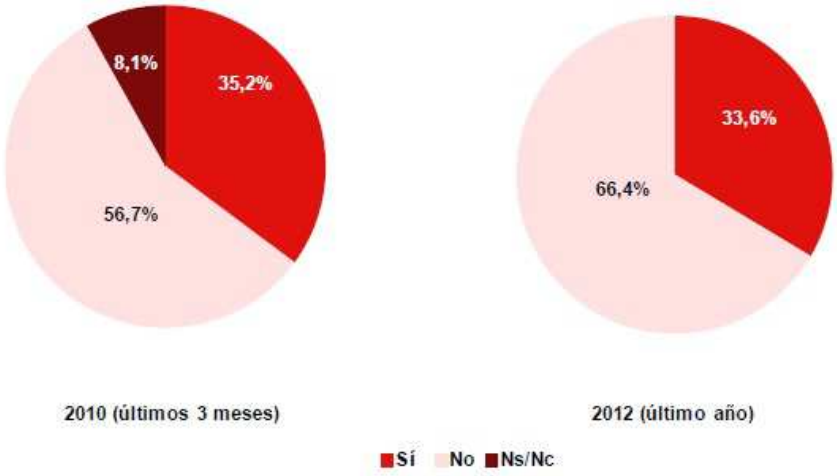


Figura 3. Incidentes de seguridad y continuidad de negocio. Fuente: Inteco, (2012, p. 73).

Los incidentes que tienen impacto en la continuidad de negocio superan el 30%. Cabe destacar que es importante el porcentaje de empresas que ni siquiera son conscientes de la afectación de los incidentes a su negocio.

Tabla 9: Consecuencias que tuvo el incidente (%)

Consecuencias	Incidentes que afectan a la continuidad del negocio				
	Falta de servicio/ suministro por el proveedor	Caída de sistemas/ aplicaciones informát.	Fallo/ avería del sistema de soporte	Daño físico en equipos	Ataques informát.
Retrasos / horas perdidas / impacto en la productividad	83,9	81,8	73,4	70,2	52,7
Económico (coste directo)	14,6	21,3	21,1	46,3	10,4
Daño a la imagen de la empresa (impactos reputaciones)	2,0	6,2	4,4	4,9	2,1
Pérdida de clientes con los que existiera un contrato en firme (impacto contractual)	0,1	7,2	3,4	0,4	0,4
Sanciones / multas (impacto legal)	0,4	4,0	-	-	-
Otra consecuencia	0,3	0,1	0,1	-	4,3
Ningún impacto	9,8	7,5	10,6	10,0	36,7
No sabe/ No contesta	2,3	0,9	0,6	0,1	-

Tabla 2. Consecuencias de incidentes de seguridad. Fuente: Inteco, (2012, p. 77).

Los incidentes de seguridad se ven reflejados en un alto porcentaje en costes económicos, principalmente por pérdida de productividad o parada de la actividad empresarial.

A su vez, el porcentaje de ocasiones en que el incidente no tuvo impacto o consecuencias es mínimo.

Gráfico 32: Posición afirmada por la empresa para afrontar una situación de crisis, desastre o contingencia (%)

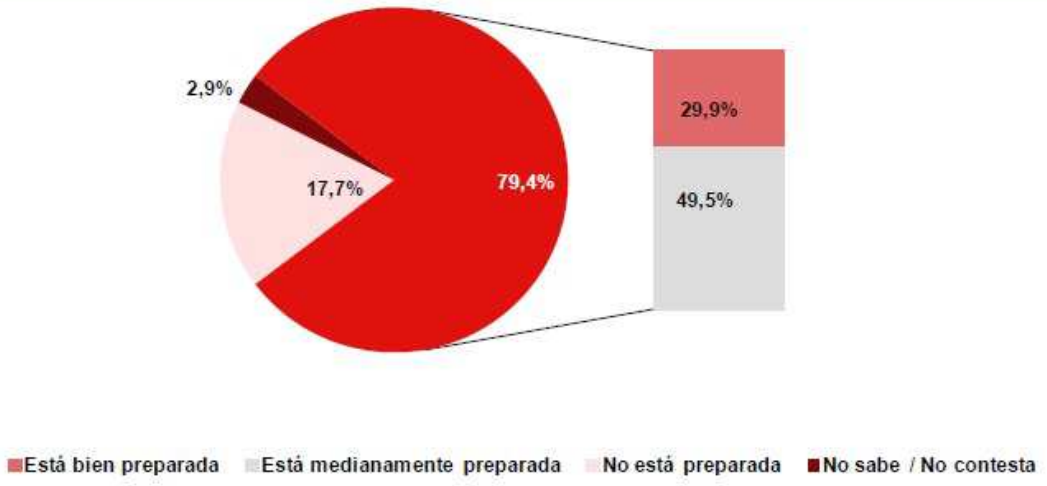


Figura 4. Posicionamiento de las empresas. Fuente: Inteco, (2012, p. 58).

Las empresas piensan en un alto porcentaje 79,4% que están protegidas ante incidentes de seguridad.

Gráfico 31: Razón por la que no se ha previsto una estrategia o procedimiento ante situaciones de crisis o desastre (%)

Figura 5. Razones para la ausencia de estrategias. Fuente: Inteco, (2012, p. 57).

En un porcentaje que está en desacuerdo con los datos de incidentes, las empresas afirman que la probabilidad de verse afectadas es muy baja.

Las otras razones para no establecer métodos de defensa son la falta de personal y tiempo así como el coste excesivo.

Tabla 4: Motivos señalados por las empresas para no utilizar las herramientas y soluciones de seguridad (%)

Soluciones	% empresas que no utilizan en la actualidad	Motivos						
		No conoce	No necesita	Precio	Ineficaces	Entorpecen	Otros	No contesta
Antivirus / Antiespia	3,9	2,3	**39,6**	0,4	5,1	17,4	14,9	20,3
Cortafuegos	24,6	**35,6**	27,2	3,2	0,8	2,8	0,2	30,2
Antispam	24,7	28,0	**38,8**	0,1	0,8	3,8	0,2	28,3
Plugins	48,6	**37,0**	28,4	0,5	0,5	2,0	0,4	31,2
Bloqueo de ventanas emergentes	28,5	**33,3**	29,7	0,0	0,9	2,9	0,2	33,0
Sistemas de control de intrusión	47,1	**38,0**	26,0	1,4	0,4	2,1	0,2	31,9
Cifrado de datos	65,9	35,1	**35,2**	0,4	0,5	1,6	0,8	26,4
Eliminación de archivos temporales y cookies	32,6	29,1	**32,5**	0,7	1,1	3,1	1,5	32,0

Base: pymes que no utilizan las herramientas y soluciones de seguridad *Fuente: INTECO*

Tabla 3. Motivos para la ausencia de herramientas. Fuente: Inteco, (2012, p. 28).

Las empresas afirman mayoritariamente que la razón principal para no adoptar medidas básicas de seguridad es no necesitarlas o no conocerlas.

Gráfico 49: Reacción adoptada tras los incidentes de seguridad (%)

Figura 6. Reacciones tras incidentes de seguridad. Fuente: Inteco, (2012, p. 78).

En un porcentaje superior al 50% las empresas afirman no tomar ninguna medida correctiva tras un incidente de seguridad.

Tabla 3: Disponibilidad de herramientas para proteger equipos y sistemas según tamaño de las empresas (%)

Soluciones	Microempresa	Pequeña empresa	Mediana empresa
Antivirus/Antiespía	96,1	97,6	98,2
Cortafuegos	74,9	82,6	90,4
Antispam	74,9	80,6	93,6
Bloqueo de ventanas emergentes, banners publicitarios	71,4	72,7	80,2
Eliminación de archivos temporales y cookies	67,2	69,3	73,9
Sistemas de control de intrusión	52,5	56,8	66,7
Plugins o complementos de seguridad para el navegador	51,0	57,1	65,3
Cifrado de datos	33,4	45,7	54,5

Tabla 4. Disponibilidad de herramientas. Fuente: Inteco, (2012, p. 27).

Se utilizan mayoritariamente herramientas básicas de protección de equipos.

Tabla 6: Principales incidentes de seguridad declarados por las pymes según tamaño (%)

	Microempresa	Pequeña empresa	Mediana empresa
Malware (virus, troyanos, etc.)	14,4	17,5	25,9
E-mails masivos publicitarios (spam)	11,9	11,9	21,6
Fallos técnicos	4,0	8,4	10,6
Daño físico en equipos/programas	2,1	2,8	10,4
Sustracción/extravío de dispositivos	0,9	0,5	6,1

Tabla 5. Principales incidentes declarados. Fuente: Inteco, (2012, p. 70).

La detección de incidentes está relacionada con el tipo de herramientas empleadas.

Gráfico 27: Empresas que declaran estar certificadas en ISO 27001 sobre Sistemas de Gestión de la Seguridad de la Información o SGSI (%)

Figura 7. Certificaciones ISO 27001. Fuente: Inteco, (2012, p. 52).

La adaptación del estándar de seguridad es muy baja en empresas de este tipo.

2.4.3 Conclusiones

Estas conclusiones se han extraído de *Estudio sobre seguridad de la información y continuidad de negocio en las pymes española,* Inteco (2012) *[2],* y de opiniones aportadas por profesionales, consultados principalmente en la estancia en prácticas en SCASSI Conseil.

Las empresas españolas tienen un nivel muy bajo de seguridad aunque su percepción es la contraria.

Existe una baja concienciación acerca de las amenazas y las consecuencias que los incidentes pueden provocar en los negocios.

El mercado español es poco maduro en términos de demanda de soluciones de seguridad informática por lo que no se crean soluciones específicas. La demanda del mercado se cubre con soluciones básicas o genéricas así como por consultoras generalistas o jurídicas que han ampliado su oferta a este sector.

¿Qué piensan las empresas?

Seguridad = Coste + Complejidad

La implantación de herramientas y procedimientos de seguridad en los procesos productivos de las empresas implica un esfuerzo para sus empleados sobre todo cuando su formación o nivel de concienciación son bajos.

Coste = Menor beneficio

El coste de implantación de soluciones generalistas suele ser muy alto tanto en tiempo como en dinero. Estas soluciones suelen ir acompañadas con la contratación de personal especialista o la contratación de servicios externos para el mantenimiento.

Complejidad = Menor productividad

Los órganos directivos ven la seguridad como un aumento de la complejidad en sus procesos que en muchas ocasiones ralentizará y dificultará su negocio. Esto va unido a una visión poco clara de los beneficios que aporta.

Estrategia = Mínima Seguridad

De los datos aportados por el estudio estadístico de Inteco, *Estudio sobre seguridad de la información y continuidad de negocio en las pymes española,* Inteco (2012) [2], la estrategia elegida mayoritariamente por las pymes españolas es escoger herramientas básicas de protección de equipos y redes (antivirus y firewalls). Esto les permite minimizar la ecuación presentada anteriormente reduciendo así la seguridad.

Existe una baja adopción de normativas y estándares como ISO27001. Esto es debido a que se perciben como soluciones generalistas de alto coste. Estas normas pretenden ser válidas para la totalidad de situaciones y amenazas que puedan presentarse en los sistemas de información pero son difíciles de implementar para pequeñas empresas ya que gran parte de lo que se presenta en ellas no es de aplicación. Esto se ve potenciado por la gran variedad de pymes así como de sus necesidades específicas.

Según diferentes profesionales consultados en empresas, organismos públicos y consultoras, la baja demanda percibida es el motivo para que no exista una oferta específica de soluciones. En términos utilizados por estos profesionales, el mercado español es poco maduro para este tipo de soluciones de seguridad.

2.4.4 Planteamiento del problema.

El mercado español está formado mayoritariamente por pymes. El nivel de seguridad de los sistemas informáticos de estas pymes es bajo aunque la visión de estas empresas es que poseen un nivel alto de protección o que no lo necesitan. La falta de seguridad es causa del desconocimiento y falta de concienciación. Las principales barreras para la adopción de mejores soluciones son el coste y la complejidad.

Para solucionar este problema es necesario:

•Analizar qué necesitan las empresas españolas

•Poder evaluar las necesidades concretas de una empresa

•Dar una solución adaptada a cada organización

•Cambiar la perspectiva de las empresas de que la seguridad solo es una respuesta a las amenazas demostrándoles que implica un valor competitivo

3 Estado de la cuestión y fundamentación teórica

3.1 Antecedentes

3.1.1 Proceso de investigación

Para la elaboración de este punto se han tomado como referencia las fuentes citadas en el apartado 8.2 Bases de investigación.

Este punto se ha basado en la búsqueda y lectura de bibliografía de base. En esta parte se ha pretendido adquirir los conocimientos necesarios para poder orientar y definir correctamente el trabajo.

El primer problema encontrado al realizar una investigación sobre seguridad informática es la gran cantidad de artículos de muy diversa temática dedicados a la seguridad.

- Artículos académicos

Investigaciones orientadas mayoritariamente a temas muy específicos. Los artículos académicos que se han encontrado sobre seguridad tratan sobre mejoras particulares o investigaciones en líneas muy concretas. Al buscar investigaciones generales he podido encontrar algunos pocos artículos referidos a están estándares o partes de ellos pero no he podido encontrar una línea de investigación que se refiriera a líneas de investigación sobre soluciones generales.

- Tesis, TFM y TFG

Investigaciones concretas, trabajos generalistas o implantación de soluciones. Los trabajos académicos sobre seguridad que he leído trataban en la mayoría de casos de la seguridad en sentido amplio y teórico. Aquellos trabajos que tenían una orientación práctica lo hacían sobre proyectos de implantación de soluciones a diferentes entornos. En el caso concreto de las Tesis el caso era el similar al punto anterior donde las investigaciones eran sobre temas muy específicos.

- Artículos y soluciones empresariales

Generalistas con foco en sus productos. Los artículos, guías y trabajos obtenidos de empresas líderes en el campo de la seguridad informática suelen comenzar a tratar la seguridad de forma generalista para, rápidamente poner foco en su herramienta y la solución que aporta. Suelen contar las bondades de los productos, muchas veces en oposición a los de la competencia y siempre están orientados a vender el miedo a los posibles daños que pueden producir las amenazas a nuestro negocio.

- Estándares

Evolución y especialización de los estándares. Marco teórico, aplicación práctica en desarrollo. He encontrado en los diferentes estándares de seguridad una mayor línea de trabajo. He entendido que los diferentes estándares han ido creándose y evolucionando junto con la tecnología y el entorno. Pretenden ser soluciones de amplio espectro que cubran la totalidad

del campo a que hacen referencia. Suelen crearse partiendo de bases teóricas siendo marcos de actuación o reglamentarios en donde adaptar cada caso particular.

Estos estándares, agrupados en familias desarrollan normas o recomendaciones prácticas pero lo hacen de forma ambigua y generalista sin llegar al detalle práctico.

- Guías, organizaciones y comunidad

Comunidades de especialistas. Gran cantidad de publicaciones y estudios. Orientado a profesionales o técnicos. Existen gran cantidad de guías y publicaciones con recomendaciones de seguridad. Desde mi punto de vista, la mayoría reflejan objetivos concretos de sus creadores y dejan de lado las necesidades de los destinatarios de estas guías. En algunos casos, como las guías y normativas generadas por organismos oficiales como Inteco en España o ANSSI en Francia, suelen tener un carácter mayor de servicio por lo que sí que se encuentra una intención de cubrir necesidades.

- Normativas legales

Las normativas legales investigadas son marcos jurídicos que pretenden arbitrar en problemas concretos de la sociedad. Leyes como la LOPD sirven para proteger a los ciudadanos en el uso de sus derechos pero están muy alejadas del tema de estudio de este trabajo. Cabe destacar que las normativas tienen un marcado carácter geográfico y son muy distintas en diferentes países. Estas leyes suelen ser antiguas y poco adaptables a necesidades y al contexto.

3.1.2 Estancia en prácticas

Durante el proceso de investigación entendí que era necesario conocer el punto de vista de las empresas que se dedicaban a implantar soluciones de seguridad en las empresas.

Primero investigué que tipos de empresas estaban cubriendo ese mercado específico en el entorno geográfico de Valencia y España y observé que mayoritariamente era cubierto por consultoras de ámbito generalista o asesorías jurídicas con departamentos especializados.

Con el objetivo de conocer de primera mano las opiniones y experiencias de una empresa especializada en seguridad informática así como su visión en otros mercados solicité una estancia en prácticas en la empresa SCASSI Conseil con sede en Toulouse.

Al presentar el trabajo realizado hasta ese momento se me aportó y corrigió principalmente dos líneas de trabajo:

- Las barreras de adopción de las empresas a los proyectos de seguridad son particulares de los mercados y están delimitados geográficamente. Una solución generalista deberá estar orientada a un mercado objetivo y solucionar sus problemas particulares.
- La fase de análisis del contexto y las amenazas supone un punto necesario y aporta una gran reducción del volumen de los proyectos.

3.2 Marco teórico

3.2.1 INTECO

3.2.1.1 Descripción

"El Instituto Nacional de Tecnologías de la Comunicación, S.A., (INTECO), sociedad dependiente del Ministerio de Industria, Energía y Turismo (MINETUR) a través de la Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información (SETSI), es la entidad de referencia para el desarrollo de la ciberseguridad y de la confianza digital de ciudadanos, red académica y de investigación española (RedIRIS) y empresas, especialmente para sectores estratégicos.

Como centro de excelencia, INTECO es un instrumento del Gobierno para desarrollar la ciberseguridad como motor de transformación social y oportunidad para la innovación. Para ello, con una actividad basada en la investigación, la prestación de servicios y la coordinación con los agentes con competencias en la materia, INTECO lidera diferentes actuaciones para la ciberseguridad a nivel nacional e internacional.

INTECO, centro de respuesta a incidentes de seguridad TIC, trabaja para aumentar la capacidad de detección y alerta temprana de nuevas amenazas, la respuesta y análisis de incidentes de seguridad de la información, y el diseño de medidas preventivas para atender a las necesidades de la sociedad en general y, en virtud del Convenio de Colaboración suscrito entre la Secretaría de Estado de Seguridad y la Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información, a las necesidades de seguridad de las infraestructuras críticas, en coordinación con el Centro Nacional para la Protección de las Infraestructuras críticas (CNPIC).

La misión de INTECO es por tanto reforzar la ciberseguridad, la confianza y la protección de la privacidad en los servicios de la Sociedad de la Información, aportando valor a ciudadanos, empresas, Administración, red académica y de investigación española, sector de las tecnologías de la información y las comunicaciones y sectores estratégicos en general. (http://www.inteco.es/que_es_inteco/)"

3.2.1.2 Estudio sobre seguridad de la información y continuidad de negocio en las pymes españolas

"El Estudio sobre seguridad de la información y continuidad de negocio en las pymes españolas realiza un diagnóstico de la percepción sobre el nivel de preparación ante los riesgos de seguridad y la adopción de estrategias de continuidad de negocio por parte de las pymes españolas que utilizan Internet como parte de su negocio en 2012.

Para llevar a cabo la investigación, se ha desarrollado una metodología que comprende: encuestas a una muestra representativa de empresas españolas de menos de 250 empleados repartidas por todo el territorio nacional y entrevistas en profundidad a responsables en seguridad de la información de las empresas. Asimismo, Los resultados de la encuesta han sido sometidos a la consideración de un grupo de expertos, cuyas aportaciones han sido esenciales para la comprensión de la situación de la pyme española." *Estudio sobre seguridad de la información y continuidad de negocio en las pymes española,* Inteco (2012) *[2],*

3.2.2 ANSSI

3.2.2.1 Descripción

“La Agencia Nacional de Seguridad de Sistemas de Información (Anssi) es un servicio francés creado por decreto el 7 de julio de 2009. Este servicio nacional se adjunta a la Secretaria General de Defensa y Seguridad Nacional (SGDSN) autoridad responsable de asistir al Primer Ministro en el ejercicio de sus responsabilidades en materia de defensa y seguridad nacional.

La agencia asegura que la misión como una autoridad nacional sobre la seguridad de los sistemas de información. Como tal, es responsable de proponer normas para la protección de los sistemas de información del Estado y verificar la aplicación de las medidas adoptadas.

En el campo de los sistemas de información de defensa, que ofrece un servicio para la vigilancia, detección, alerta y respuesta a los ataques cibernéticos, especialmente en las redes en el estado.

Tiene la tarea de:

Detectar y responder tan pronto como sea posible en caso de un ataque de virus, con un centro de detección de responsable de la supervisión continua de las redes sensibles y la implementación de mecanismos de defensa adecuados para atacar;

Prevenir la amenaza, lo que contribuye al desarrollo de una gama de productos de alta seguridad, así como los productos y servicios de confianza para las administraciones y los agentes económicos;

Desempeñar una función de asesoramiento y apoyo a los gobiernos y operadores de vital importancia;

Informa al público sobre las amenazas, incluso a través de la seguridad de la información sitio web del gobierno, lanzado en 2008, que tiene como objetivo ser el portal de referencia para la seguridad de los sistemas de información.

Dado que los productos y sistemas de seguridad, deberá:

Desarrollar y adquirir los productos de primera necesidad para la protección de las redes interdepartamentales estatales más sensibles;

Implementar los canales gubernamentales de mando y de enlace en materia de defensa y seguridad nacional, incluyendo la red de Rimbaud y de intranet Isis; la emisión de etiquetas para productos de seguridad.

Se trata de una reserva de habilidades diseñadas para proporcionar conocimientos y asistencia técnica a los gobiernos y operadores de vital importancia.

Es responsable de la promoción de tecnologías, sistemas y conocimientos nacionales. Contribuye a la construcción de la confianza en la economía digital.

Ella supervisa el centro de gobierno responsable de la transmisión de implementar los medios de mando y de enlace necesarias para el Presidente de la República y el Gobierno.

Para más información: Los Sistemas de Información de la Agencia de Seguridad Nacional (Anssi) es un servicio francés creado por decreto el 7 de julio de 2009.1 Este servicio nacional se adjunta a la Secretaria General de Defensa y Seguridad Nacional (SGDSN), responsable de asistir al Primer Ministro en el ejercicio de sus responsabilidades en la defensa y la autoridad de seguridad nacional.

La agencia es responsable del diseño, implementación y evolución de los sistemas de información de seguridad y productos de seguridad. Por lo tanto responsable de la prestación de la comunicación electrónica segura disponible en todo momento para los más altos niveles de los medios gubernamentales, así como las autoridades públicas y los organismos que participan en la gestión de situaciones de emergencia y crisis (http://www.ssi.gouv.fr/fr/anssi/)"

3.2.2.2 Guía de madurez SSI

"La Seguridad de los Sistemas de Información (SSI) de una organización debe ser manejada de acuerdo con sus problemas reales de SSI. De hecho, las organizaciones con bajas necesidades no deberían gestionar la SSI con el mismo rigor que cuando son elevadas. Esta declaración aparentemente simple, es cuestionable si queremos responder de manera.

Utilizando preguntas pragmáticas, esta guía tiene como objetivo determinar rápidamente cuestiones relacionadas con el sistema de información de la organización, para medir la diferencia entre lo que debe hacerse y lo que se está haciendo, y para explicar las acciones que se implementarán para gestionar adecuadamente la ISS.

El enfoque se inspira en la ISO 21827. Este estándar define los niveles de madurez, llamados acumulativos para la gestión de un SSI. Cada nivel representa cómo una organización ejecuta, controla, mantiene y supervisa un proceso SSI. Lograr un nivel supone haber alcanzado los anteriores." *Maturité SSI – Approche méthodologique,* ANSSI (2007) [4]

3.2.3 ISO/IEC 27000

La información descrita en este apartado se ha obtenido de (http://www.iso27000.es/)

3.2.3.1 Descripción

ISO/IEC 27000 es un conjunto de estándares desarrollados -o en fase de desarrollo- por ISO (International Organization for Standardization) e IEC (International Electrotechnical Commission), que proporcionan un marco de gestión de la seguridad de la información utilizable por cualquier tipo de organización, pública o privada, grande o pequeña.

Objetivos

Esta familia de normas tiene como objetivo proporcionar un marco para la gestión de la seguridad de la información a partir de la definición, desarrollo, implementación y

mantenimiento de un Sistema de Gestión de la Información (SGSI). La serie contiene las mejores prácticas recomendadas en seguridad de la información.

Es aplicable a empresas de cualquier tamaño en cualquier parte del mundo.

3.2.3.2 Familia 27000

3.2.3.2.1 Beneficios

- Garantía de los controles internos y cumplimiento de requisitos de gestión corporativa y de continuidad de la actividad comercial.
- Pone de manifiesto el respeto a las leyes y normativas que sean de aplicación.
- Fiabilidad de cara al cliente demostrar que la información está segura.
- Identificación, evaluación y gestión de riesgos.
- Evaluaciones periódicas que ayudan a supervisar el rendimiento y las posibles mejoras.
- Se integra con otros sistemas de gestión
- Reducción de costes y mejora de procesos
- Aumento de la motivación y satisfacción del personal al contar con unas directrices claras.

3.2.3.2.2 Implantación

La norma ISO 27001 (la principal de la familia) es certificable por una entidad de certificación externa y su implantación puede tardar de 6 a 12 meses dependiendo del nivel de seguridad de la información y del alcance de la empresa en la que se implante y es preferible realizar el proceso con ayuda de alguna consultoría externa a la organización.

3.2.3.2.3 Sistema de Gestión de la Seguridad de la Información

El SGSI (Sistema de Gestión de Seguridad de la Información) es el concepto central sobre el que se construye ISO 27001.

Diferentes autores se refieren a Sistemas de Seguridad de la Información SSI de forma similar a SGSI. En este documento, y a efectos de cálculos se utilizará el término SSI.

La gestión de la seguridad de la información debe realizarse mediante un proceso sistemático, documentado y conocido por toda la organización.

Este proceso es el que constituye un SGSI, que podría considerarse, por analogía con una norma tan conocida como ISO 9001, como el sistema de calidad para la seguridad de la información.

Garantizar un nivel de protección total es virtualmente imposible, incluso en el caso de disponer de un presupuesto ilimitado. El propósito de un sistema de gestión de la seguridad de la información es, por tanto, garantizar que los riesgos de la seguridad de la información sean conocidos, asumidos, gestionados y minimizados por la organización de una forma documentada, sistemática, estructurada, repetible, eficiente y adaptada a los cambios que se produzcan en los riesgos, el entorno y las tecnologías.

En el contexto aquí tratado, se entiende por información todo aquel conjunto de datos organizados en poder de una entidad que posean valor para la misma, independientemente de la forma en que se guarde o transmita (escrita, en imágenes, oral, impresa en papel, almacenada electrónicamente, proyectada, enviada por correo, fax o e-mail, transmitida en conversaciones, etc.), de su origen (de la propia organización o de fuentes externas) o de la fecha de elaboración.

La seguridad de la información, según ISO 27001, consiste en la preservación de su confidencialidad, integridad y disponibilidad, así como de los sistemas implicados en su tratamiento, dentro de una organización. Así pues, estos tres términos constituyen la base sobre la que se cimienta todo el sistema de seguridad de la información:

• Confidencialidad: la información no se pone a disposición ni se revela a individuos, entidades o procesos no autorizados.

• Integridad: mantenimiento de la exactitud y completitud de la información y sus métodos de proceso.

• Disponibilidad: acceso y utilización de la información y los sistemas de tratamiento de la misma por parte de los individuos, entidades o procesos autorizados cuando lo requieran.

Para garantizar que la seguridad de la información es gestionada correctamente, se debe hacer uso de un proceso sistemático, documentado y conocido por toda la organización, desde un enfoque de riesgo empresarial. Este proceso es el que constituye un SGSI.

La información, junto a los procesos y sistemas que hacen uso de ella, son activos muy importantes de una organización. La confidencialidad, integridad y disponibilidad de información sensible pueden llegar a ser esenciales para mantener los niveles de competitividad, rentabilidad, conformidad legal e imagen empresarial necesarios para lograr los objetivos de la organización y asegurar beneficios económicos.

Las organizaciones y sus sistemas de información están expuestos a un número cada vez más elevado de amenazas que, aprovechando cualquiera de las vulnerabilidades existentes, pueden someter a activos críticos de información a diversas formas de fraude, espionaje, sabotaje o vandalismo. Los virus informáticos, el “hacking” o los ataques de denegación de servicio son algunos ejemplos comunes y conocidos, pero también se deben considerar los riesgos de sufrir incidentes de seguridad causados voluntaria o involuntariamente desde dentro de la propia organización o aquellos provocados accidentalmente por catástrofes naturales y fallos técnicos.

El cumplimiento de la legalidad, la adaptación dinámica y puntual a las condiciones variables del entorno, la protección adecuada de los objetivos de negocio para asegurar el máximo beneficio o el aprovechamiento de nuevas oportunidades de negocio, son algunos de los aspectos fundamentales en los que un SGSI es una herramienta de gran utilidad y de importante ayuda para la gestión de las organizaciones.

El nivel de seguridad alcanzado por medios técnicos es limitado e insuficiente por sí mismo. En la gestión efectiva de la seguridad debe tomar parte activa toda la organización, con la gerencia al frente, tomando en consideración también a clientes y proveedores de bienes y servicios. El modelo de gestión de la seguridad debe contemplar unos procedimientos adecuados y la planificación e implantación de controles de seguridad basados en una evaluación de riesgos y en una medición de la eficacia de los mismos.

El Sistema de Gestión de la Seguridad de la Información (SGSI) ayuda a establecer estas políticas y procedimientos en relación a los objetivos de negocio de la organización, con objeto de mantener un nivel de exposición siempre menor al nivel de riesgo que la propia organización ha decidido asumir.

Con un SGSI, la organización conoce los riesgos a los que está sometida su información y los asume, minimiza, transfiere o controla mediante una sistemática definida, documentada y conocida por todos, que se revisa y mejora constantemente.

3.2.3.2.4 Implantación de un SGSI

Localizar y arreglar vulnerabilidades en una solución incompleta, lo que aporta valor añadido es desarrollar estrategias para prevenir las vulnerabilidades.

3.2.3.3 ISO 27002:2005(anterior ISO 17799:2005)

3.2.3.3.1 Descripción

Es una guía de buenas prácticas que describe los objetivos de control y controles recomendables en cuanto a seguridad de la información. No es certificable. Contiene 39 objetivos de control y 133 controles, agrupados en 11 dominios. Como se ha mencionado en su apartado correspondiente, la norma ISO 27001 contiene un anexo que resume los controles de ISO 27002:2005.

3.2.4 SANS

3.2.4.1 Descripción

“El Instituto SANS (SysAdmin Audit, Networking and Security Institute) es una institución con ánimo de lucro fundada en 1989, con sede en Bethesda (Maryland, Estados Unidos) que agrupa a 165.000 profesionales de la seguridad informática (consultores, administradores de sistemas, universitarios, agencias gubernamentales, etc.)

Sus principales objetivos son:

Reunir información sobre todo lo referente a seguridad informática (sistemas operativos, routers, firewalls, aplicaciones, IDS, etc.)

Ofrecer capacitación y certificación en el ámbito de la seguridad informática

Igualmente, el SANS Institute es una universidad formativa en el ámbito de las tecnologías de seguridad. Es una referencia habitual en la prensa sobre temas de auditoría informática. (http://es.wikipedia.org/wiki/SANS_Institute/)"

3.2.4.2 Controles críticos de seguridad para una ciberdefensa efectiva

"Con los años, muchas normas de seguridad y marcos normativos han sido desarrolladas para intentar de contrarrestar los riesgos en los sistemas empresariales críticos y los datos que hay en ellos. Sin embargo, la mayor parte es de estos esfuerzos se han convertido esencialmente en la presentación de informes sobre el cumplimiento y la seguridad se ha descuidado. Es necesario atender a la constante evolución en los ataques. En 2008, esto era un problema grave como reconoció la Agencia Nacional de Seguridad de Estados Unidos (NSA), y comenzaron un trabajo de años que tuvo como objetivo mejorar la defensa mediante la priorización de una lista de los controles que tendrían el mayor impacto en la mejor posición contra las amenazas terroristas en el mundo real. Un consorcio de organismos internacionales y de Estados Unidos creció rápidamente, y fue acompañado por expertos de la industria privada en todo el mundo. En última instancia, las recomendaciones que se concretaron en los controles de seguridad críticos fueron coordinadas a través del Instituto SANS. En 2013, la administración y el mantenimiento de los controles fueron trasladados al Consejo sobre Ciberseguridad, una entidad independiente global sin ánimo de lucro comprometida con un Internet seguro y abierto.

Los controles de seguridad críticos se centran en las funciones de seguridad priorizando su eficacia contra las últimas y más avanzadas amenazas, con un fuerte énfasis en "lo que funciona". La estandarización y la automatización son las otras máximas prioridades, para ganar eficiencia operativa mientras se mejora la eficacia. La acción definida por los controles es un subconjunto del amplio catálogo definido por el Instituto Nacional de Estándares y Tecnología (NIST) SP 800-53. Dado que los controles se derivaron de los patrones de ataque más comunes y fueron sometidos, a través de una amplia comunidad del gobierno y de la industria, con un fuerte consenso sobre el resultado, el conjunto de controles sirven como base para las acciones de alto valor inmediato. (http://www.sans.org/critical-security-controls/)"

3.2.5 Conclusiones

Las normas y guías de ANSSI e ISO 27000 se enfocan en el nivel organizativo de los sistemas de información. Al no encontrar ninguna solución que abarque tanto los niveles teóricos y organizativos como prácticos proponemos una metodología que permita alcanzar objetivos prácticos cumpliendo los marcos teóricos y organizativos.

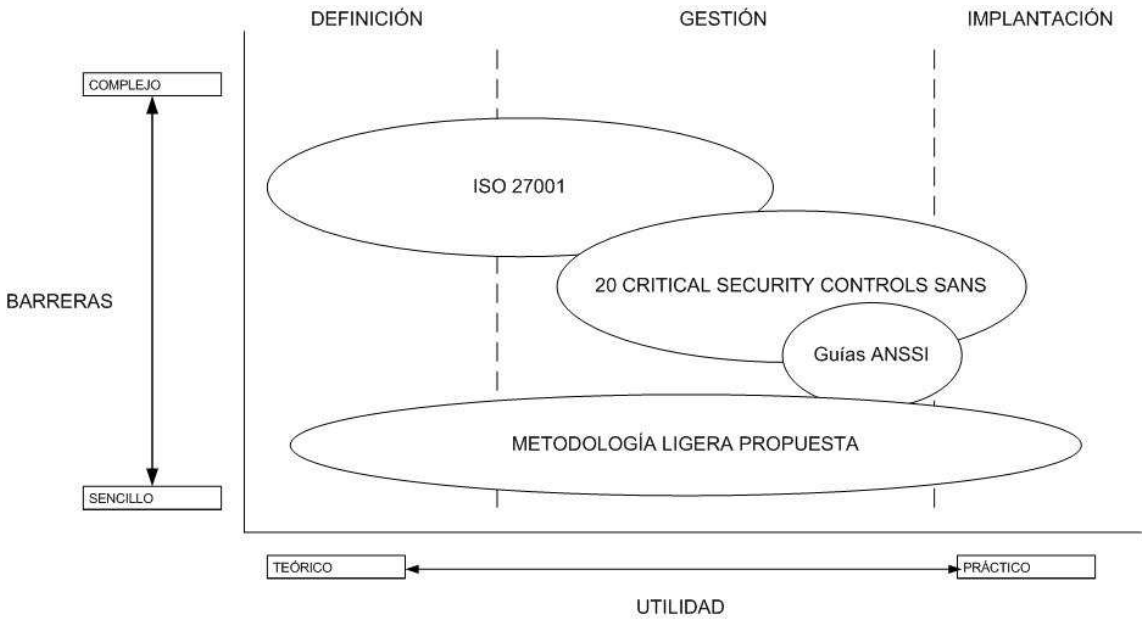


Figura 8. Cobertura de las diferentes normas.

4 Plan de trabajo y/o metodología utilizada

4.1 Introducción

Esta metodología pretende ser una herramienta para un tipo de empresas, las PYMES en un mercado concreto, el español.

Se ha creado un método a partir de normas y estándares aceptados que permita evaluar y mejorar los sistemas de seguridad en empresas. Este referencial debe reducir o eliminar la complejidad tanto de implantación como de mantenimiento y autoevaluación. Pretende ser práctico y de coste reducido. Generar confianza es una prioridad.

Se pretende determinar los niveles efectivo (nivel de protección real) y adecuado (nivel de protección que debe tener la empresa) y presentar un método para definir, de forma práctica, la forma más rápida y de menor coste para pasar de un nivel a otro.

Los objetivos concretos de la metodología presentada son:

1. Evaluar los riesgos en los sistemas informáticos.
2. Localizar los activos vulnerables y los datos sensibles y documentar su topología en dominios y perímetros.
3. Identificar la existencia y el grado de madurez del Sistema de Seguridad Informática SSI.
4. Realizar un análisis del grado de eficiencia del SSI.
5. Presentar informes sencillos y comprensibles donde se reflejen tanto el nivel actual de protección como el nivel adecuado a la tipología y volumen de la empresa.
6. Presentar una hoja de ruta con las tareas a realizar para la obtención del nivel adecuado.
7. Tutorizar la creación o mejora del SSI y entregar la documentación necesaria para la autogestión en las empresas por personal no experto.
8. Presentar un catálogo con las diferentes soluciones existentes en el mercado para cubrir las necesidades detectadas.

Esta metodología pretende:

- Minimizar los costes de implantación y gestión de un SSI.
- Industrializar los procesos de protección de los sistemas informáticos en PYMES.
- Crear un método que haga llegar a todas las empresas las normativas, estándares y directrices de seguridad.

4.2 Estructura de la metodología

A partir del estudio del estado del arte, se ha comprobado la necesidad de cimentar tanto la estructura del método como cada una de sus fases en estándares, normativas, directrices legales y recomendaciones ampliamente aceptadas.

El método se compone de 4 fases, y se argumentará en cada una de ellas su función, la base teórica o normativa que la sustenta y los beneficios que aporta al método.

Estas fases son:

1. Análisis.
2. Evaluación.
3. Presentación de resultados.
4. Propuesta y hoja de ruta.

Tanto la estructura del método como cada una de sus partes ha sido diseñada con el objetivo de reducir las barreras a la adopción al mínimo pero manteniendo el cumplimiento de las normas aplicadas en cada parte.

La seguridad de los sistemas de información en una organización debe ser la adecuada a sus características, a sus necesidades y a su relación con el entorno.

Dado que los diferentes estándares y normas suelen ser generalistas y de amplio espectro esto hace que el estudio y la implantación de estas soluciones sea complejo y costoso tanto económicamente como en tiempo.

El método presentado pretende presentar unos cuestionarios de evaluación reducidos que determinen el estado real y las necesidades específicas de la organización.

En la primera fase de análisis, mediante la realización de diferentes cuestionarios se determinan las características de la empresa evaluada, sus entornos y perímetros así como los activos a proteger y su grado de sensibilidad. También se determinará en esta fase el grado de madurez del SSI.

En la fase 2, de evaluación, se ha realizado un referencial que se compone de unos cuestionarios que evaluarán con detalle y de forma práctica el nivel de protección de cada una de las partes de los sistemas informáticos de la organización.

Estos cuestionarios están estructurados de forma jerárquica y utilizan como parámetros las conclusiones obtenidas en la fase anterior.

Los parámetros como el tipo de empresa, el nivel de madurez efectivo y adecuado así como la determinación de los riesgos se utilizarán como filtro que reducirán en este nivel la cantidad de cuestiones a realizar de entre todas las posibles y focalizará los resultados a los diferentes ambientes de aplicación.

La estructuración jerárquica de los cuestionarios permite ignorar o eliminar cuestiones de niveles inferiores cuando la información aportada en el nivel superior sea suficiente.

La fase 3 es la de generación de resultados. Se han realizado plantillas en las que a partir de las respuestas a los formularios y aplicando un sistema de pesos y discriminado auto calcule los diferentes valores del estado del sistema.

En esta fase se considera oportuno presentar dos tipos de resultados. Un sumario que refleje el estado y las necesidades de forma resumida y comprensible para los órganos ejecutivos de las organizaciones y un informe técnico con los resultados de las diferentes evaluaciones. Se

pretende en esta fase reducir la falta de concienciación así como conseguir el apoyo necesario para la mejora de los SSI.

En la fase 4 se presenta una hoja de ruta con las diferentes tareas a realizar para conseguir alcanzar el nivel adecuado. En esta fase se presenta un algoritmo en el cual deberán realizarse los diferentes proyectos y tareas de forma iterativa desde el menor nivel de protección hasta que cada una de las partes vaya escalando hasta el nivel adecuado a la organización.

La estructuración de los controles y subcontroles del referencial en 4 niveles según el beneficio aportado, permitirá determinar las tareas que supondrán una ganancia rápida pudiendo realizar una primera tarea de estabilización con un coste económico y de tiempo muy reducido y rápidos beneficios.

La aplicación dinámica de este método aportará a las empresas la visibilidad y la comprensión de su SSI de una forma resumida y permitirá mantener una autogestión adecuada del SSI por el personal de la organización.

4.3 Fases de la metodología

4.3.1 Fase 1: Análisis

Para la elaboración de este punto se han tomado como referencia las fuentes citadas en el apartado 8.3 Fase de análisis.

La seguridad de los sistemas de información (SSI) de una organización debe ser la adecuada a sus necesidades. Para ello es necesario determinar cuáles son estas necesidades concretas antes de evaluar el SSI.

Dado que las necesidades de las pymes en este contexto son más reducidas en algunos aspectos y a su vez, diferentes por las particularidades de cada empresa, el proceso de evaluación debe también ser reducido.

En esta fase se pretende conseguir una primera aproximación de las necesidades de cada empresa para poder adaptar el referencial de evaluación. Para ello se realizarán unas cuestiones iniciales sobre el tipo de empresa, el grado de exposición a incidentes informáticos y sobre su topología.

Con el resultado de las cuestiones anteriores se catalogará la empresa en 4 tipos básicos. A continuación se realizará un estudio del grado de madurez de la protección del sistema informático.

El grado de madurez del SSI será el valor de referencia utilizado para reducir el número de cuestiones y la extensión del estudio.

En este punto sería importante solicitar a la empresa diagramas de la topología de los sistemas en caso de existir.

4.3.1.1 Tipo de empresa:

Este valor es estimado por el tipo de empresa y será subjetivo. Este valor pretende ser una medida de control para empresas que aunque aparentemente tuvieran un nivel de exposición bajo tengan unas características singulares como por ejemplo banca, salud, telecomunicaciones, más de 300 empleados, etc.

En caso de estimarse que el nivel adecuado es bajo para las particularidades del tipo de empresa (ej. Microempresas con datos muy críticos o sensibles, pequeñas empresas con alta repercusión social, etc.). Este nivel se podrá elevar al nivel inmediatamente superior de forma consensuada entre el evaluador y la empresa.

Estos valores pretenden ser utilizados en futuras líneas de trabajo para reducir y ajustar las diferentes fases de la metodología.

¿A qué sector pertenece la empresa?

Sector	Servicios Financieros y Banca	
	Construcción/Ingeniería	
	Telecomunicaciones	
	Sector de Energía	
	Salud	
	Alimentos	
	Educación	
	Gobierno/Sector público	
	Manufactura	
	Consultoría Especializada	

¿Cuántos empleados tiene?

Nº Empleados	1 a 50	
	51 a 100	
	101 a 200	
	201 a 300	
	301 a 500	

¿Cuál es el tipo de propiedad de la empresa?

Propiedad del capital	Empresa privada	
	Empresa pública	
	Empresa Mixta	

¿Cuál es el ámbito de actividad?

Ámbito de actividad	Local	
	Provincial	
	Nacional	
	Multinacional	

¿A qué se destinan los beneficios?

Destino de los beneficios	Con ánimo de lucro	
	Sin ánimo de lucro	

¿Cuál es la forma jurídica?

Forma jurídica	Unipersonal	
	Sociedad colectiva	
	Cooperativa	
	Comanditaria	
	Sociedad de responsabilidad limitada	
	Sociedad Anónima	

4.3.1.2 Catalogación del tipo de empresa según su grado de exposición a amenazas

Grado de afectación por incidentes tecnológicos:

Valor	Cuestiones	0 Nada 5 Completamente

V1	¿Cómo afectaría la perdida de conexión a internet a su negocio?	
V2	¿Cómo afectaría la imposibilidad de acceder a sus equipos informáticos?	
V3	¿Cómo afectaría la perdida de información o datos almacenada?	

Topología:

Valor	Cuestiones	
V4	¿Cuántos equipos informáticos estima que hay en su empresa?	
V4	¿Cuántos de ellos gestionan información o procesos críticos?	
V5	¿Cuántos servidores estima que hay en su empresa?	
V5	¿Cuántos de ellos gestionan información o procesos críticos?	
V6	¿Cuántas sedes tiene su empresa?	
V6	¿Existen líneas de comunicación entre ellas?	
V6	¿Las redes de comunicación entre las sedes son críticas?	
V7	¿Utiliza servicios de internet para su negocio?	
V7	¿Son críticos?	
V7	¿Guarda información crítica en estos servicios?	

Con el resultado de las cuestiones anteriores se catalogará la empresa en uno de los siguientes tipos dependiendo del grado de exposición.

Se asignarán 8 valores:

Grado de afectación.

Uno por cada respuesta V1, V2, V3:

Las respuestas tendrán la siguiente asignación de valores.

0 y 1	Baja
2	Media
3	Alta
4 y 5	Muy Alta

Tabla 6: Niveles de grado de afectación

Topología:

Proporción entre el número de equipos y los que son críticos V4.

<=10%	Baja
>10%<=20%	Media
>20%<=30%	Alta
>30%	Muy Alta

Tabla 7: Proporción de equipos por criticidad

Proporción de servidores críticos V5

<=30%	Baja
>30%<=40%	Media
>40%<=50%	Alta
>50%	Muy Alta

Tabla 8: Proporción de servidores por criticidad

Importancia de las comunicaciones entre sedes V6

No existen sedes	Baja
Varias sedes no comunicadas	Media
Varias sedes comunicadas	Alta
La comunicación es crítica	Muy Alta

Tabla 9: Importancia de las comunicaciones

Se utilizan servicios de internet, son críticos o almacenan información crítica V7.

No se utilizan servicios de internet	Baja
Se utilizan pero ni procesos ni datos son críticos	Media
Los procesos o los datos son críticos.	Alta
Ambos son críticos	Muy Alta

Tabla 10: Criticidad de los servicios de internet

El grado de exposición será el valor máximo de Vn y en caso de que este valor aparezca en al menos 3 ocasiones el inmediatamente superior.

Grado de exposición del negocio ante incidentes de seguridad informática	
T1	Baja
T2	Media
T3	Alta
T4	Muy Alta

Tabla 11: Grado de exposición ante incidentes de seguridad

Este valor podrá ser aumentado por consenso entre el evaluador y la empresa, dependiendo del resultado de los cuestionarios de tipo de empresa en casos poco comunes.

4.3.1.3 Estudio del estado de madurez del SSI. Determinar los niveles efectivo y adecuado

4.3.1.3.1 Introducción

Una vez estimados el grado de afectación y el tipo de empresa es necesario estimar el nivel de protección actual.

En este punto se explicará y detallará el método de evaluación de madurez de ANSSI

Para la realización de este módulo se ha tomado como referencia *Maturité SSI – Approche méthodologique, ANSSI* (2007) [4] al cual está inspirado a su vez en *ISO 21827 - Systems Security Engineering – Capability Maturity Model*, ISO, (2001) [3].

En este apartado se pretende evaluar la diferencia entre lo que debería estar hecho y lo que realmente hay hecho.

Esta norma define 5 niveles de madurez acumulativos para la gestión de SSI en organizaciones. Estos niveles representan la forma en que un organismo ejecuta, controla, mantiene y asegura el SSI. Para conseguir un nivel se debe haber conseguido el anterior. Para facilitar el trabajo durante el método, se ha realizado una correspondencia entre estos 5 niveles y la organización en 4 niveles presentada. Para ello, simplemente se unen los niveles 4 y 5 como nivel 4.

Nivel	Nivel adecuado de madurez SSI	Explicación
0	Práctica inexistente o incompleta	Prácticas de base eventuales y aisladas donde no se conoce las necesidades
1	Práctica informal	Prácticas de base implantadas de forma informal y reactiva

2	Práctica repetible y seguida	Prácticas de base implantadas de forma planificada y con soporte de la organización
3	Proceso definido	Implantación de un proceso descrito, adaptado a la organización y entendido por todos los actores en la organización
4	Proceso controlado	Procesos coordinados y controlados con la ayuda de medidas que permitan su corrección
5	Proceso optimizado continuamente	Mejora del proceso dinámica, institucionalizada y que tiene en cuenta la evolución del contexto

Tabla 12: Niveles de madurez SSI

4.3.1.3.2 Aplicación del módulo

La aplicación de este apartado se compone originalmente de tres partes, la determinación del nivel adecuado, la determinación del nivel efectivo y la definición de cómo conseguir el nivel adecuado. Esta última parte se utilizará como base para la fase 4 del método.

4.3.1.3.3 Determinación del nivel adecuado

Esta parte se compone de un diagnóstico de 12 cuestiones que debe responder el responsable del perímetro a evaluar.

A continuación se presentan el cuestionario organizado en 4 grupos y el diagrama para el cálculo.

- **Estimación del nivel de consecuencias potenciales:**

Pregunta 1: ¿Cuál es la importancia del sistema de información para el negocio?

El objetivo es evaluar el grado de dependencia del sistema de información.

Respuestas	Valor
El SI es accesorio al cumplimiento del negocio	0
El SI es útil para el cumplimiento del negocio	1
El SI es necesario para el cumplimiento del negocio	2
El SI es vital para el cumplimiento del negocio	3

Pregunta 2: ¿Cuáles son las consecuencias internas (problemas de funcionamiento, impacto financiero, impacto jurídico,…) de un incidente de seguridad en su SI? Ej.: DoS, pérdida de información, ataque de virus, etc.

El objetivo es evaluar el impacto para la organización de un incidente de seguridad.

Respuestas	Valor
Las consecuencias internas de un siniestro SSI son despreciables	0
Las consecuencias internas de un siniestro SSI son significativas	1
Las consecuencias internas de un siniestro SSI son graves	2
Las consecuencias internas de un siniestro SSI son fatales	3

Pregunta 3: ¿Cuáles son las consecuencias externas (imagen, seguridad del entorno, contratos,…) de un incidente de seguridad en su SI?

El objetivo es evaluar el impacto externo tras un incidente de seguridad.

Respuestas	Valor
Las consecuencias externas de un siniestro SSI son despreciables	0
Las consecuencias externas de un siniestro SSI son significativas	1
Las consecuencias externas de un siniestro SSI son graves	2
Las consecuencias externas de un siniestro SSI son fatales	3

- **Estimación de la sensibilidad de la información:**

Pregunta 4: ¿En qué medida es importante la disponibilidad de los sistemas informáticos?

El objetivo es estimar la necesidad de disponibilidad de los activos informáticos a partir del nivel de impacto que pueda tener la falta de disponibilidad.

Respuestas	Valor
La falta de accesibilidad al SI no afecta a la actividad	0
La falta de accesibilidad al SI perturba a la actividad	1
La falta de accesibilidad al SI es grave para la actividad	2
La falta de accesibilidad al SI es fatal para la actividad	3

Pregunta 5: ¿Dentro del marco de la actividad, en qué medida es importante la integridad de los datos?

El objetivo es estimar la importancia de la integridad de la información en los sistemas informáticos a partir del nivel de impacto.

Respuestas	Valor
La alteración de datos no afecta a la actividad	0
La alteración de datos perturba a la actividad	1
La alteración de datos es grave para la actividad	2
La alteración de datos es fatal para la actividad	3

Pregunta 6: ¿En qué medida es importante la confidencialidad de la información en el ámbito de actividad de la empresa?

El objetivo es evaluar la importancia de la confidencialidad de la información en los SI a partir del nivel de impacto.

Respuestas	Valor
Si la seguridad de la información ha sido comprometida, no afecta a la actividad	0
Si la seguridad de la información ha sido comprometida, perturba a la actividad	1
Si la seguridad de la información ha sido comprometida, es grave para la actividad	2
Si la seguridad de la información ha sido comprometida, es fatal para la actividad	3

- **Estimación del grado de exposición a las amenazas:**

Pregunta 7: ¿Cuál es la frecuencia estimada de incidentes SSI?

El objetivo es evaluar la frecuencia de incidentes SSI accidentales o provocados.

Respuestas	Valor
Los siniestros SSI son muy raros	0
Varios siniestros SSI por año	1

Varios siniestros SSI por trimestre	2
Varios siniestros SSI por mes	3

Pregunta 8: ¿Cuál es el grado de motivación de los atacantes potenciales?

El objetivo es evaluar el grado de motivación de los posibles atacantes, los cuales pueden ser de carácter estratégico, ideológico, político, terrorista, etc.

Respuestas	Valor
Un ataque SSI sobre el perímetro es prácticamente inimaginable	0
La motivación de los atacantes potenciales es baja	1
La motivación de los atacantes potenciales es alta	2
La motivación de los atacantes potenciales es muy alta	3

Pregunta 9: ¿Cuáles son las competencias y recursos de los atacantes potenciales?

El objetivo es evaluar la capacidad de daño potencial de los atacantes.

Respuestas	Valor
Loa atacantes potenciales poseen medios débiles	0
Loa atacantes potenciales poseen medios significativos	1
Loa atacantes potenciales poseen medios avanzados	2
Loa atacantes potenciales poseen medios ilimitados	3

- **Estimación de la importancia de las vulnerabilidades:**

Pregunta 10: ¿Cuál es el nivel de heterogeneidad del sistema de información?

El objetivo es evaluar la variedad de componentes y complejidad de la arquitectura funcional, física y de la red ya que a mayor complejidad mayor vulnerabilidad.

Respuestas	Valor
El SI es homogéneo	0
El SI es débilmente heterogéneo	1

El SI es fuertemente heterogéneo	2
El SI es extremadamente heterogéneo	3

Pregunta 11: ¿Cuál es el grado de apertura del SI?

El objetivo es evaluar el grado de interconexión con otros SI internos o externos así como el grado de control.

Respuestas	Valor
El SI no es abierto	0
El SI solo está abierto a los sistemas internos	1
El SI está abierto a sistemas externos bajo control	2
El SI está abierto a sistemas externos sin control	3

Pregunta 12: ¿Cuál es el nivel de variabilidad de los componentes del SI (material, SW, redes, locales, personal,…) y del contexto en el que opera (restricciones, exigencias normativas, amenazas,…)?

El objetivo es evaluar la estabilidad del SI.

Respuestas	Valor
El SI es estable	0
El SI y su contexto cambian poco	1
El SI y su contexto cambian a menudo	2
El SI y su contexto cambian continuamente	3

Después de responder a cada una de las preguntas sumaremos los valores máximos de cada uno de los bloques y los compararemos con la siguiente tabla obteniendo así el nivel adecuado:

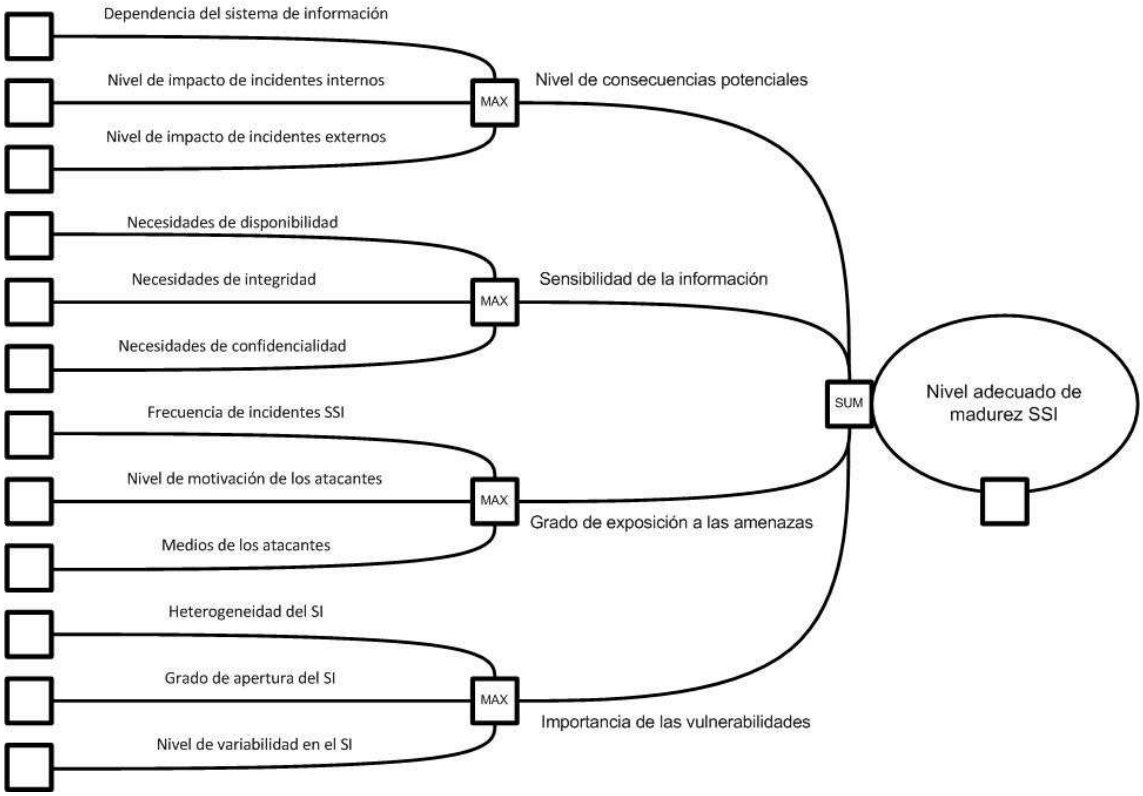


Figura 9. Cálculo del nivel de madurez.

Nivel	Nivel adecuado de madurez SSI	Suma de valores	Nivel
0	Práctica inexistente o incompleta	Todos 0	N0
1	Práctica informal	De 0 a 2	N1
2	Práctica repetible y seguida	De 3 a 5	N2
3	Proceso definido	De 6 a 8	N3
4	Proceso controlado	De 9 a 10	N4
5	Proceso optimizado continuamente	De 11 a 12	N4

Tabla 13: Nivel adecuado de madurez SSI

En caso de existir procesos y perímetros diferentes y aislados dentro de la organización habría que aplicar el método en cada caso y documentar convenientemente el proceso y su justificación.

En este punto se han determinado dos valores, el del grado de exposición y el de madurez del SSI. Estos valores son indicativos de las amenazas que afectan a la empresa y de cómo se gestionan.

El **nivel adecuado** será el valor más alto de los dos

4.3.1.3.4 Determinación del nivel efectivo.

Según la metodología aplicada en esta fase basada en *Maturité SSI – Approche méthodologique, ANSSI* (2007) [4], el punto siguiente sería el de determinar el nivel efectivo.

El método original estimaba el grado de madurez efectiva del SSI. En nuestro caso se pretende además evaluar el nivel efectivo de protección de forma más práctica por lo que se complementará en la fase 2.

Para ello, será necesario reconocer los procesos SSI implementados en la organización.

Los siete principales procesos SSI genéricos son los siguientes:

Categoría	Proceso genérico	Objetivo
Procesos de gestión	Definir la estrategia SSI	Disponer de objetivos SSI medibles, directrices SSI y de un plan de acción adaptado al nivel adecuado de madurez y alineado con la estrategia del organismo
	Gestionar los riesgos SSI	Identificar los riesgos SSI y mantenerlos a un nivel aceptable para el organismo teniendo en cuenta su contexto
	Gestionar las reglas SSI	Disponer de reglas SSI adecuadas y basadas en la gestión de riesgos, prever las acciones para cumplir estas reglas y disponer de elementos para comprobar el cumplimiento
	Supervisar el SSI	Definir un marco de control y asegurarse que las medidas de supervisión se ajustan a ese marco.
Procesos operacionales	Definir las medidas SSI	Asegurar la integración de las medidas en el contexto operacional y documentar las características de estas medidas
	Realizar las medidas SSI	Implementar las medidas, integrarlas y validarlas
	Explotar las medidas SSI	Desplegar las medidas en el entorno operacional, asegurar su conformidad e identificar los incidentes que se generen

Tabla 14: Procesos SSI genéricos

Estos procesos están definidos de forma genérica por lo que es conveniente verificar su existencia y de las actividades ligadas a ellos para determinar si es conveniente su evaluación.

A continuación se presenta una tabla en donde identificar las exigencias de cumplimiento de cada nivel de madurez del SSI con cada uno de los procesos.

El responsable de cada proceso SSI deberá posicionarlo dentro de esta estructura de niveles indicando el cumplimiento de cada punto.

El cumplimiento de todas las exigencias de un proceso indicará que este ha alcanzado dicho nivel. Un nivel es alcanzado por una organización.

Exigencias para alcanzar un nivel de madurez SSI	Definir la estrategia SSI	Gestionar los riesgos SSI	Gestionar las reglas SSI	Supervisar el SSI	Definir las medidas SSI	Realizar las medidas SSI	Explotar las medidas SSI
Las acciones se realizan utilizando prácticas de base							
Nivel 1							
Las acciones están planificadas							
Los actores son competentes en SSI							
Algunas prácticas están formalizadas							
Se realizan algunas medidas cualitativas							
Las autoridades competentes están informadas de las medidas							
Nivel 2							
Los procesos están definidos, estandarizados y formalizados							
Los actores tienen las competencias apropiadas a los procesos							
La organización apoya los procesos							
Nivel 3							
Los procesos están coordinados en todo el perímetro							
Medidas cuantitativas se efectúan regularmente							
Se analizan las medidas efectuadas							
Los procesos se mejoran como resultado del análisis							
Nivel 4							
El proceso se adapta de forma dinámica a las situaciones							
El análisis de las medidas está definido, estandarizado y formalizado							
La mejora de los procesos está definida, estandarizada y formalizada							
La mejora de los procesos está documentada							
Nivel 5							
Nivel efectivo de madurez de los procesos SSI							

Tabla 15: Exigencias de los procesos

4.3.1.3.5 Conseguir el nivel adecuado.

En este punto paso a explicar la tercera parte del método basado en *Maturité SSI – Approche méthodologique, ANSSI* (2007) [4] donde se plantea el método para conseguir el nivel de madurez adecuado para una organización. Este punto servirá de base para la fase 4 de la metodología dentro del proceso para conseguir el nivel adecuado de protección.

El objetivo de este paso es planificar una serie de acciones que permitan evolucionar progresivamente el nivel de madurez efectiva hasta que coincida con el nivel de madurez adecuado.

Para pasar del nivel efectivo al nivel adecuado, la empresa deberá planificar una serie de tareas para mejorar progresivamente sus prácticas. Ya que el nivel de madurez es un nivel acumulativo, para alcanzar un nivel será necesario conseguir antes en nivel anterior.

Para ello se plantea como principio general comenzar por los procesos en donde el nivel sea el más bajo hasta conseguir la uniformidad de todos los procesos en un nivel. A continuación se repetirá de forma iterativa la definición de tareas para hacer evolucionar los niveles más bajos al siguiente nivel, acabando cuando todos los procesos alcancen el nivel adecuado.

Este método permite obtener resultados visibles y ganancias rápidas.

A continuación se muestra un ejemplo del método de iteraciones:

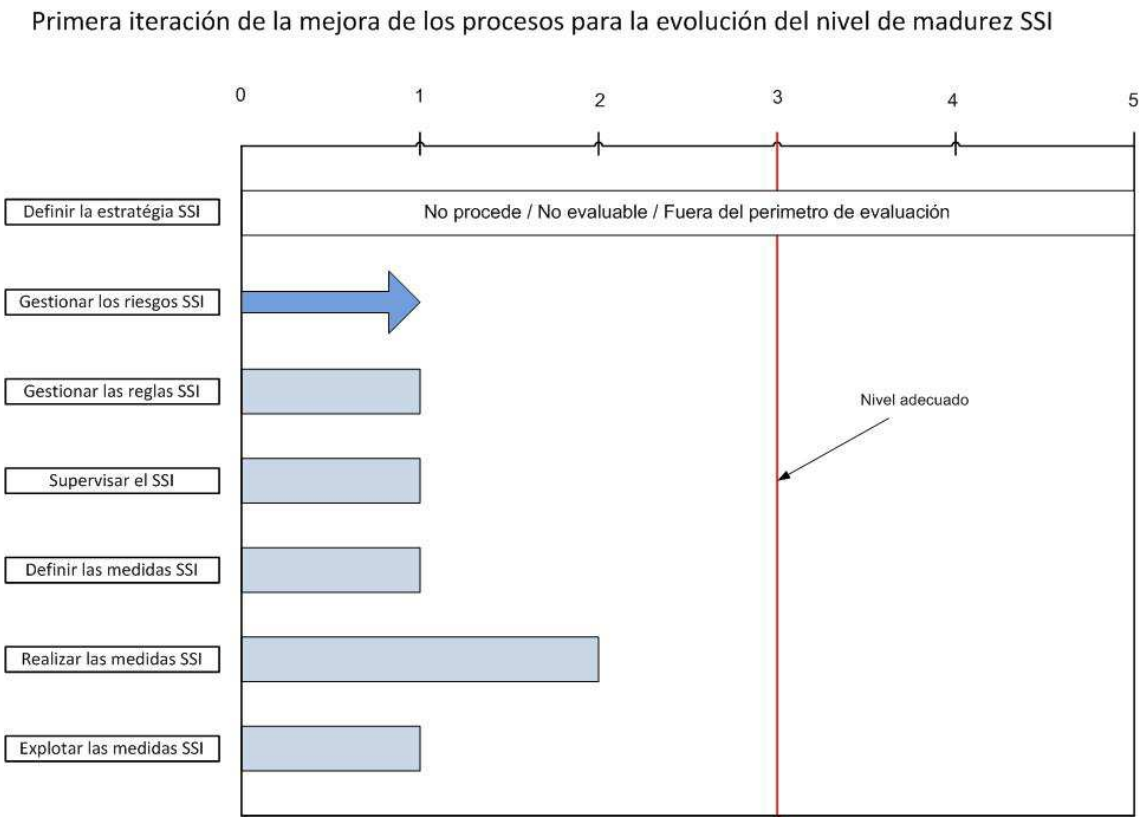


Figura 10. Primera iteración para alcanzar el nivel de madurez

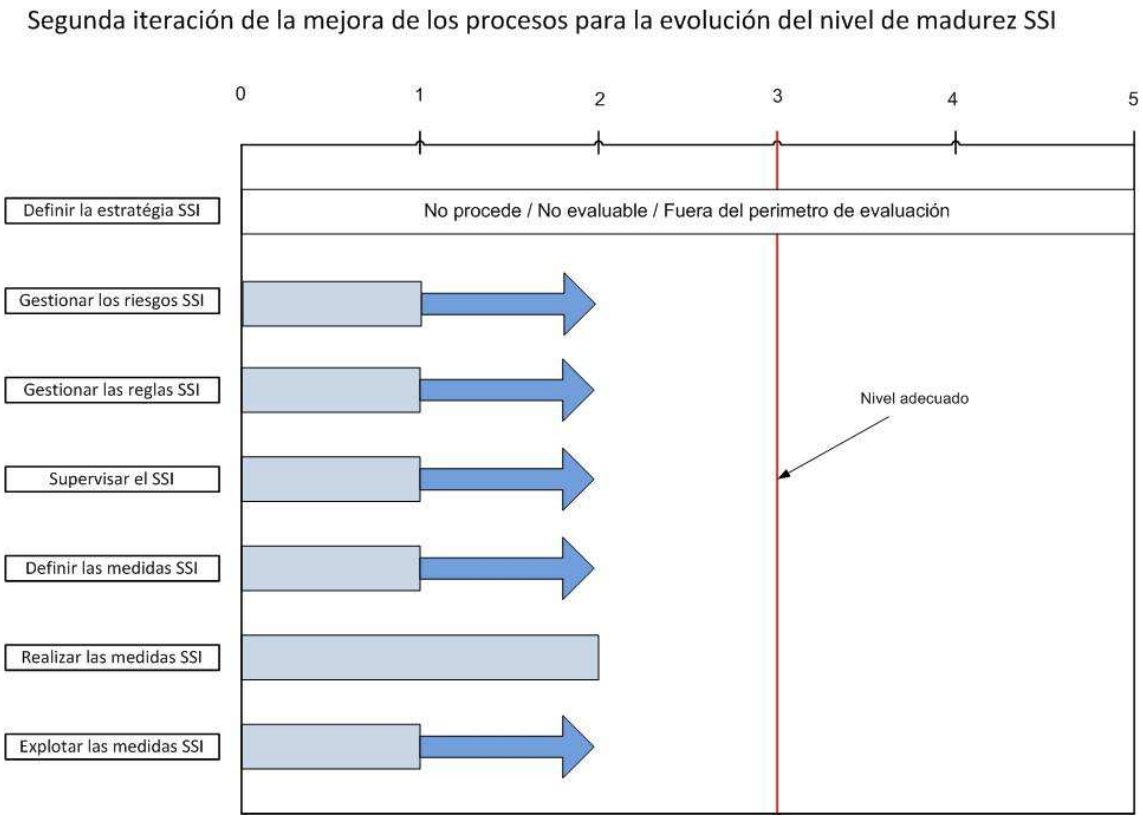


Figura 11. Segunda iteración para alcanzar el nivel de madurez

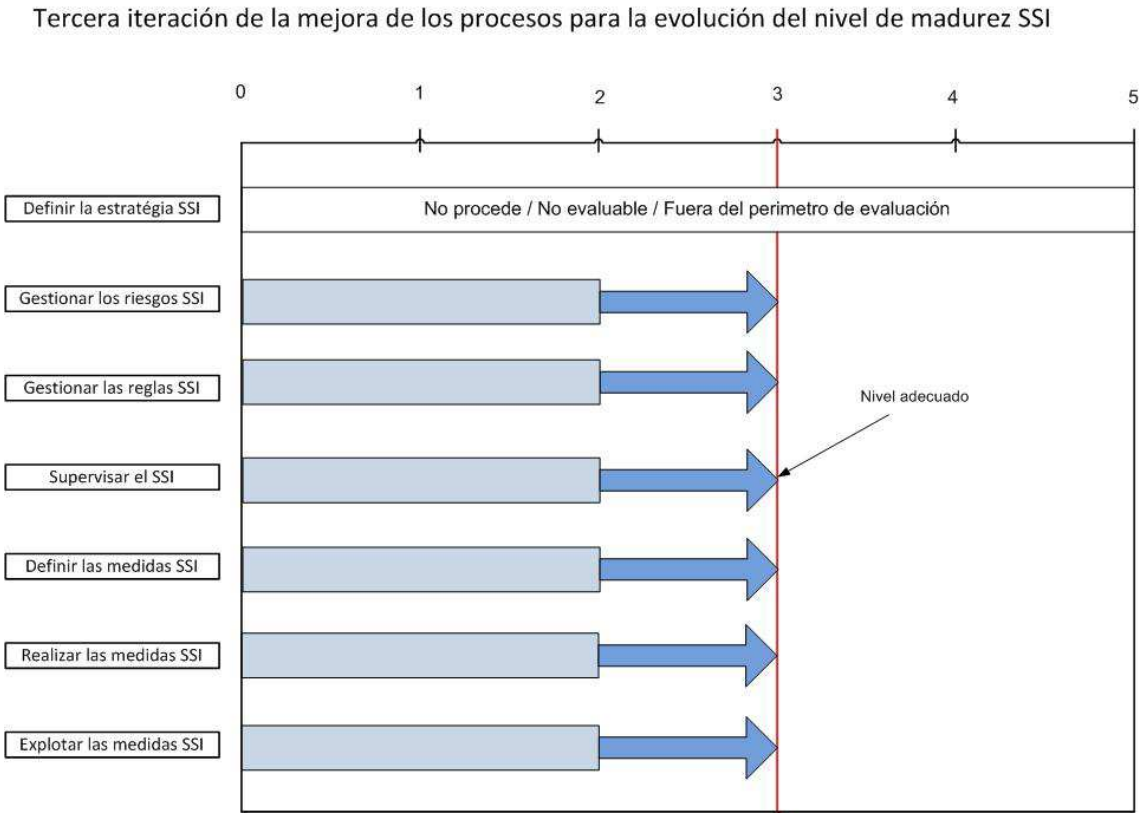


Figura 12. Tercera iteración para alcanzar el nivel de madurez

4.3.2 Fase 2: Evaluación. Aplicación del referencial

Para la elaboración de este punto se han tomado como referencia las fuentes citadas en el apartado 8.3 Metodología.

4.3.2.1 Introducción

En esta fase se pretende determinar cuál es el nivel efectivo de protección así como el grado de cumplimiento del estándar con el objetivo de definir una guía de implementación que permita adquirir el nivel adecuado de protección particular a cada empresa.

Las normas que se han utilizado como base para desarrollar esta fase son *The Critical Security Controls for Effective Cyber Defense, SANS (2013). Publicado en* http://www.sans.org/critical-security-controls/ [5] y *Controles ISO27002:2005*, ISO27000.es (2013) [1]

Esta fase se compone de dos puntos en los que se pretende evaluar el estado real de protección de los sistemas y el estado de cumplimiento del estándar.

Se han documentado los 20 controles y los 196 puntos de control de la norma de SANS con sus diferentes niveles de clasificación. Con estos niveles se ha realizado una correspondencia para poder determinar los niveles adecuado y efectivo definidos anteriormente.

Se han realizado cuestionarios para evaluar el cumplimiento de cada control y de cada punto de implementación. Estos cuestionarios cubren toda la norma en su extensión por lo que es difícilmente aplicable a todas las empresas y a todos sus contextos.

Utilizando el valor del nivel adecuado estimado en la fase anterior se pretende filtrar todas las cuestiones que no sean aplicables al tipo de empresa que se esté evaluando consiguiendo una notable reducción del proceso tanto en esta fase como en la posterior implementación.

Para ello se ha realizado una identificación de los niveles de las dos fases.

En esta norma se clasifican los diferentes controles por el nivel de mitigación de las amenazas en Muy Alto, Alto Medio y Bajo (VH, H, M, L).

Controles		
Mitigación		
VH	Muy Alta	M1
H	Alta	M2
M	Media	M3
L	Baja	M4

Tabla 16: Niveles de mitigación

Dentro de cada control se clasifican los puntos de implementación de los controles según la ganancia que aportan: Ganancia rápida, Visibilidad/Reconocimiento, Configuración/Higiene y Avanzada (QW, V/A, C/H, A).

Puntos de implementación		
Ganancia		
QW	Ganancia Rápida	G1
V/A	Visibilidad/Reconocimiento	G2
C/H	Configuración/Higiene	G3
A	Avanzado	G4

Tabla 17: Niveles de ganancia

Se ha realizado la siguiente asignación de niveles para identificar todos los puntos de implementación y controles.

Asignación de niveles	
N1	M1,M2(G1)
N2	M1,M2(G2)+M3(G1)
N3	M1,M2(G3)+M3(G2)+M4(G1)
N4	M1,M2(G4)+M3(G3,G4)+M4(G2,G3,G4)

Tabla 18: Asignación de niveles

Los 20 controles y su nivel de mitigación se presentan en la siguiente tabla, los niveles de implementación y sus ganancias se presentan ordenados en cada control en un documento anexo.

	Control	Mitigación
1	Inventario de dispositivos autorizados y no autorizados	VH
2	Inventario de Software autorizado y no autorizado	VH
3	Configuraciones seguras para Hardware y Software en dispositivos móviles, ordenadores portátiles, estaciones de trabajo y servidores	VH
4	Evaluación continua y corrección de vulnerabilidades	VH

5	Defensas de malware	H
6	Seguridad en aplicaciones software	H
7	Control de dispositivos inalámbricos	H
8	Capacidad de recuperación de datos	M
9	Habilidades de seguridad, evaluación y formación adecuadas	M
10	Configuraciones seguras para los dispositivos de red, tales como firewalls, routers y switches	H
11	Limitación de puertos de red, protocolos y servicios	H
12	Uso controlado de privilegios administrativos	H
13	Defensa perimetral	H
14	Mantenimiento, Monitoreo y Análisis de Log de registro	M
15	Acceso Controlado con base en la necesidad de conocer	M
16	Supervisión y control de cuentas	M
17	Prevención de pérdida de datos	M
18	Respuesta y manejo de Incidentes	M
19	Ingeniería de red segura	L
20	Pruebas de penetración y RedTeam	L

Tabla 19: 20 Controles críticos de seguridad

4.3.2.2 Referencial

En esta fase se realizarán diferentes cuestionarios a los responsables de los sistemas informáticos de las organizaciones o a sus equipos técnicos.

Estos cuestionarios se distribuyen en cuatro niveles y están ordenados para su aplicación. Dependiendo del nivel adecuado a la organización estimado en la fase anterior se deberán realizar todos los cuestionarios desde el nivel 1 hasta el nivel adecuado. La distribución por niveles tiene como objetivo reducir la fase de evaluación pero sobre todo reducir la fase de implementación.

A continuación se presentan los diferentes cuestionarios así como los puntos de implementación a los que hacen referencia, en estas tablas se identifica el código asociado a cada control o punto de implementación, su grado de mitigación y ganancia, una breve descripción y la cuestión asociada. La respuesta a cada cuestión será Si/No/No procede:

- **Cuestionarios para el Nivel 1:**

Nivel1				
Control		M/G	Controles	Cuestiones
1	VH	M1	Inventario de dispositivos autorizados y no autorizados	

1.1	QW	G1	Herramienta de descubrimiento de activos para construir un inventario. Herramientas activas (rango de ips) y pasivas (análisis de tráfico)	¿Se utilizan herramientas activas/pasivas para el descubrimiento de activos?
1.2	QW	G1	Implementar DHCP con registro, mejora del sistema de inventario y detección de sistemas desconocidos.	¿Se mantiene registro del sistema DHCP? ¿Se detectan sistemas desconocidos?
1.3	QW	G1	Control de cambios y adquisiciones.	¿Existe una gestión de altas y bajas en inventario? (cambios, adquisiciones)
2	VH	M1	Inventario de Software autorizado y no autorizado	
2.1	QW	G1	Implementar tecnología de control de software por listas blancas	¿Existe un control de software por listas blancas?
2.2	QW	G1	Elaborar listas de software permitido	¿Se gestionan listas blancas de SW?
2.3	QW	G1	Escaneo regular de software no autorizado y generación de alertas. Proceso estricto de control de cambios.	¿Existe un proceso de alerta y control estricto de software instalado?
3	VH	M1	Configuraciones seguras para Hardware y Software en dispositivos móviles, ordenadores portátiles, estaciones de trabajo y servidores	
3.1	QW	G1	Uso de configuraciones estándar seguras en SO y aplicaciones. Imágenes de SO endurecidas. Control de cambios.	¿Existe una política de configuraciones estándar seguras para SO, plantillas de despliegue y aplicaciones con control de cambios?
3.2	QW	G1	Implementar herramientas automatizadas de parcheo de SO y aplicaciones.	¿Se utiliza alguna herramienta para el parcheo de SO y aplicaciones?
3.3	QW	G1	Limitar privilegios administrativos a muy pocos usuarios con conocimientos y necesidades de negocio.	¿El uso de privilegios administrativos está limitado y aislado en todos los casos?
3.4	QW	G1	Utilización de imágenes para todos los equipos y gestión de configuración estricta.	¿Existen plantillas de imágenes de configuración estricta para el despliegue de equipos?
3.5	QW	G1	Custodia de las imágenes en servidores seguros y/o fuera de línea.	¿Estas imágenes están custodiadas en ubicaciones seguras y/o fuera de línea?
4	VH	M1	Evaluación continua y corrección de vulnerabilidades	
4.1	QW	G1	Programar y ejecutar herramientas de análisis de vulnerabilidades con entrega de listas a los administradores de sistemas.	¿Existen procesos programados de análisis de vulnerabilidades con entrega de informes y alertas?
4.2	QW	G1	Correlación de datos con la información de análisis.	¿La información del análisis está correlacionada?
4.3	QW	G1	Utilizar modo autenticado exclusivo en el análisis de vulnerabilidades.	¿El análisis de vulnerabilidades está protegido por autenticación exclusiva?
4.4	QW	G1	Subscripción y gestión a servicios de inteligencia de vulnerabilidades. Actualización de las herramientas.	¿Las herramientas de análisis de vulnerabilidades están convenientemente actualizadas?

5	H	M2	Defensas de malware	
5.1	QW	G1	Utilizar herramientas antivirus, antimalware, Firewalls personales e IPS basados en host en equipos, servidores y dispositivos móviles. Envío a servidores centralizados de registro y evaluación.	¿Se utilizan herramientas antivirus, antimalware, firewalls personales e IPS basados en host con registro y evaluación centralizados en servidor?

5.2	QW	G1	Emplear software antimalware de estructura centralizada con control de actualizaciones, reputación y gestión de cambios.	¿Se utiliza software centralizado con control de actualizaciones, reputación y gestión de cambios?
5.3	QW	G1	Configurar equipos para impedir la ejecución automática en dispositivos externos o extraíbles así como el montado automático de unidades.	¿La configuración de los equipos impide la ejecución automática de dispositivos externos y extraíbles así como el montado automático de unidades?
5.4	QW	G1	Configurar escaneo automático de dispositivos externos al insertarlos.	¿Está habilitado el escaneo automático de dispositivos externos?
5.5	QW	G1	Escanear y bloquear adjuntos de correo maliciosos o innecesarios para la organización antes de que sean descargados en los equipos. Filtrado de correo y de contenido web.	¿Está configurado el escaneo y bloqueo de contenidos web y correo?
5.6	QW	G1	Habilitar funciones anti-explotación y mitigación.	¿Están habilitadas funciones de anti explotación y mitigación?
5.7	QW	G1	Limitar el uso de dispositivos externos a las necesidades de negocio. Monitorizar el uso y el intento de uso de estos dispositivos.	¿Existen políticas definidas sobre el uso de dispositivos externos por necesidades de negocio? ¿Se monitoriza el uso o intento de uso?
6	H	M2	Seguridad en aplicaciones software	
6.1	QW	G1	Comprobar si las aplicaciones adquiridas tienen soporte del vendedor e instalar la versión más actual y parches.	¿Está gestionado el soporte de vendedor a las aplicaciones? ¿Hay un control de versiones y parches instalados?
6.2	QW	G1	Proteger las aplicaciones con cortafuegos específicos. WAF de aplicación o HIDS.	¿Las aplicaciones cuentan con protección específica como cortafuegos específicos, WAF de aplicación o HIDS?
7	H	M2	Control de dispositivos inalámbricos	
7.1	QW	G1	Asegurar que cada dispositivo inalámbrico tiene una configuración aprobada y un perfil de seguridad y denegar el acceso a dispositivos que no lo cumplan.	¿Todos los dispositivos inalámbricos poseen una configuración de seguridad aprobada y se deniega el acceso a los que no lo cumplen?
7.2	QW	G1	Configurar herramientas de escaneo para detectar dispositivos inalámbricos conectados a LAN. Conciliar los dispositivos detectados con permitidos y desactivar los no permitidos.	¿Existen herramientas de detección de dispositivos inalámbricos conectados a la red? ¿Existe un procedimiento de conciliación entre detectados y permitidos?
10	H	M2	Configuraciones seguras para los dispositivos de red, tales como firewalls, routers y switches	
10.1	QW	G1	Definir configuraciones seguras estándar para cada dispositivo de electrónica de red. Las configuraciones deben estar comprobadas, documentadas y debe existir un control de cambios.	¿Los dispositivos de red tienen configuraciones seguras? Deben estar comprobadas, documentadas y con control de cambios.
11	H	M2	Limitación de puertos de red, protocolos y servicios	
11.1	QW	G1	Asegurarse de que solo los puertos, protocolos y servicios con necesidades de negocio validadas se ejecutan en los equipos.	¿Están habilitados solamente los puertos, protocolos y servicios necesarios para el negocio en los equipos?
11.2	QW	G1	Aplicar cortafuegos basados en host con políticas de denegación por defecto.	¿Los hosts poseen cortafuegos con políticas de denegación por defecto?
11.3	QW	G1	Realizar análisis de puertos de manera regular con control de cambios y alerta.	¿Se realizan escaneos de puertos regularmente con control de cambios y alerta?

11.4	QW	G1	Mantener los servicios actualizados y desinstalar los componentes innecesarios.	¿Se mantienen los servicios actualizados y se desinstalan los componentes innecesarios en los equipos de la red?
12	H	M2	Uso controlado de privilegios administrativos	
12.1	QW	G1	Minimizar los privilegios administrativos y solo usarlos cuando se requiera. Implementar auditorías focalizadas en el uso de privilegios administrativos y monitorizar el comportamiento anómalo.	¿El uso de privilegios administrativos está minimizado? ¿Existen auditorias y métodos de monitorización para su control?
12.2	QW	G1	Utilizar herramientas automatizadas para el control de cuentas administrativas. Validar que las personas con privilegios administrativos están autorizadas por la dirección.	¿Se gestiona la autorización de cuentas privilegiadas por la dirección?
12.3	QW	G1	Configurar las contraseñas de las cuentas administrativas cumpliendo requisitos de complejidad y evitando palabras de diccionario.	¿Las cuentas administrativas cumplen los requisitos de complejidad?
12.4	QW	G1	Cambiar todas las contraseñas por defecto en equipos y aplicaciones antes de implementarlos en la red.	¿Se cambian las contraseñas por defecto de los equipos nuevos en la red?
12.5	QW	G1	Asegurarse de que las cuentas de servicio cumplen los requisitos de complejidad y las periodicidades de cambio.	¿Las cuentas de servicio cumplen requisitos de complejidad y cambio?
12.6	QW	G1	Las contraseñas deben almacenarse cifradas y hasheadas. Los archivos que las contienen solo deben ser editados por superusuarios.	¿Las contraseñas se almacenan cifradas y hasheadas?
12.7	QW	G1	Usar listas de control de acceso para asegurar que las cuentas administrativas se usan para labores administrativas. Debe impedirse el uso de aplicaciones de correo electrónico o navegadores con cuentas administrativas.	¿Las cuentas administrativas se utilizan para otros usos?
12.8	QW	G1	Cada persona que tenga acceso administrativo debe tener cuentas separadas con privilegios. Debe utilizarse administrador y root en situaciones de emergencia. Utilizar antes cuentas de dominio que locales.	¿Las personas con usos privilegiados utilizan cuentas diferentes para diferentes usos?
12.9	QW	G1	Configurar los sistemas para que no puedan reutilizarse contraseñas en 6 meses.	¿Está configurada la caducidad de todas las contraseñas?
13	H	M2	Defensa perimetral	
13.1	QW	G1	Limitar las comunicaciones con listas negras o listas blancas. Se realizaran pruebas periódicas.	¿Las comunicaciones están limitadas por listas negras/blancas? ¿Se testean periódicamente?
13.2	QW	G1	En redes DMZ utilizar sistemas de monitorización con integración IDS. Reenvío de eventos a un gestor de seguridad SIEM para su correlación.	¿Se utilizan en redes DMZ monitorización integrada con IDS y correlación con SIEM?

Tabla 20: Cuestionario nivel 1

- **Cuestionarios para el Nivel 2:**

Nivel 2				
Control		M/G	Controles	Cuestiones
8	M	M3	Capacidad de recuperación de datos	

8.1	QW	G1	Asegurar que se realizan copias de seguridad al menos una vez por semana y más frecuentes en datos críticos. Añadir copias de SO. El sistema de copias debe estar reglamentado y ser oficial.	¿Existe un sistema de copias de seguridad periódico que incluya todos los datos críticos reglamentado y oficial?
8.2	QW	G1	Se deben realizar pruebas periódicas de restauración para comprobar que el sistema de backup funciona correctamente.	¿Se realizan pruebas periódicas de restauración e integridad?
9	M	M3	Habilidades de seguridad, evaluación y formación adecuadas	
9.1	QW	G1	Realizar un análisis de las habilidades que poseen y necesitan los empleados y generar una hoja de ruta.	¿Los empleados poseen la formación necesaria en seguridad?
9.2	QW	G1	Formar y capacitar a los empleados. Realizar formación jerarquizada cuando sea posible. Cubrir vacíos mediante formación online o conferencias.	¿Se realiza formación específica en seguridad?
9.3	QW	G1	Implementar un programa de sensibilización. 5 puntos	¿Existe un programa de sensibilización en la empresa?
14	M	M3	Mantenimiento, Monitoreo y Análisis de Log de registro	
14.1	QW	G1	Incluir al menos dos fuentes de sincronización de tiempos (ej.: NTP) para cada servidor o dispositivo de red para que las marcas de tiempo sean consistentes.	¿Existen al menos dos fuentes NTP para marcas de tiempo consistentes?
14.2	QW	G1	Validar la configuración de registros para cada dispositivo hardware y para el software instalado en él incluyendo sello de tiempo, origen, destino así como descriptores de la transacción. Los registros deberán estar estandarizados o ser normalizados.	¿Están validadas las configuraciones de registros de cada dispositivo HW? ¿Están estandarizados o normalizados?
14.3	QW	G1	Asegurar que los sistemas de almacenamiento de registro tienen suficiente espacio y que son archivados y firmados sobre una base periódica.	¿Se comprueba que los sistemas de almacenamiento de registros tengan suficiente espacio y mantengan las marcas de tiempo y firma?
14.4	QW	G1	Desarrollar una política de retención de registros que permitan determinar con precisión los incidentes tras un periodo de tiempo. Las organizaciones pueden pasar meses sin detectar sistemas comprometidos.	¿Existe una política de retención de registros que permita el análisis tardío de eventos?
14.5	QW	G1	El personal de seguridad y sistemas debe realizar informes quincenales para identificar anomalías en los registros las cuales deben ser resueltas y documentadas.	¿Se realizan análisis e informes periódicos sobre identificación, resolución y documentación de anomalías?
15	M	M3	Acceso Controlado con base en la necesidad de conocer	
15.1	QW	G1	Ubicar la información sensible en VLANs separadas protegiendo el tráfico entre ellas con firewalls. El tráfico a través de redes no confiables debe estar cifrado.	¿La información sensible está separada por VLAN? ¿El flujo de datos entre redes sensibles está cifrado?
16	M	M3	Supervisión y control de cuentas	
16.1	QW	G1	Revisar todas las cuentas de los sistemas y deshabilitar aquellas que no estén asociadas a un propietario o proceso de negocio.	¿Se revisa periódicamente las cuentas de los sistemas y se deshabilitan las no asociadas a procesos de negocio?
16.2	QW	G1	Asegurar que todas las cuentas tienen una fecha de caducidad asociada.	¿Todas las cuentas tienen fecha de caducidad asociada?
16.3	QW	G1	Crear informes automáticos de los sistemas que incluyan cuentas cerradas, deshabilitadas, contraseñas sin caducidad o con duración máxima superada. El envío debe producirse de forma segura.	¿Se controla de forma automática las cuentas sin caducidad, cerradas o deshabilitadas?

16.4	QW	G1	Establecer procedimientos de revocación de acceso para usuarios que finalicen su relación con la organización. Deshabilitar las cuentas permite mantener las trazas de auditoría.	¿Existen procedimientos de revocación de derechos de usuarios? ¿Se mantienen las trazas de auditoria?
16.5	QW	G1	Monitorizar regularmente el uso de todas las cuentas y programar el cierre automático de sesiones por inactividad.	¿El uso de cuentas esta monitorizado? ¿Está programado el cierre automático por inactividad?
16.6	QW	G1	Configurar el bloqueo automático de pantalla para minimizar accesos no autorizados.	¿Están configurados los bloqueos automáticos de pantalla?
16.7	QW	G1	Supervisar el uso de cuentas inactivas y deshabilitarlas si no son necesarias. Documentar y monitorizar las excepciones.	¿El uso de cuentas inactivas o deshabilitadas está supervisado?
16.8	QW	G1	Exigir que las cuentas que no son administradores tengan contraseñas seguras con letras números y caracteres especiales. Caducidad mínima de 1 día, renovación a los 90 días y 15 contraseñas recordadas. Ajustable a negocio.	¿Se exigen requisitos de complejidad para las contraseñas de usuarios no administradores?
16.9	QW	G1	Configurar y utilizar bloqueo de cuentas por intentos fallidos de inicio de sesión. Definir tiempo estándar de bloqueo.	¿Está configurado el bloqueo de cuentas por intentos fallidos y el periodo de bloqueo?
17	M	M3	Prevención de pérdida de datos	
17.1	QW	G1	Implementar software de cifrado de disco duro en dispositivos móviles y equipos con datos sensibles.	¿Los equipos con datos sensibles y los dispositivos móviles tienen discos duros cifrados?
17.2	QW	G1	Verificar que los dispositivos y software de cifrado utilizan algoritmos públicamente investigados.	¿Las herramientas de cifrado utilizan algoritmos públicamente investigados?
17.3	QW	G1	Llevar a cabo una evaluación de los datos para identificar aquellos que requieren la aplicación de controles de cifrado e integridad.	¿Se ha realizado un análisis y evaluación de los datos que requieren cifrado?
17.4	QW	G1	Revisar las prácticas de protección de datos de los proveedores de servicios cloud.	¿Se revisan las prácticas de protección de datos de los proveedores de servicios cloud?
18	M	M3	Respuesta y manejo de Incidentes	
18.1	QW	G1	Asegurar que existen procedimientos escritos para el manejo de incidentes incluyendo definiciones del personal asignado. Deben definir las fases del manejo de los incidentes.	¿Existen procedimientos con personal asignado para el manejo de incidentes?
18.2	QW	G1	Asignar funciones relativas a la resolución de incidentes al personal	¿Están asignadas al personal las funciones relativas a la resolución de incidentes?
18.3	QW	G1	Definir personal de gestión que apoye la toma de decisiones en el manejo de incidentes informáticos.	¿Está definido el personal de gestión que apoye la toma de decisiones en el manejo de incidentes?
18.4	QW	G1	Elaborar normas en toda la organización para el tiempo de reporte, tipo de información y forma de reportar eventos. Debe haber conformidad a las normativas legales.	¿Existen normas sobre el tiempo de reporte de incidentes?
18.5	QW	G1	Montar y mantener información así como modo de contacto sobre incidentes de seguridad.	¿Existe información a disposición de los usuarios sobre los métodos para reportar incidentes?
18.6	QW	G1	Publicar información para todo el personal sobre incidentes o anomalías de	¿Se publica periódicamente información sobre incidentes y anomalías de

			seguridad. Debe estar incluido en las actividades de concienciación.	seguridad?

1	VH	M1	Inventario de dispositivos autorizados y no autorizados	
1.4	V/R	G2	Inventario extenso de los dispositivos conectados.	¿Existe un inventario extenso de dispositivos conectados?
2	VH	M1	Inventario de Software autorizado y no autorizado	
2.4	V/R	G2	Implementar herramientas de inventario de software en todos los equipos en todas sus versiones.	¿Hay herramientas de control de software e inventario en todos los equipos?
3	VH	M1	Configuraciones seguras para Hardware y Software en dispositivos móviles, ordenadores portátiles, estaciones de trabajo y servidores	
3.6	V/R	G2	Adquisición de sistemas pre configurados de forma segura.	¿Los sistemas se adquieren pre configurados de forma segura?
4	VH	M1	Evaluación continua y corrección de vulnerabilidades	
4.5	V/R	G2	Implementar herramientas de gestión de parches para SO y aplicaciones para todos los sistemas.	¿Existen herramientas de gestión y despliegue de parches para todos los SO y aplicaciones?
4.6	V/R	G2	Control y custodia de los registros asociados a los análisis y exploraciones.	¿Existe un método de control y custodia de los registros de análisis de vulnerabilidades?

5	H	M2	Defensas de malware	
5.8	V/R	G2	Ampliar la detección tradicional con detección de anomalías y heurística.	¿Están habilitadas la detección de anomalías o heurística?
5.9	V/R	G2	Utilizar herramientas anti-malware a nivel de red para evitar que lleguen a los equipos.	¿Se utilizan herramientas antimalware a nivel de red?
6	H	M2	Seguridad en aplicaciones software	
6.3	V/R	G2	Para aplicaciones desarrolladas in-house comprobar que las entradas de datos están documentadas y cumplen requerimientos de seguridad.	¿Existen aplicaciones desarrolladas in-house? ¿Están documentados los flujos de datos? ¿Cumplen los requerimientos de seguridad?
6.4	V/R	G2	Testear vulnerabilidades y DDOS en aplicaciones desarrolladas in-house y de terceros.	¿Se han testeado vulnerabilidades y DOS en aplicaciones in-house o de terceros?
6.5	V/R	G2	No mostrar mensajes de error a usuarios finales.	¿Se han deshabilitado los mensajes de error a usuarios finales?
6.6	V/R	G2	Mantener entornos separados para producción y no producción. Los desarrolladores no deben acceder a producción	¿Existen y están separados los entornos de producción y no producción? ¿Se impide el acceso a PRO a desarrolladores?
7	H	M2	Control de dispositivos inalámbricos	
7.3	V/R	G2	Utilizar WIDS para identificar dispositivos, detectar ataques y accesos exitosos. Además el tráfico que pasa a la red cableada debe ser supervisado.	¿Están implementadas herramientas de WIDS?

10	H	M2	Configuraciones seguras para los dispositivos de red, tales como firewalls, routers y switches	
11	H	M2	Limitación de puertos de red, protocolos y servicios	
11.5	V/R	G2	Eliminar o mover los servidores con visibilidad desde internet o en redes inseguras. Securizar aquellos con necesidades de negocio.	¿Los servidores con visibilidad desde internet se encuentran aislados y convenientemente securizados?
12	H	M2	Uso controlado de privilegios administrativos	
12.10	V/R	G2	Configurar registros y alertas cuando se añadan cuentas con privilegios o se muevan cuentas a/desde grupos privilegiados.	¿Existen registros y alertas para el movimiento o adición de cuentas privilegiadas?
12.11	V/R	G2	Configurar registros y alertas cuando se intenten accesos sin éxito de cuentas privilegiadas.	¿Existen registros y alertas para los accesos sin éxito a cuentas privilegiadas?
13	H	M2	Defensa perimetral	
13.3	V/R	G2	Implementar SPF en DNS para disminuir la posibilidad de recibir correos falsificados.	¿Se ha implementado SPF en DNS?
13.4	V/R	G2	Implementar sensores IDS en redes y sistemas para buscar ataques inusuales. Reactivo.	¿Existen sensores IDS en los diferentes segmentos de red?
13.5	V/R	G2	Desplegar dispositivos IPS para complementar IDS.	¿Se han desplegado dispositivos IPS?
13.6	V/R	G2	Configurar el perímetro para que todo el tráfico de aplicación a internet atraviese un proxy autenticado en DMZ.	¿El tráfico de internet atraviesa al menos un proxy autenticado en DMZ?
13.7	V/R	G2	Exigir a todos los accesos remotos de inicio de sesión autenticación en dos factores.	¿Los accesos remotos tienen al menos autenticación en dos factores?

Tabla 21: Cuestionario nivel 2

- **Cuestionarios para el Nivel 3:**

Nivel 3				
Control		M/G	Controles	Cuestiones
19	L	M4	Ingeniería de red segura	
19.1	QW	G1	Diseñar la red utilizando un mínimo de arquitectura en tres niveles (DMZ, middleware y red privada). Los sistemas con acceso a internet deben estar en DMZ y no contener datos sensibles. Estos estarán en la red privada pro detrás de un proxy de aplicación en middleware.	¿Existe una arquitectura de red en, al menos, tres niveles? ¿Los datos sensibles se encuentran en los niveles inferiores protegidos por firewalls o proxis?
20	L	M4	Pruebas de penetración y RedTeam	
20.1	QW	G1	Realizar pruebas de penetración periódicas tanto internas como externas para identificar vulnerabilidades o vectores de ataque.	¿Se realizan pruebas de penetración periódicas identificando vulnerabilidades y vectores de ataque?
20.2	QW	G1	Las cuentas de sistema o de usuario utilizadas para las pruebas deben ser controladas y supervisadas así como deshabilitadas tras su uso.	¿Se utilizan cuentas especiales para las pruebas? ¿Se deshabilitan al acabar las pruebas?

8	M	M3	Capacidad de recuperación de datos	

9	M	M3	Habilidades de seguridad, evaluación y formación adecuadas	
9.4	V/R	G2	Establecer un método para validar la concienciación (enlaces de correo, datos telefónicos, etc.) principalmente a víctimas potenciales.	¿Existe algún método para evaluar la concienciación?
14	M	M3	Mantenimiento, Monitoreo y Análisis de Log de registro	
14.6	V/R	G2	Activar el registro minucioso (verbose) para el tráfico que atraviesa los dispositivos fronterizos (proxy, firewall, IDS).	¿Está activado el registro minucioso (verbose) para los dispositivos fronterizos?
14.7	V/R	G2	Para todos los dispositivos, asegurar que los registros se escriben en servidores diferentes de los de recogida y con restricciones de edición o borrado reduciendo las posibilidades de manipulación.	¿Los sistemas de almacenamiento de registros son diferentes de los de recolección? ¿Está restringida su edición y manipulación?
14.8	V/R	G2	Implementación de un SIEM o herramientas de análisis de logs para la agregación, consolidación, correlación y análisis. Esto permitirá al personal de seguridad identificar rápidamente los eventos reales, evitar falsos positivos y filtrar gran cantidad de datos.	¿Está implementado un SIEM?
15	M	M3	Acceso Controlado con base en la necesidad de conocer	
15.2	V/R	G2	Establecer auditoría detallada en datos no públicos y autenticación especial en datos sensibles.	¿Está establecida una auditoría detallada para datos no públicos y autenticación especial para datos sensibles?
16	M	M3	Supervisión y control de cuentas	
16.10	V/R	G2	Conciliar empleados activos y proveedores con cuentas y desactivar las no asignadas.	¿Empleados, proveedores y cuentas se concilian periódicamente?
16.11	V/R	G2	Registro de auditoría y supervisión del uso de cuentas deshabilitadas.	¿Existen auditorías y supervisión para el uso de cuentas deshabilitadas?
17	M	M3	Prevención de pérdida de datos	
17.5	V/R	G2	Implementar una herramienta automatizada para monitorizar información sensible o palabras clave para descubrir intentos no autorizados de exfiltración. Configurar bloqueo y alertas.	¿Existen herramientas de monitorización, detección y alerta para descubrir intentos de exfiltración de datos?
17.6	V/R	G2	Controlar mediante herramientas la efectividad de uso del cifrado de datos sensibles. Buscar e identificar patrones, ficheros en texto plano con información sensible.	¿Se testea periódicamente la efectividad del uso del cifrado?
18	M	M3	Respuesta y manejo de Incidentes	

1	VH	M1	Inventario de dispositivos autorizados y no autorizados	
5	C/H	G3	Base de datos de inventario protegida y con copia de seguridad.	¿La base de datos de inventario está protegida y respaldada?
6	C/H	G3	Mapa de información crítica en activos hardware.	¿Existe un mapa de información crítica en activos HW?
7	C/H	G3	Autenticación 802.1x	¿Está implementada la autenticación 802.1x?
8	C/H	G3	Implementar control de acceso NAC.	¿Está implementado el acceso NAC?
9	C/H	G3	Aislar BYOD y dispositivos no confiables por VLAN.	¿Los dispositivos BYOD y no confiables se

				encuentran en redes aisladas?
2	VH	M1	Inventario de Software autorizado y no autorizado	
6	C/H	G3	Integración de la herramienta de inventario con el control de software así como la instalación de SW legítimo en equipos no autorizados.	¿Las herramientas de control de SW instalado y el inventario HW/SW están vinculadas?
7	C/H	G3	Despliegue de tecnología de listas blancas en dispositivos móviles.	¿Está implementada alguna tecnología de listas blancas en dispositivos móviles?
3	VH	M1	Configuraciones seguras para Hardware y Software en dispositivos móviles, ordenadores portátiles, estaciones de trabajo y servidores	
3.7	C/H	G3	Utilización de canales seguros para la administración de equipos.	¿Los equipos se administran por canales seguros?
3.8	C/H	G3	Utilizar herramientas de control de integridad e archivos críticos de sistema así como herramientas de trazabilidad y alerta efectiva.	¿Existen herramientas para el control de integridad de archivos críticos así como herramientas de trazabilidad y alerta efectiva?
3.10	C/H	G3	Implementar herramientas de propagado de configuraciones como AD en Windows o Puppets en Linux.	¿Están implementadas herramientas de propagación de configuración por directorio?
4	VH	M1	Evaluación continua y corrección de vulnerabilidades	
4.7	C/H	G3	Sistema de comprobación y/o aceptación de vulnerabilidades detectadas y tratadas.	¿Existen políticas y sistemas de comprobación y aceptación de vulnerabilidades detectadas y tratadas?
4.8	C/H	G3	Medición del GAP de parcheo de vulnerabilidades, definición de umbrales y contramedidas.	¿Se mide el GAP de parcheo de vulnerabilidades? ¿Están definidos umbrales y contramedidas?
4.9	C/H	G3	Evaluar los parches críticos en un entorno seguro y definir soluciones de atenuación en caso de no poder aplicar en producción.	¿Hay entornos de evaluación para los parches críticos? ¿Hay definidas soluciones de atenuación para casos no aplicables?
4.10	C/H	G3	Establecer una topología de aplicación de parches en función de los riesgos y el potencial impacto. Ejecutar por fases por prioridad.	¿Está establecida una topología de aplicación de parches en función de los riesgos y el potencial impacto? ¿Se aplican por fases?

5	H	M2	Defensas de malware	
6	H	M2	Seguridad en aplicaciones software	
6.7	C/H	G3	Utilizar herramientas de testeo para el software desarrollado tanto para el código como para los valores de entrada/salida.	¿Se han utilizado herramientas de testeo para el SW desarrollado y sus entradas de datos?
6.8	C/H	G3	Estudiar el proceso de seguridad de los proveedores de aplicación como parte del proceso global de la empresa.	¿Se ha estudiado el proceso de seguridad de los proveedores de aplicaciones?
6.9	C/H	G3	Utilizar plantillas de configuración estándar endurecidas para bases de datos y aplicaciones basadas en ellas. Testear los procesos críticos de negocio.	¿Existen plantillas de configuración endurecidas para bases de datos? ¿Se testean los procesos críticos de negocio?

6.10	C/H	G3	El personal de desarrollo debe recibir o estar capacitado en desarrollos seguros.	¿Los desarrolladores están capacitados y concienciados para realizar desarrollos seguros?
6.11	C/H	G3	Asegurarse de que las herramientas de desarrollo (scripts, debug code, tools) no se incluyen en el entorno de producción.	¿Se incluyen herramientas de desarrollo en el entorno de producción?
7	H	M2	Control de dispositivos inalámbricos	
7.4	C/H	G3	Configurar equipos para que accedan solo a las redes inalámbricas permitidas y que sean necesidades de negocio.	¿Se gestiona que los equipos conectados a las redes inalámbricas permitidas sean por necesidades de negocio?
7.5	C/H	G3	En aquellos equipos que no haya necesidad de uso de dispositivos inalámbricos, deshabilitarlos y proteger las configuraciones por contraseña.	¿Se encuentran deshabilitadas los dispositivos inalámbricos sin necesidad de uso y protegidos con contraseña?
7.6	C/H	G3	Asegurar que todo el tráfico inalámbrico utiliza cifrado (AES WPA2)	¿Está habilitado cifrado seguro AES WPA2?
7.7	C/H	G3	Asegurar que se utilizan protocolos de autenticación segura (EAP/TLS)	¿Se utilizan protocolos de autenticación segura EAP/TLS?
7.8	C/H	G3	Desactivar las capacidades p2p en equipos a menos que haya una necesidad de negocio documentada.	¿Están desactivadas las capacidades P2P en todos los equipos?
7.9	C/H	G3	Desactivar las capacidades bluetooth en equipos a menos que haya una necesidad de negocio documentada.	¿Están desactivadas las capacidades bluetooth en equipos sin necesidad documentada?
7.10	C/H	G3	Crear redes virtuales independientes (VLAN) para dispositivos BYOD o inseguros. El acceso a internet debe ser seguro y catalogado como no confiable.	¿Los dispositivos BYOD están aislados en VLAN y su acceso a internet catalogado como no seguro?
10	H	M2	Configuraciones seguras para los dispositivos de red, tales como firewalls, routers y switches	
10.2	C/H	G3	Todas aquellas configuraciones que difieran de la línea base endurecida de configuraciones deben quedar documentadas junto a la razón y el responsable de negocio.	¿Las variantes de configuración están documentadas junto al responsable de negocio?
10.3	C/H	G3	Utilizar herramientas automatizadas para comprobar configuraciones y controlar cambios. Las modificaciones deben ser reportadas al personal de seguridad.	¿Se utilizan herramientas automatizadas para el control de cambios con reporte?
10.4	C/H	G3	Administrar dispositivos de red con autenticación two-factors y sesiones cifradas.	¿Se administran los dispositivos con autenticación en dos factores?
10.5	C/H	G3	Instalar los últimos parches de seguridad.	¿Los equipos de red poseen los últimos parches de seguridad?
11	H	M2	Limitación de puertos de red, protocolos y servicios	
11.6	C/H	G3	Operar los servicios críticos en hosts diferentes (DNS, Archivo, correo electrónico, Web, BBDD)	¿Los servicios críticos se encuentran separados en hosts diferentes?
12	H	M2	Uso controlado de privilegios administrativos	
12.12	C/H	G3	Utilizar autenticación multifactor para acceso a cuentas privilegiadas.	¿Se utiliza acceso multifactor para el uso de cuentas privilegiadas?
12.13	C/H	G3	Cuando se utilice autenticación basada en certificados asegurar que están protegidos con contraseñas seguras, almacenamiento de confianza o	¿Están protegidos convenientemente los

			tokens HW.	certificados de autenticación?
12.14	C/H	G3	Impedir el acceso a máquinas con cuenta de administrador y permitir lo solo ha usuarios con registro. Utilizar los privilegios con escalado (sudo, runas)	¿Se impide el acceso externo con cuentas privilegiadas y solo se permite mediante escalado y registro?
13	H	M2	Defensa perimetral	
13.8	C/H	G3	Debe gestionarse la configuración, software instalado y niveles de parches de los dispositivos que se conecten remotamente. Se publicarán normas de mínimos.	¿Los equipos que se conectan remotamente cumplen las políticas de seguridad de la organización?
13.9	C/H	G3	Escanear periódicamente los canales con conexión de retorno a internet no autorizados (VPN, DialUp, Wifi).	¿Se escanean periódicamente los canales con conexión de retorno no autorizados?
13.10	C/H	G3	Segmentar las redes para limitar el acceso a información privilegiada a agentes externos (proveedores, subcontratistas) para evitar accesos o contagios.	¿La red está segmentada? ¿La información privilegiada se encuentra aislada en las redes internas?
13.13	C/H	G3	Desplegar herramientas de recolección y análisis de flujos en DMZ.	¿Existen herramientas de recolección y análisis de flujos en DMZ?

Tabla 22: Cuestionario nivel 3

- **Cuestionarios para el Nivel 4:**

Nivel 4				
Control		M/G	Controles	Cuestiones
19	L	M4	Ingeniería de red segura	
19.2	C/H	G3	Diseñar la red permitiendo métodos de respuesta rápida para el rápido despliegue de nuevas listas de control de acceso, reglas, firmas, bloqueos, blackholes u otras medidas defensivas.	¿El diseño de la red permite el despliegue rápido de defensas y contramedidas (actualizaciones, listas de control de acceso, reglas firmas, etc.)?
19.3	V/R	G2	Implementar una estructura jerárquica de DNS donde los equipos internos realicen las peticiones a servidores DNS de la intranet y estos escalen peticiones desconocidas a servidores en DMZ.	¿Se utilizan DNS internos con escalado jerárquico de peticiones?
19.4	C/H	G3	Segmentar la red en diferentes zonas de confianza para proporcionar un control más granular de los accesos a los sistemas y de los métodos de defensa.	¿La red está segmentada permitiendo un control granular de los accesos y de los métodos de defensa?
20	L	M4	Pruebas de penetración y RedTeam	
20.3	V/R	G2	Realizar ejercicios periódicos de Red Team para evaluar ataques y respuestas.	¿Se realizan ejercicios periódicos de Red Team?
20.4	V/R	G2	Incluir en las pruebas información o documentación que podrían ser útiles a los atacantes, diagramas de red, PenTest antiguos, emails o documentos de contraseñas, etc.	¿Se incluye documentación útil a los atacantes en las pruebas?
20.5	V/R	G2	Planear metas claras y ataques multi-vector (ingeniería social, explotación de la red, web) en las pruebas de penetración para una evaluación más realista.	¿Se planean objetivos claros en las pruebas de penetración?
20.6	C/H	G3	Utilizar el escaneo de vulnerabilidades y los test de penetración de forma conjunta para focalizar la obtención de resultados.	¿Se utilizan escaneos de vulnerabilidades y test de penetración de forma combinada?
20.7	A	G4	Idear un sistema de medida o puntuación para la comparación de	¿Existe un sistema de puntuación o normalización de los resultados que permita

			resultados en el tiempo.	la evaluación y el seguimiento?
20.8	A	G4	Crear un banco de pruebas para los test de penetración similar al entorno de producción para ataques más agresivos o sensibles.	¿Existe un entorno de pruebas similar al entorno de producción?

8	M	M3	Capacidad de recuperación de datos	
8.3	C/H	G3	Asegurar que las copias de seguridad se encuentran protegidas físicamente y cifradas cuando viajan por la red.	¿Las copias de seguridad se encuentran protegidas físicamente? ¿Están cifradas cuando viajan por la red?
8.4	C/H	G3	Asegurar que los sistemas de copia de seguridad tienen al menos un destino no direccionable por sistema operativo para protegerlos de ataques de cifrado (CryptoLocker)	¿Las copias tienen al menos un destino no direccionable para protegerlas de ataques?
9	M	M3	Habilidades de seguridad, evaluación y formación adecuadas	
9.5	C/H	G3	Evaluar las habilidades de seguridad para cada uno de los roles de misión crítica. Utilizar ejemplos prácticos.	¿Existe un método de evaluación para los roles de misión crítica?
14	M	M3	Mantenimiento, Monitoreo y Análisis de Log de registro	
14.9	A	G4	Monitorizar la creación de servicios y auditar determinados procesos. La utilización de procesos como psexec o la creación de nuevos servicios son algo inusual.	¿Se monitorizan y auditan la creación de servicios o la utilización de herramientas de administración de sistemas?
14.10	A	G4	Asegurar que el sistema de recogida no pierde eventos incluso en periodos de gran carga, desconexiones o ancho de banda limitado.	¿El sistema de recolección de eventos está asegurado ante la pérdida o fallo en la recolección?
15	M	M3	Acceso Controlado con base en la necesidad de conocer	
16	M	M3	Supervisión y control de cuentas	
16.12	C/H	G3	Configurar el acceso para todas las cuentas a través de un punto de acceso único.	¿Se utiliza punto de acceso único para todas las cuentas?
16.13	C/H	G3	Definir y controlar perfiles de uso de las cuentas de usuario por franjas horarias y por equipos. Registrar y alertar los usos inapropiados.	¿Están configurados perfiles de uso de cuentas y equipos por franjas horarias?
16.14	A	G4	Autenticación multi-factor para datos y equipos sensibles	¿Equipos y datos sensibles poseen autenticación multifactor?
16.15	A	G4	Para el acceso autenticado a servicios web pasar por un canal cifrado y mantener los ficheros de contraseñas almacenados de forma segura.	¿El acceso autenticado a servicios web pasa por canales cifrados? ¿Se almacenan los ficheros de contraseñas de forma segura?
16.16	A	G4	Utilizar canales cifrados para la transmisión de contraseñas.	¿La transmisión de contraseñas pasa por canales cifrados?
16.17	A	G4	Comprobar que todos los archivos de contraseñas están cifrados y haseados, solo son accesibles a administrador o root y está auditado el acceso a ellos.	¿Se comprueba periódicamente que todos los archivos de contraseñas están cifrados, haseados, auditados y con acceso a usuarios privilegiados?
17	M	M3	Prevención de pérdida de datos	
17.7	C/H	G3	Movimiento de datos sensibles entre redes cifrado.	¿El movimiento de datos sensibles entre redes está cifrado?
17.8	C/H	G3	Si no hay necesidad deshabilitar el uso de dispositivos USB. En caso de necesidad controlar el uso por identificación de dispositivo y	¿Está controlado el uso de dispositivos de

			mantener un inventario.	almacenamiento externo?
17.9	C/H	G3	Utilizar soluciones DLP basadas en red. Detectar y gestionar las anomalías.	¿Se ha implementado Data Loss Prevention para los datos y equipos sensibles?
17.10	C/H	G3	Solo permitir Autoridades de Certificación aprobadas. Revisar y verificar CPS y CP.	¿Las autoridades de certificación están aprobadas?
17.11	C/H	G3	Llevar a cabo una revisión anual de algoritmos y longitudes de clave en el uso de la protección de datos sensibles.	¿Se comprueba al menos anualmente los algoritmos y claves en el uso de información sensible?
17.12	A	G4	Supervisar todo el tráfico que sale de la organización y detectar usos indebidos de canales cifrados. Los atacantes suelen cifrar los canales de extrusión de datos. Hay que detectar y bloquear las conexiones no autorizadas.	¿Se supervisa el uso de canales cifrados no autorizados?
17.13	A	G4	Bloquear el acceso a webs conocidas de transferencia de ficheros y correo electrónico.	¿Se bloquea el acceso a webs de transferencia de ficheros y correo electrónico?
17.14	A	G4	Definir funciones y responsabilidades relacionadas con claves de cifrado de datos así como definir los ciclos de vida.	¿Están definidas las funciones y responsabilidades relacionadas con claves de cifrado? ¿Tienen definidos ciclos de vida?
17.15	A	G4	En su caso aplicar Hardware Security Modules (HSM) para la protección de claves privadas o de cifrado.	¿Se utiliza Hardware Security Modules para la protección de claves privadas o de cifrado en casos necesarios?
18	M	M3	Respuesta y manejo de Incidentes	
18.7	C/H	G3	Llevar a cabo sesiones periódicas con escenarios de incidentes para asegurarse de que las personas del equipo de gestión conoce y entienden las amenazas, los riesgos y las responsabilidades.	¿Se realizan pruebas periódicamente con el personal simulando escenarios de incidentes?

1	VH	M1	Inventario de dispositivos autorizados y no autorizados	
10	A	G4	Validación y autenticación por certificado.	¿Está implementada la autenticación por certificados?
2	VH	M1	Inventario de Software autorizado y no autorizado	
8	A	G4	Utilización de máquinas virtuales o Live para la ejecución de SW de riesgo.	¿El SW de riesgo está aislado en máquinas virtuales?
9	A	G4	Entornos de trabajo virtualizados y no persistentes fácilmente restaurables a una base periódica.	¿Existen procesos de restauración a sistema base para equipos virtualizados y no persistentes?
10	A	G4	Software con etiquetas de identificación	¿Se ha implementado alguna tecnología de etiquetas para la integridad del SW base?
3	VH	M1	Configuraciones seguras para Hardware y Software en dispositivos móviles, ordenadores portátiles, estaciones de trabajo y servidores	
3.9	A	G4	Implementar sistema de monitorización automática de cambios en elementos de configuración de seguridad. Alertas.	¿Está implementado un sistema de monitorización y alerta automática para los cambios en los elementos de seguridad?
4	VH	M1	Evaluación continua y corrección de vulnerabilidades	

5	H	M2	Defensas de malware	
5.10	A	G4	Implementar un procedimiento de respuesta a incidentes.	¿Se ha implementado un procedimiento de respuesta a incidentes?
5.11	A	G4	Habilitar detección de dominios C2 en DNS.	¿Está habilitada la detección de dominios C2 en DNS?
6	H	M2	Seguridad en aplicaciones software	
7	H	M2	Control de dispositivos inalámbricos	
10	H	M2	Configuraciones seguras para los dispositivos de red, tales como firewalls, routers y switches	
10.6	A	G4	Segmentación de redes basada en VLAN o separación física. Mantener el acceso de gestión en un segmento separado.	¿El acceso de gestión se mantiene en un segmento de red separado?
11	H	M2	Limitación de puertos de red, protocolos y servicios	
11.7	A	G4	Colocar WAF frente a los servidores críticos. El tráfico no autorizado debe ser bloqueado y generar una alerta.	¿Los servidores críticos están protegidos por firewalls específicos de aplicación?
12	H	M2	Uso controlado de privilegios administrativos	
13	H	M2	Defensa perimetral	
13.11	A	G4	Minimizar la posibilidad de que un atacante pivote entre redes filtrando el tráfico a redes privadas mediante proxy de aplicación o firewalls.	¿El tráfico entre redes está filtrado mediante proxis o firewalls?
13.12	A	G4	Para ayudar a identificar canales encubiertos, activar los mecanismos integrados de detección de sesiones largas en firewalls.	¿Están activados la detección de detección de sesiones largas en firewalls para detectar canales encubiertos?

Tabla 23: Cuestionario nivel 4

4.3.2.3 Cumplimiento.

Para muchas organizaciones es importante determinar cuál es el nivel de cumplimiento del estándar. Esto aporta un nivel complementario de normalización a la metodología presentada.

Se han documentado los dominios (11), objetivos de control (39) y controles de *Controles ISO27002:2005*, ISO27000.es (2013) [1] y se han generado cuestionarios para determinar el grado de cumplimiento. Las diferentes cuestiones se han formulado para responderse con Si/No/No procede.

El cuestionario debe ser contestado por el responsable de sistemas informáticos de la organización o su equipo técnico. En este caso se ha decidido no organizar por niveles los controles ya que el objetivo en este caso es informar del grado de cumplimiento.

A continuación se presentan los cuestionarios donde se identifican los dominios, objetivos de control y controles asociados:

Dominios		Objetivos de Control		Controles		Cuestiones
5	Política de Seguridad	1	Política de seguridad de la información	1	Documento de política de seguridad de la información	¿Existe un documento de política de seguridad de la información?
				2	Revisión de la política de seguridad de la información	¿Este documento se revisa periódicamente?
6	Aspectos organizativos de la seguridad de la información	1	Organización interna	1	Comité de gestión de seguridad de la información	¿Están claramente asignadas las responsabilidades en la gestión de la seguridad de la información?
				2	Coordinación de seguridad de la información	¿Las actividades SSI están coordinadas por miembros relevantes de la organización?
				3	Asignación de responsabilidades para la seguridad de la información	¿Están claramente definidas las responsabilidades SSI?
				4	Proceso de autorización de recursos para el tratamiento de la información	¿Existe un proceso de autorización para los nuevos recursos de tratamiento de la información?
				5	Acuerdos de confidencialidad	¿Están identificados y se revisan periódicamente los acuerdos de confidencialidad?
				6	Contacto con las autoridades	¿Se mantienen contactos con las autoridades pertinentes?
				7	Contacto con organizaciones de especial interés	¿Se mantiene contacto con grupos o foros de seguridad especializados y asociaciones profesionales?
				8	Revisión independiente de la seguridad de la información	¿La gestión de SSI se revisa de forma independiente?
		2	Terceros	1	Identificación de los riesgos derivados del acceso de terceros	¿Están identificados los accesos de terceros a los SI y los riesgos asociados?
				2	Tratamiento de la seguridad en la relación con los clientes	¿Están informados los clientes de todos los requisitos de seguridad en el acceso a los SI?
				3	Tratamiento de la seguridad en contratos con terceros	¿Están cubiertos todos los requisitos de seguridad en los acuerdos con terceros que impliquen acceso, procesamiento o gestión de la información?
7	Gestión de Activos	1	Responsabilidad sobre los activos	1	Inventario de activos.	¿Existe un inventario donde estén claramente identificados todos los activos?
				2	Responsable de los activos.	¿Está claramente definido el responsable del inventario de activos SI?
				3	Acuerdos sobre el uso aceptable de los activos.	¿Está identificado y documentado el uso de activos asociados a recursos SI?
		2	Clasificación de la información	1	Directrices de clasificación.	¿Existe una clasificación de la información en relación a su valor, requisitos legales, sensibilidad y criticidad para la Organización?
				2	Marcado y tratamiento de la información.	¿Existe un conjunto apropiado de procedimientos para el etiquetado y tratamiento de la información?
8	Seguridad ligada a los recursos humanos	1	Antes del empleo	1	Inclusión de la seguridad en las responsabilidades laborales.	¿Están definidos y documentados los roles y responsabilidades de la seguridad de los empleados, contratistas y terceros en concordancia con la política de seguridad de la información de la organización?
				2	Selección y política de personal.	¿Se revisan y verifican los antecedentes y perfiles de candidatos de empleo, contratistas y terceros?

				3	Términos y condiciones de la relación laboral.	¿Están definidas y aceptadas mutuamente las obligaciones para la seguridad de la información?
		2	Durante el empleo	1	Supervisión de las obligaciones.	¿Se supervisa que todas las partes sean conscientes de las amenazas, responsabilidades y obligaciones en seguridad de la información?
				2	Formación y capacitación en seguridad de la información.	¿Todas las partes han recibido la formación adecuada en SSI?
				3	Procedimiento disciplinario.	¿Existe un proceso disciplinario para los empleados que produzcan brechas de seguridad?
		3	Cese del empleo o cambio de puesto de trabajo	1	Cese de responsabilidades.	¿Está garantizado que los actores abandonan su relación con la organización de forma ordenada?
				2	Restitución de activos.	¿Está garantizado que los actores devuelven los activos cuando abandonan la organización?
				3	Cancelación de permisos de acceso.	¿Se retiran los derechos de acceso a los diferentes actores cuando abandonan la organización?
9	Seguridad física y del entorno	1	Áreas seguras	1	Perímetro de seguridad física.	¿Está definido un perímetro de seguridad física para los activos SI?
				2	Controles físicos de entrada.	¿Las áreas de seguridad están protegidas por controles de entrada?
				3	Seguridad de oficinas, despachos y recursos.	¿Existe seguridad física para oficinas, despachos y recursos?
				4	Protección contra amenazas externas y del entorno.	¿Existen medidas de protección física contra agresiones del entorno (incendios, inundaciones, etc.)?
				5	El trabajo en áreas seguras.	¿Está diseñada y se aplican pautas de seguridad para el trabajo en áreas seguras?
				6	Áreas aisladas de carga y descarga.	¿Las áreas de carga y descarga están controladas y aisladas de los recursos SI?
		2	Seguridad de los equipos	1	Instalación y protección de equipos.	¿Los equipos se encuentran protegidos y aislados de agresiones del entorno o accesos no autorizados?
				2	Suministro eléctrico.	¿Los equipos están protegidos contra fallos de suministro eléctrico?
				3	Seguridad del cableado.	¿El cableado está protegido contra daños o posibles interceptaciones de datos?
				4	Mantenimiento de equipos.	¿Existe un mantenimiento adecuado de los equipos que garantice su disponibilidad e integridad?
				5	Seguridad de equipos fuera de los locales de la Organización.	¿Se aplican métodos específicos de seguridad para equipos que se encuentran fuera de los locales de la organización?
				6	Seguridad en la reutilización o eliminación de equipos.	¿Se revisan convenientemente los equipos antes de su reutilización o destrucción?
				7	Traslado de activos.	¿Los equipos que salen de los locales de la organización tienen la autorización pertinente?
10	Gestión de comunicaciones y operaciones	1	Procedimientos y responsabilidades de operación	1	Documentación de procedimientos operativos	¿Existe documentación sobre os procedimientos de seguridad a disposición d los usuarios?
				2	Control de cambios operacionales	¿Se gestiona el control de cambios operacionales?

				3	Segregación de tareas	¿Las tareas y áreas de responsabilidad están segregadas?
				4	Separación de los recursos para desarrollo y producción	¿Están separados los entornos de desarrollo de los de producción?
		2	Supervisión de los servicios contratados a terceros	1	Prestación de servicios	¿Se garantizan los controles de seguridad adecuados a la prestación de servicios externos?
				2	Monitorización y revisión de los servicios contratados	¿Los controles de seguridad de servicios externos se monitorizan y revisan periódicamente?
				3	Gestión de los cambios en los servicios contratados	¿Existe una gestión de cambios para los servicios contratados?
		3	Planificación y aceptación del sistema	1	Planificación de capacidades	¿Está monitorizados y previstos los requisitos de los sistemas?
				2	Aceptación del sistema	¿Están establecidos criterios de aceptación para la incorporación de nuevos sistemas?
		4	Protección contra software malicioso y código móvil	1	Medidas y controles contra software malicioso	¿Existen controles de detección, prevención y recuperación ante ataques de software malicioso?
				2	Medidas y controles contra código móvil	¿Existe un control para le ejecución de código móvil? ¿Se impide la ejecución de código no autorizado?
		5	Gestión interna de soportes y recuperación	1	Recuperación de la información	¿Se realiza periódicamente copias de seguridad de la información conforme a las políticas de recuperación?
		6	Gestión de redes	1	Controles de red	¿Existen métodos de control, monitorización y protección de redes?
				2	Seguridad en los servicios de red	¿Se extienden las características de seguridad de redes a los servicios externos?
		7	Utilización y seguridad de los soportes de información	1	Gestión de soportes extraíbles	¿Existen procedimientos para la gestión de medios extraíbles?
				2	Eliminación de soportes	¿Existen procedimientos formales para la eliminación de medios?
				3	Procedimientos de utilización de la información	¿Existen procedimientos para la manipulación y almacenamiento de la información?
				4	Seguridad de la documentación de sistemas	¿La documentación de los sistemas está protegida?
		8	Intercambio de información y software	1	Políticas y procedimientos de intercambio de información y software	¿Existen procedimientos formales para el intercambio de información en medios de comunicación?
				2	Acuerdos de intercambio	¿Existen acuerdos para los intercambios de información con entidades externas?
				3	Soportes físicos en tránsito	¿Están protegidos los medios físicos y soportes en tránsito?
				4	Mensajería electrónica	¿La mensajería electrónica está protegida convenientemente?
				5	Sistemas de información empresariales	¿Está protegida la información asociada a la interconexión de sistemas?
		9	Servicios de comercio electrónico	1	Seguridad en comercio electrónico	¿Está protegida la información involucrada en servicios de comercio electrónico?
				2	Seguridad en transacciones en línea	¿Está protegida la información involucrada en transacciones en línea?

				3	Seguridad en información pública	¿Está protegida la información puesta a disposición en sistemas de acceso público?
		10	Monitorización	1	Registro de incidencias	¿Se mantienen los registros de auditoría por un período definido?
				2	Seguimiento del uso de los sistemas	¿Están establecidos y se revisan regularmente métodos de monitorización de los sistemas?
				3	Protección de los registros de incidencias	¿Están protegidos convenientemente los sistemas de monitorización y alerta?
				4	Diarios de operación del administrador y operador	¿Están registradas y monitorizadas las operaciones de las cuentas privilegiadas?
				5	Registro de fallos	¿Existe una gestión apropiada de las averías?
				6	Sincronización de reloj	¿Están sincronizados todos los relojes de los sistemas con fuentes autorizadas de tiempo?
11	Control de acceso	1	Requisitos de negocio para el control de accesos	1	Política de control de accesos	¿Está establecida y documentada una política de control de acceso a la información?
		2	Gestión de acceso de usuario	1	Registro de usuario	¿Existe una auditoría sobre la gestión de cuentas de usuario?
				2	Gestión de privilegios	¿Está restringida y controlada la asignación de privilegios?
				3	Gestión de contraseñas de usuario	¿Existen procedimientos formales para la gestión de contraseñas de usuario?
				4	Revisión de los derechos de acceso de los usuarios	¿Se revisan regularmente los derechos de acceso de los usuarios?
		3	Responsabilidades del usuario	1	Uso de contraseña	¿Se exige a los usuarios el uso de buenas prácticas en la gestión de contraseñas?
				2	Equipo informático de usuario desatendido	¿El usuario garantiza la seguridad de los equipos desatendidos?
				3	Políticas para escritorios y monitores sin información	¿Existe una política de escritorios y monitores sin información?
		4	Control de acceso en red	1	Política de uso de los servicios de red	¿Se provee a los usuarios únicamente los servicios de red a los que se les ha autorizado?
				2	Autenticación de usuario para conexiones externas	¿Existen métodos adecuados para el acceso de usuarios a conexiones externas?
				3	Autenticación de nodos de la red	¿Se utilizan métodos de identificación de equipos como método de autenticación?
				4	Protección a puertos de diagnóstico remoto	¿Se controla el acceso a puertos de diagnóstico remoto?
				5	Segregación en las redes	¿Las redes están segregadas?
				6	Control de conexión a las redes	¿Existe un control para el establecimiento de conexiones de usuarios en las redes?
				7	Control de encaminamiento en la red	¿Existen controles de enrutamiento en las redes conforme a las políticas de seguridad?

		5	Control de acceso al sistema operativo	1	Procedimientos de conexión de terminales	¿Existen procesos seguros de conexión a terminales?
				2	Identificación y autenticación de usuario	¿Existen procedimientos seguros de identificación y autenticación de usuario?
				3	Sistema de gestión de contraseñas	¿Existen sistemas adecuados para la gestión de contraseñas?
				4	Uso de los servicios del sistema	¿Está restringido y controlado el uso de servicios del sistema?
				5	Desconexión automática de terminales	¿Existen procedimientos de desconexión automática de terminales?
				6	Limitación del tiempo de conexión	¿Existen procedimientos para la limitación del tiempo de conexión?
		6	Control de acceso a las aplicaciones	1	Restricción de acceso a la información	¿Está protegido y gestionado el acceso a la información y funciones en sistemas de aplicaciones?
				2	Aislamiento de sistemas sensibles	¿Los sistemas sensibles están aislados?
		7	Informática móvil y tele trabajo	1	Informática móvil	¿Están establecidos métodos de protección para informática móvil?
				2	Tele trabajo	¿Están desarrolladas e implantadas políticas específicas de operación para el teletrabajo?
12	Adquisición, desarrollo y mantenimiento de sistemas de información	1	Requisitos de seguridad de los sistemas	1	Análisis y especificación de los requisitos de seguridad	¿Se especifican las demandas de seguridad para la incorporación o mejora de sistemas?
		2	Seguridad de las aplicaciones del sistema	1	Validación de los datos de entrada	¿Se valida que los datos de entrada sean correctos y apropiados?
				2	Control del proceso interno	¿Existen herramientas de chequeo de integridad de los datos en los procesos internos?
				3	Autenticación de mensajes	¿Existen herramientas de chequeo de integridad de los mensajes en los procesos internos?
				4	Validación de los datos de salida	¿Existen herramientas de chequeo de integridad de los datos de salida?
		3	Controles criptográficos	1	Política de uso de los controles criptográficos	¿Existe una política de uso de controles criptográficos?
				2	Cifrado	¿Se ha establecido una gestión de las claves que respaldan los métodos de cifrado?
		4	Seguridad de los ficheros del sistema	1	Control del software en explotación	¿Existen procedimientos de control de software en entornos de explotación?
				2	Protección de los datos de prueba del sistema	¿Están seleccionados, protegidos y controlados cuidadosamente los datos utilizados para las pruebas?
				3	Control de acceso a la librería de programas fuente	¿Está restringido y controlado el acceso a las librerías fuente de los programas?
		5	Seguridad en los procesos de desarrollo y soporte	1	Procedimientos de control de cambios	¿Existen procedimientos formales para el control de cambios en entornos de desarrollo y soporte?
				2	Revisión técnica de los cambios en el sistema operativo	¿Se revisan y aprueban los cambios en entornos de sistemas críticos?
				3	Restricciones en los cambios a los paquetes de software	¿Se desaconsejan los cambios en los paquetes de software?

				4	Canales encubiertos y código Troyano	¿Se previene el uso de canales encubiertos y código troyano?
				5	Desarrollo externalizado del software	¿Se supervisa y controla las especificaciones de seguridad en el desarrollo realizado por terceros?
		6	Gestión de las vulnerabilidades técnicas	1	Control de las vulnerabilidades técnicas	¿Están establecidos los procedimientos adecuados para el control de vulnerabilidades?
13	Gestión de incidentes en la seguridad de la información	1	Comunicación de eventos y debilidades en la seguridad de la información	1	Comunicación de eventos en seguridad	¿Se garantiza la comunicación adecuada de los eventos de seguridad?
				2	Comunicación de debilidades en seguridad	¿Existen procedimientos de comunicación ante la detección de debilidades?
		2	Gestión de incidentes y mejoras en la seguridad de la información	1	Identificación de responsabilidades y procedimientos	¿Están correctamente definidos y establecidos las responsabilidades y procedimientos ante la gestión de incidentes?
				2	Evaluación de incidentes en seguridad	¿Existe un mecanismo para evaluar la afectación de los incidentes de seguridad?
				3	Recogida de pruebas	¿Existen procedimientos regularizados para la recogida de pruebas?
14	Gestión de la continuidad de negocio	1	Aspectos de la gestión de continuidad del negocio	1	Proceso de la gestión de continuidad del negocio	¿Existe un proceso de gestión de la continuidad de negocio?
				2	Continuidad del negocio y análisis de impactos	¿Se evalúan los evento, su probabilidad así como el impacto que puede producir la interrupción del negocio?
				3	Redacción e implantación de planes de continuidad	¿Existen planes de mantenimiento y recuperación de procesos de negocio tras una interrupción?
				4	Marco de planificación para la continuidad del negocio	¿Existe un esquema único que garantice la consistencia de los planes de continuidad de negocio?
				5	Prueba, mantenimiento y reevaluación de planes de continuidad	¿Se prueban, mantienen y reevalúan los planes de continuidad de negocio?
15	Cumplimiento	1	Conformidad con los requisitos legales	1	Identificación de la legislación aplicable	¿Está identificada la legislación aplicable?
				2	Derechos de propiedad intelectual (IPR)	¿Están implementados los procedimientos adecuados que garanticen la protección de la propiedad intelectual?
				3	Salvaguarda de los registros de la Organización	¿Están convenientemente protegidos los registros de la organización?
				4	Protección de datos de carácter personal y de la intimidad de las personas	¿Se garantiza la protección de la privacidad de los datos de carácter personal?
				5	Evitar mal uso de los dispositivos de tratamiento de la información	¿Se restringe el mal uso de los dispositivos de tratamiento de la información?
				6	Reglamentación de los controles de cifrados	¿Los controles de cifrado están conformes a las normativas y regulaciones pertinentes?
		2	Revisiones de la política de seguridad y de la conformidad técnica	1	Conformidad con la política de seguridad	¿La dirección de la organización asegura que los procedimientos de seguridad cumplen la normativa en su área de gestión?
				2	Comprobación de la conformidad técnica	¿Se comprueba regularmente la conformidad de los procedimientos con normas y estándares?

		3	Consideraciones sobre la auditoria de sistemas	1	Controles de auditoria de sistemas	¿El uso de controles de auditoría está convenientemente integrado con los sistemas para producir la mínima intrusión?
				2	Protección de las herramientas de auditoria de sistemas	¿El uso de herramientas de auditoría está convenientemente protegido?

Tabla 24: Cuestionario de cumplimiento ISO 27002

4.3.3 Fase 3: Presentación de resultados. Informes

Con los resultados de los cuestionarios se realizarán varios informes.

En primer lugar un informe a modo de síntesis que recoja los valores estadísticos del grado de protección y las conclusiones desprendidas de estos.

El segundo informe recogerá el detalle de los diferentes controles que no se cumplen y que deberían estar implementados en la organización. Este informe será la base para el establecimiento del nivel adecuado de protección.

A partir de los resultados del cuestionario de ISO 27002 se presentará un tercer informe con el resumen y las conclusiones sobre el grado de cumplimiento del estándar.

4.3.4 Fase 4: Implementación del nivel adecuado de seguridad. Hoja de ruta.

Una vez determinado el nivel efectivo de protección y las necesidades prácticas para conseguir el nivel adecuado pasamos a la Fase 3 en donde se definirá el método para implementar los controles necesarios.

Para el proceso de implantación se ha utilizado un método similar al definido en el punto 3 de la fase de análisis en donde se consiguen los diferentes niveles mejorando los niveles más bajos de forma iterativa.

Partiendo de los cuestionarios implementados en la fase anterior, se filtrarán aquellos controles y puntos de implementación ya cubiertos y que no procedan. La tabla resultante, manteniendo el orden y agrupamiento presentado en la fase anterior, será la que se utilice para definir las diferentes fases de la hoja de ruta del proceso de implementación del nivel adecuado.

A continuación se presenta el método de iteraciones sucesivas. En este método se parte desde el nivel más bajo de protección. Dentro de él se acometerán primero las tareas de los controles que impliquen un mayor nivel de mitigación y dentro de estos, a su vez los niveles más altos de ganancia. Con esto se maximizamos la inversión tanto de recursos como de tiempo o personal consiguiendo los mayores resultados en las primeras fases y de la forma más rápida posible.

- **Proceso para alcanzar el nivel 1**

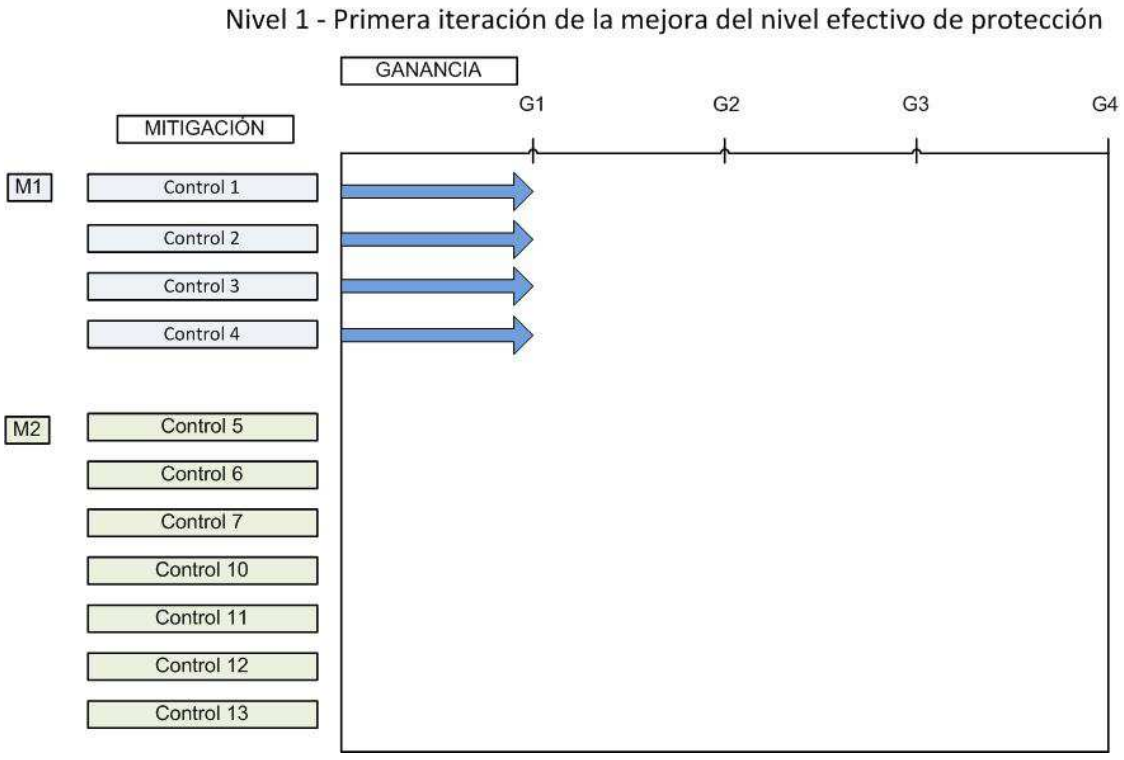


Figura 13. Primera iteración para alcanzar el nivel 1 efectivo

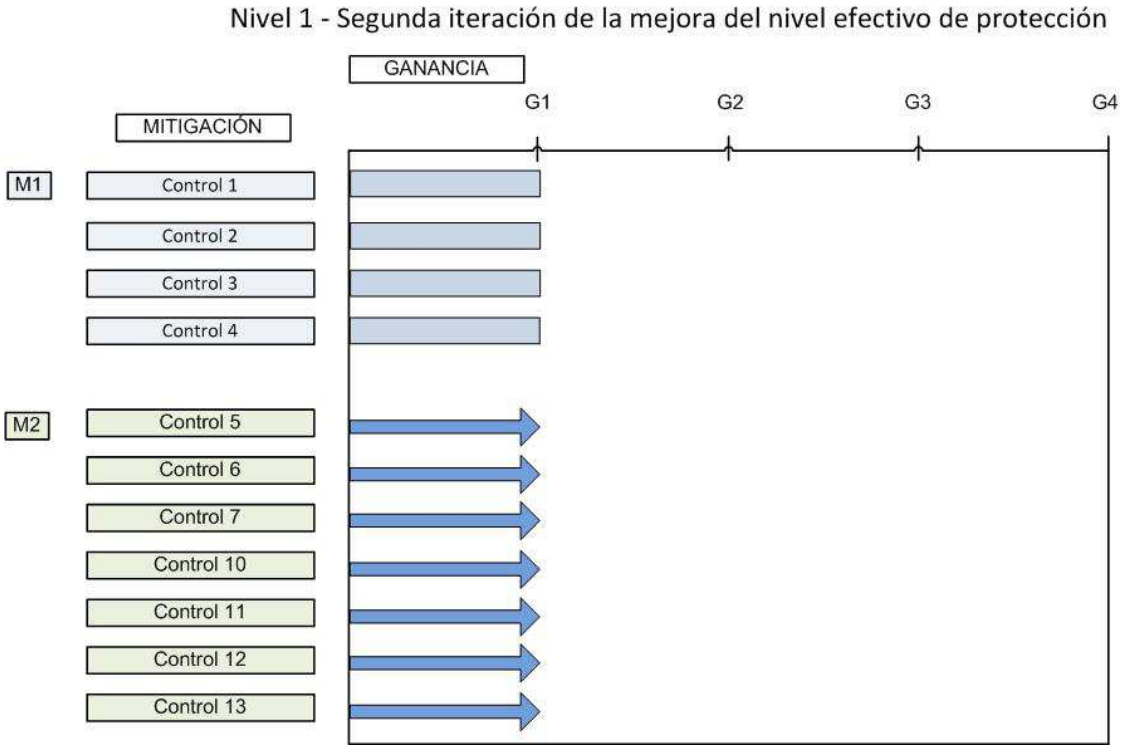


Figura 14. Segunda iteración para alcanzar el nivel 1 efectivo

- **Proceso para alcanzar el nivel 2**

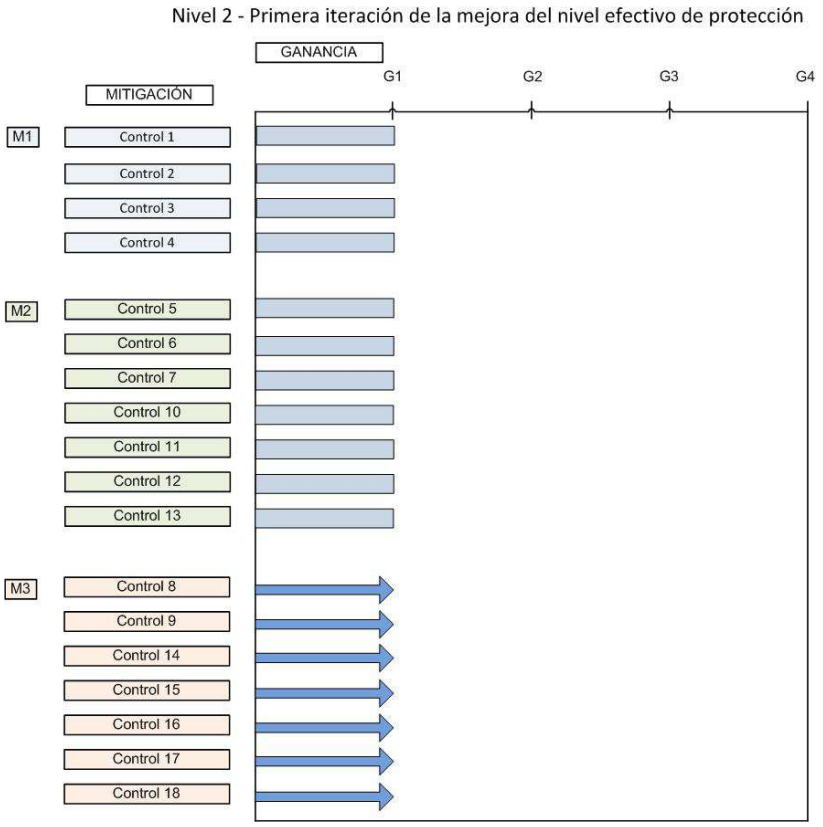


Figura 15. Primera iteración para alcanzar el nivel 2 efectivo

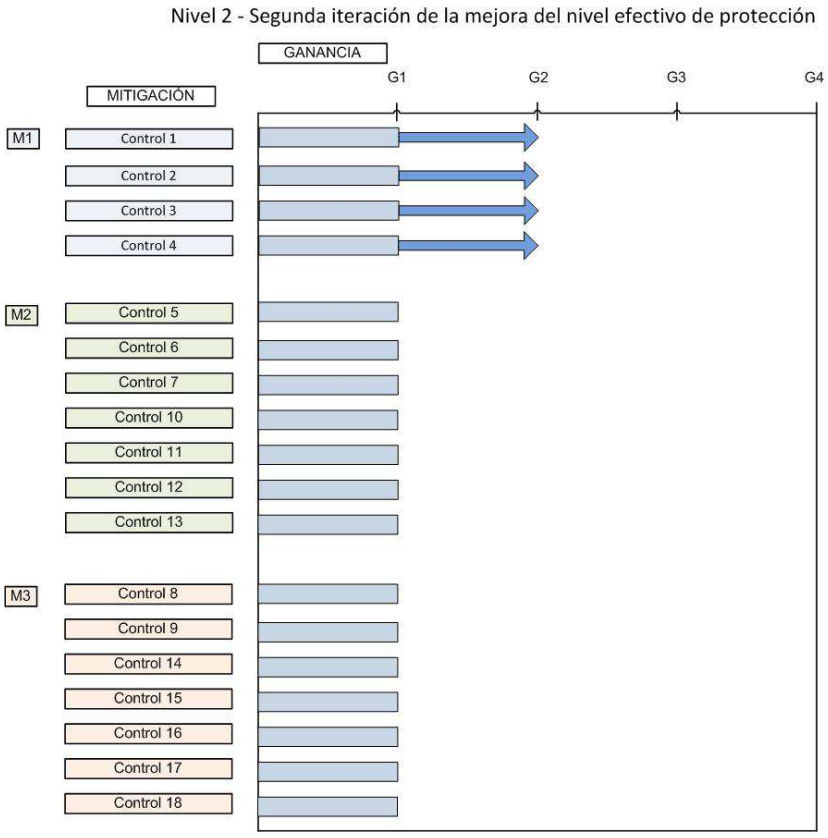


Figura 16. Segunda iteración para alcanzar el nivel 2 efectivo

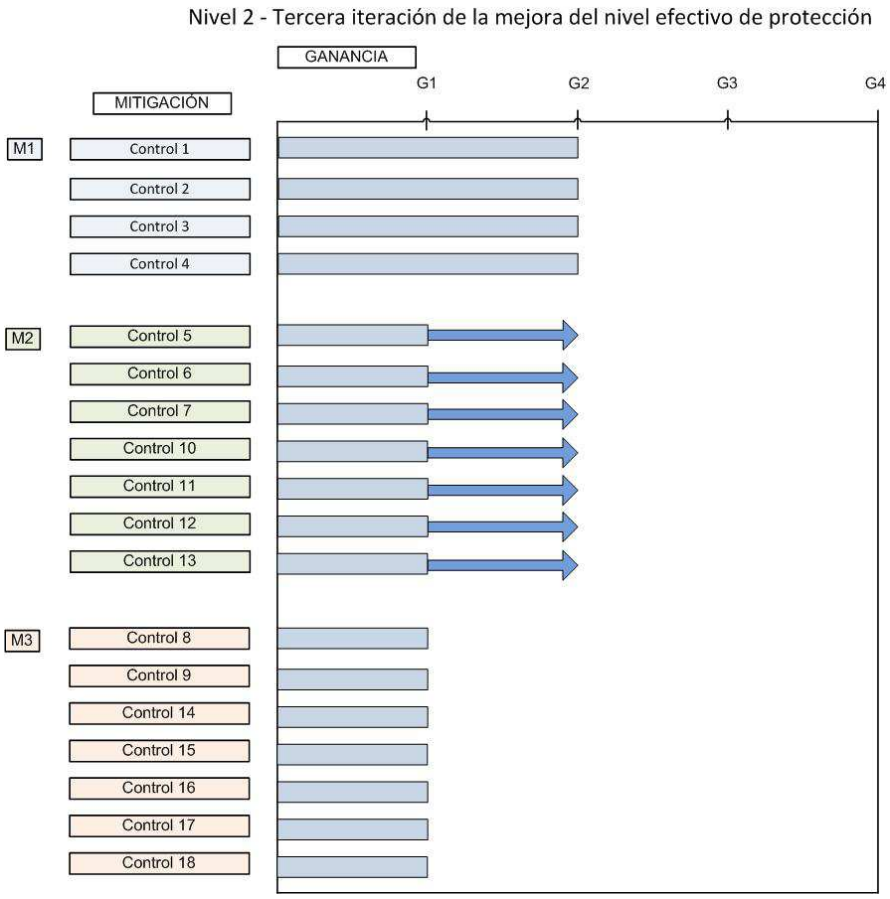


Figura 17. Tercera iteración para alcanzar el nivel 2 efectivo

Proceso para alcanzar el nivel 3:

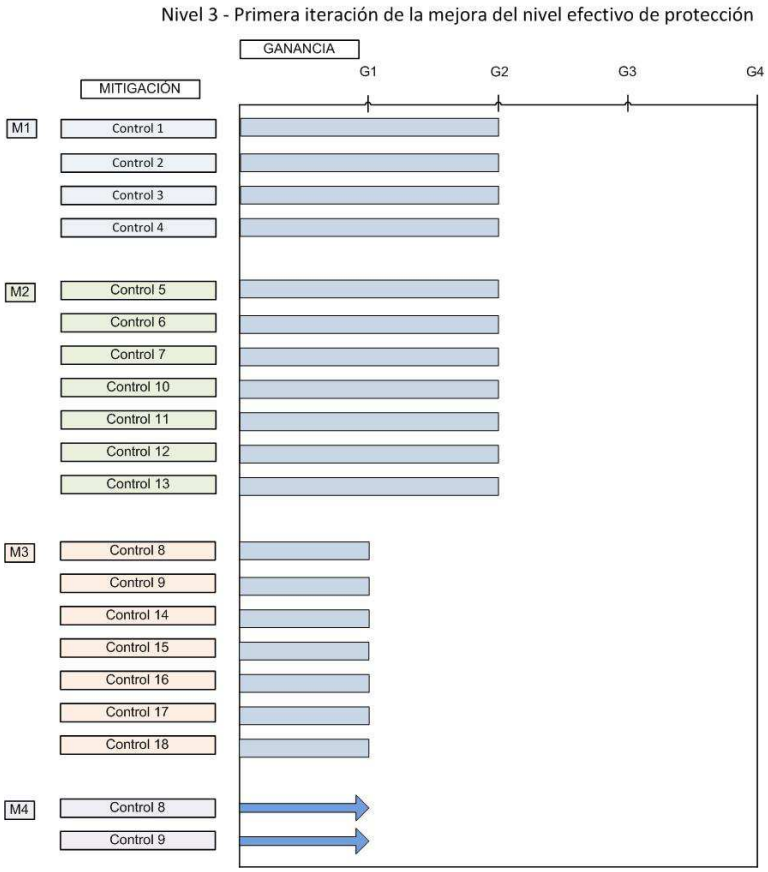


Figura 18. Primera iteración para alcanzar el nivel 3 efectivo

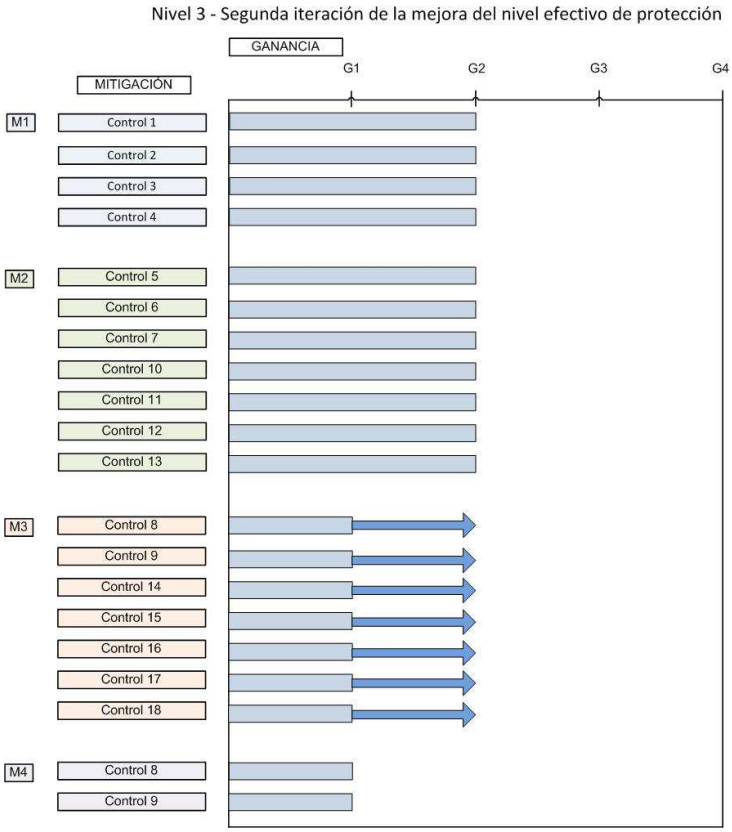


Figura 19. Segunda iteración para alcanzar el nivel 3 efectivo

Proceso para alcanzar el nivel 4:

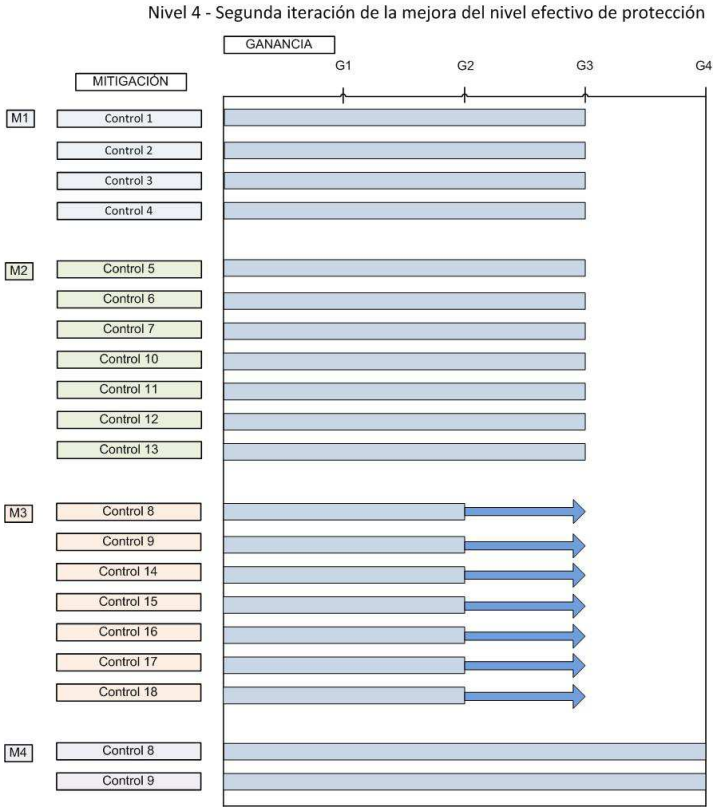


Figura 20. Primera iteración para alcanzar el nivel 4 efectivo

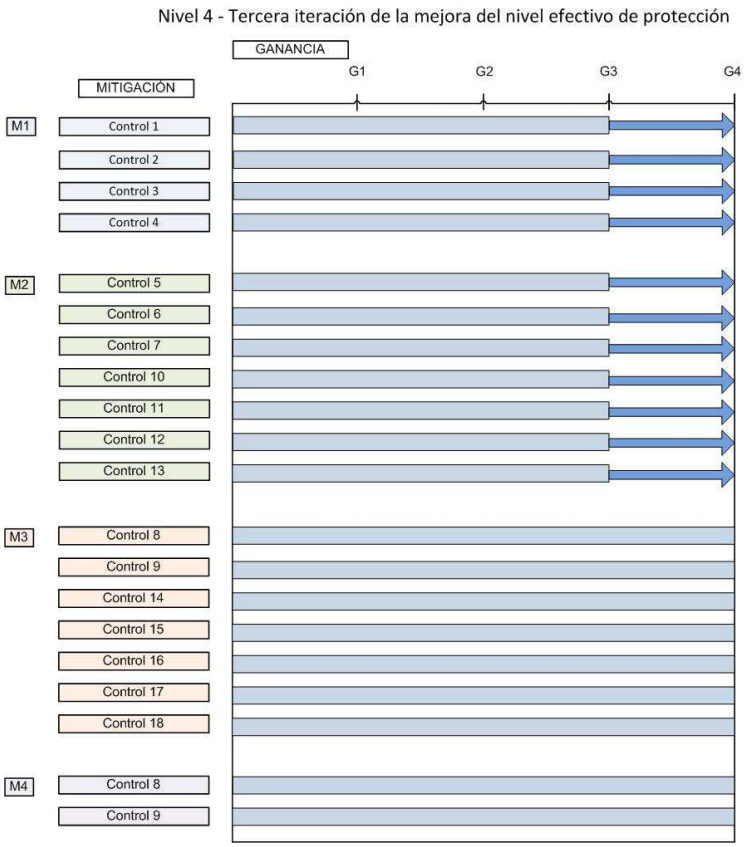


Figura 21. Segunda iteración para alcanzar el nivel 4 efectivo

5 Caso práctico

En este apartado se va a exponer un caso de ejemplo de la aplicación del método. La empresa objeto del estudio es una universidad privada, la Universitat Internacional Valenciana – VIU. Las diferentes cuestiones e información han sido facilitadas por el responsable de sistemas y seguridad o han sido obtenidas de la página web (http://www.viu.es/)

5.1 Introducción.

"La enseñanza de la VIU es online y audiovisual y tiene como seña de identidad su carácter interactivo y multimedia.

Potencia la innovación educativa. Se apoya en nuevas formas de enseñar más adecuadas a las exigencias del siglo XXI y fomenta los conocimientos y destrezas que deben desarrollar los estudiantes para adaptarse a la sociedad de la información.

No se trata de una universidad a distancia cualquiera. Se trata de una universidad presencial en internet que reproduce audiovisualmente las condiciones de una clase tradicional. Nuestro sistema de videoconferencias bidireccionales permite que el alumnado y el profesorado interaccione en vivo y en directo.

Las videoconferencias se complementan con clases grabadas en vídeos a los mejores expertos internacionales. Se acompañan de textos e-learning que aúnan texto, imagen, sonido y palabra escrita.

Los vídeos, textos y videoconferencias audiovisuales se pueden consultar a cualquier hora.

La docencia se completa con tutorías individuales y colectivas de manera que el estudiante se siente acompañado y guiado durante todo su proceso formativo. El sistema de evaluación es continuo.

La diversidad de herramientas de comunicación (correo, foro, chat, wikis….) permite una mayor proximidad entre el alumnado y el profesorado y posibilita comentar las actividades, elaborar trabajos individuales o en grupo, exponer y debatir ideas, plantear dudas y realizar consultas. En definitiva, promueve experiencias de interconexión e innovación educativa.

Esta flexibilidad metodológica y horaria permite organizar el propio ritmo de aprendizaje, adaptarlo a las necesidades o intereses profesionales, a las características y circunstancias del alumnado, así como al nivel de formación previa. (http://www.viu.es/)"

Dentro de este contexto, se definen una serie de servicios y tecnologías asociadas que conforman el ecosistema tecnológico de la VIU.

Servicios ofrecidos:

• Portal corporativo

• Campus Virtual

• Acceso a contenidos multimedia

• Docencia presencial online y tutorías (Videoconferencias)

• Soporte online

A continuación se describen brevemente los diferentes servicios ofrecidos y las tecnologías en las que se apoyan.

5.2 Entorno tecnológico.

Se diferencian dos entornos funcionales dentro del sistema de la VIU.

Por un lado está el entorno de aplicaciones que se encuentra físicamente ubicado en un Centro de Datos en modalidad de Hosting. Está compuesto de dos entornos, Test y Producción. Cada uno de ellos aloja las diferentes etapas evolutivas de las herramientas.

En Producción se presenta una arquitectura por capas que separa por seguridad la presentación de las aplicaciones del almacenamiento de contenidos, autorización de acceso y bases de datos.

Se compone de seguridad perimetral con Firewalls dedicados en alta disponibilidad, balanceadores de carga, sistemas IDS y gestor de eventos de seguridad SIEM. Una capa de servidores redundados en HA para Portal, Campus, Videoconferencias, Gestor de Incidencias, Chat de Soporte, etc. y por último una capa interna de infraestructura para estas aplicaciones compuesta por bases de datos Oracle, autenticación y autorización LDAP SSO, streaming de video, etc.

El segundo entorno sería el de las 4 sedes físicas de la VIU, 2 en Valencia y 2 en Castellón. Todas ellas tienen sistemas de Directorio Activo redundado en combinación de servidores físicos y virtuales, comunicaciones compuestas por un canal dedicado para videoconferencias, otro para internet y otro de backup, sistemas de copias de seguridad en diferentes capas y con diferentes tecnologías (DFS, NAS, cintas,…)

Además están implementados servidores de antivirus, copias de seguridad, IDS, contabilidad, etc. La VIU hace un uso exhaustivo de la tecnología de virtualización por lo que en todas las sedes los servidores se ejecutan en entornos virtuales para maximizar la eficiencia de la inversión y minimizar el consumo energético.

Servicios externos.

Los servicios actualmente externalizados son:

• Alojamiento de la plataforma de aplicaciones

• Servicios de videoconferencia para las clases

• ERP

5.3 Aplicación del método

5.3.1 Fase 1: Análisis

5.3.1.1 Tipo de empresa

Encuesta y datos facilitados por los departamentos de Administración y Tecnología de la organización.

¿A qué sector pertenece la empresa?

Sector	Educación	X

¿Cuántos empleados tiene?

Nº Empleados	51 a 100	X

¿Cuál es el tipo de propiedad de la empresa?

Propiedad del capital	Empresa privada	X

¿Cuál es el ámbito de actividad?

Ámbito de actividad	Multinacional	X

¿A qué se destinan los beneficios?

Destino de los beneficios	Con ánimo de lucro	X

¿Cuál es la forma jurídica?

Forma jurídica	Unipersonal	X

Las respuestas a las cuestiones sobre el tipo de empresa no indican ningún valor fuera de lo común por lo que no se modificará el valor obtenido en grado de exposición a incidentes

5.3.1.2 Grado de exposición a incidentes tecnológico

Respuesta a los cuestionarios.

Cuestiones	0 Nada 5 Completamente
¿Cómo afectaría la perdida de conexión a internet a su negocio?	5
¿Cómo afectaría la imposibilidad de acceder a sus equipos informáticos?	5
¿Cómo afectaría la perdida de información o datos almacenada?	5

Topología

Cuestiones	
¿Cuántos equipos informáticos estima que hay en su empresa?	100
¿Cuántos de ellos gestionan información o procesos críticos?	10
¿Cuántos servidores estima que hay en su empresa?	60
¿Cuántos de ellos gestionan información o procesos críticos?	10
¿Cuántas sedes tiene su empresa?	4
¿Existen líneas de comunicación entre ellas?	No
¿Las redes de comunicación entre las sedes son críticas?	No
¿Utiliza servicios de internet para su negocio?	Si
¿Son críticos?	Si
¿Guarda información crítica en estos servicios?	Si

Cálculo de valores

Valores obtenidos aplicando la Tabla 6: Niveles de grado de afectación.

V1	5	Muy Alta
V2	5	Muy Alta
V3	5	Muy Alta

Valores obtenidos aplicando la Tabla 7: Proporción de equipos por criticidad.

V4	10%	Baja

Valores obtenidos aplicando la Tabla 8: Proporción de servidores por criticidad.

V5	16,67%	Media

Valores obtenidos aplicando la Tabla 9: Importancia de las comunicaciones.

V6	No hay líneas de comunicación entre sedes	Media

Valores obtenidos aplicando la Tabla 10: Criticidad de los servicios de internet.

V7	Se utilizan servicios de internet y tanto procesos como datos son críticos	Muy Alta

El grado de afectación a incidentes tecnológicos es muy alto, cualquier incidente grave afectaría directamente al negocio. La proporción de equipos críticos es baja, esto implica que es fácil mejorar la protección con métodos como segmentación de redes, agrupado, etc.

La proporción de servidores críticos también es baja, esto denota baja exposición por lo que los procesos de securización pueden ser efectivos. El número de sedes y la criticidad de sus comunicaciones no son relevantes.

Es una empresa que basa su negocio en internet con procesos y datos, distribuidos y expuestos.

Catalogación del tipo de empresa para la aplicación del método.

De los cuestionarios anteriores podemos extraer que se trata de una mediana empresa con presencia internacional, con una dependencia media de equipos y sistemas informáticos pero una alta dependencia de internet en sus procesos de negocio.

V1	Muy Alta
V2	Muy Alta
V3	Muy Alta
V4	Baja
V5	Media
V6	Media
V7	Muy Alta
V8	Alta

Aplicando la fórmula VMax=Muy Alta, VMax>3

Valores obtenidos aplicando la Tabla 11: Grado de exposición ante incidentes de seguridad.

Grado de exposición del negocio ante incidentes de seguridad informática	
T4	Muy Alta

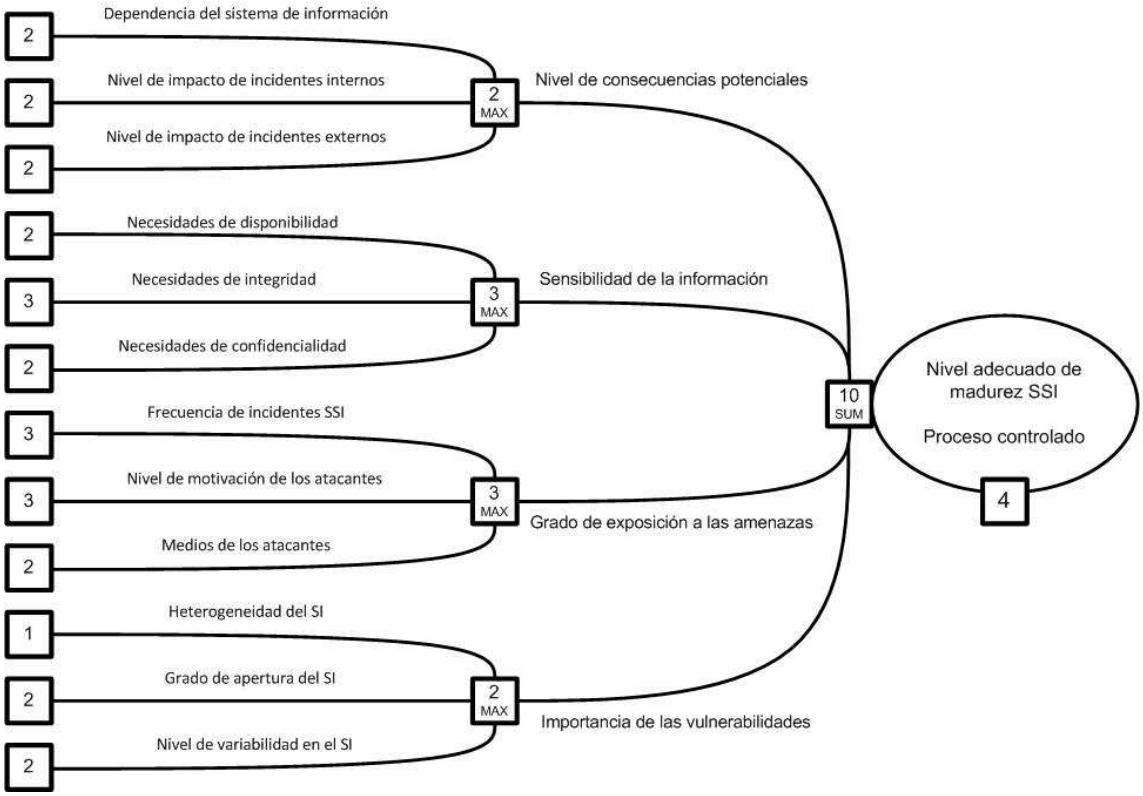
Nivel adecuado de madurez:

A continuación se evaluará el nivel adecuado de madurez del sistema de seguridad de la información con el objetivo de comprobar el grado de gestión.

Grupo	Nº	Cuestiones	Respuestas	Valor
Nivel de consecuencias potenciales	1	¿Cuál es la importancia del sistema de información para el negocio?	El SI es necesario para el cumplimiento del negocio	2
	2	¿Cuáles son las consecuencias internas (problemas de funcionamiento, impacto financiero, impacto jurídico,…) de un incidente de seguridad en su SI?	Las consecuencias internas de un siniestro SSI son graves	2
	3	¿Cuáles son las consecuencias externas (imagen, seguridad del entorno, contratos,…) de un incidente de seguridad en su SI?	Las consecuencias externas de un siniestro SSI son graves	2
Sensibilidad de la información	4	¿En qué medida es importante la disponibilidad de los sistemas informáticos?	La falta de accesibilidad al SI es grave para la actividad	2
	5	¿Dentro del marco de la actividad, en qué medida es importante la integridad de los datos?	La alteración de datos es fatal para la actividad	3
	6	¿En qué medida es importante la confidencialidad de la información en el ámbito de actividad de la empresa?	Si la seguridad de la información ha sido comprometida, es grave para la actividad	2
Grado de exposición a las amenazas	7	¿Cuál es la frecuencia estimada de incidentes SSI?	Varios siniestros SSI por mes	3
	8	¿Cuál es el grado de motivación de los atacantes potenciales?	La motivación de los atacantes potenciales es muy alta	3
	9	¿Cuáles son las competencias y recursos de los atacantes potenciales?	Loa atacantes potenciales poseen medios avanzados	2
Importancia de las vulnerabilidades	10	¿Cuál es el nivel de heterogeneidad del sistema de información?	El SI es débilmente heterogéneo	1
	11	¿Cuál es el grado de apertura del SI?	El SI está abierto a sistemas externos bajo control	2
	12	¿Cuál es el nivel de variabilidad de los componentes del SI (material, SW, redes, locales, personal,…) y del contexto en	El SI y su contexto cambian a	2

		el que opera (restricciones, exigencias normativas, amenazas,…)?	menudo	

Aplicación de la Figura 9. Cálculo del nivel de madurez.



De estos dos apartados se extrae que tanto el nivel de exposición del negocio a incidentes de seguridad como el nivel adecuado de madurez tienen el valor 4, el más alto nivel.

Nivel de madurez efectivo del SSI

Exigencias para alcanzar un nivel de madurez SSI	Definir la estrategia SSI	Gestionar los riesgos SSI	Gestionar las reglas SSI	Supervisar el SSI	Definir las medidas SSI	Realizar las medidas SSI	Explotar las medidas SSI
Las acciones se realizan utilizando prácticas de base	X	X	X				
Nivel 1	Completo	Completo	Completo				
Las acciones están planificadas							
Los actores son competentes en SSI	X	X	X				
Algunas prácticas están formalizadas	X		X				
Se realizan algunas medidas cualitativas	X						
Las autoridades competentes están informadas de las medidas							
Nivel 2							
Los procesos están definidos, estandarizados y formalizados							
Los actores tienen las competencias apropiadas a los procesos							
La organización apoya los procesos							
Nivel 3							
Los procesos están coordinados en todo el perímetro							
Medidas cuantitativas se efectúan regularmente							
Se analizan las medidas efectuadas							
Los procesos se mejoran como resultado del análisis							
Nivel 4							
El proceso se adapta de forma dinámica a las situaciones							
El análisis de las medidas está definido, estandarizado y formalizado							
La mejora de los procesos está definida, estandarizada y formalizada							
La mejora de los procesos está documentada							
Nivel 5							
Nivel efectivo de madurez de los procesos SSI							

El nivel de madurez en los diferentes procesos de gestión del sistema de seguridad es muy bajo. Esto indica un pobre nivel de implicación por parte de la empresa en estos procesos. Una vez evaluados los procesos de gestión pasamos a evaluar el estado de protección a nivel práctico aplicando los cuestionarios del referencial.

5.3.2 Fase 2: Evaluación

Respuestas a los cuestionarios. Se presentan solo las respuestas negativas ya que serán los puntos de control que habrá que implementar en las siguientes fases. Los puntos de control ya implementados, o no aplicables a la empresa, se han eliminado.

Nivel1				
Control		M/G	Cuestiones	Si/No/No procede
1.1	QW	G1	¿Se utilizan herramientas activas/pasivas para el descubrimiento de activos?	No
1.2	QW	G1	¿Se mantiene registro del sistema DHCP? ¿Se detectan sistemas desconocidos?	No
2.1	QW	G1	¿Existe un control de software por listas blancas?	No
2.2	QW	G1	¿Se gestionan listas blancas de SW?	No
2.3	QW	G1	¿Existe un proceso de alerta y control estricto de software instalado?	No
3.3	QW	G1	¿El uso de privilegios administrativos está limitado y aislado en todos los casos?	No
3.4	QW	G1	¿Existen plantillas de imágenes de configuración estricta para el despliegue de equipos?	No
3.5	QW	G1	¿Estas imágenes están custodiadas en ubicaciones seguras y/o fuera de línea?	No
5.3	QW	G1	¿La configuración de los equipos impide la ejecución automática de dispositivos externos y extraíbles así como el montado automático de unidades?	No
5.7	QW	G1	¿Existen políticas definidas sobre el uso de dispositivos externos por necesidades de negocio? ¿Se monitoriza el uso o intento de uso?	No
7.1	QW	G1	¿Todos los dispositivos inalámbricos poseen una configuración de seguridad aprobada y se deniega el acceso a los que no lo cumplen?	No
7.2	QW	G1	¿Existen herramientas de detección de dispositivos inalámbricos conectados a la red? ¿Existe un procedimiento de conciliación entre detectados y permitidos?	No
10.1	QW	G1	¿Los dispositivos de red tienen configuraciones seguras? Deben estar comprobadas, documentadas y con control de cambios.	No
11.1	QW	G1	¿Están habilitados solamente los puertos, protocolos y servicios necesarios para el negocio en los equipos?	No
11.4	QW	G1	¿Se mantienen los servicios actualizados y se desinstalan los componentes innecesarios en los equipos de la red?	No
12.1	QW	G1	¿El uso de privilegios administrativos está minimizado? ¿Existen auditorias y métodos de monitorización para su control?	No
12.5	QW	G1	¿Las cuentas de servicio cumplen requisitos de complejidad y cambio?	No

12.7	QW	G1	¿Las cuentas administrativas se utilizan para otros usos?	No
13.1	QW	G1	¿Las comunicaciones están limitadas por listas negras/blancas? ¿Se testean periódicamente?	No

Nivel 2				
Control		M/G	Cuestiones	Si/No/No procede
9.1	QW	G1	¿Los empleados poseen la formación necesaria en seguridad?	No
9.2	QW	G1	¿Se realiza formación específica en seguridad?	No
9.3	QW	G1	¿Existe un programa de sensibilización en la empresa?	No
14.1	QW	G1	¿Existen al menos dos fuentes NTP para marcas de tiempo consistentes?	No
14.2	QW	G1	¿Están validadas las configuraciones de registros de cada dispositivo HW? ¿Están estandarizados o normalizados?	No
14.5	QW	G1	¿Se realizan análisis e informes periódicos sobre identificación, resolución y documentación de anomalías?	No
15.1	QW	G1	¿La información sensible está separada por VLAN? ¿El flujo de datos entre redes sensibles está cifrado?	No
16.1	QW	G1	¿Se revisa periódicamente las cuentas de los sistemas y se deshabilitan las no asociadas a procesos de negocio?	No
16.3	QW	G1	¿Se controla de forma automática las cuentas sin caducidad, cerradas o deshabilitadas?	No
16.4	QW	G1	¿Existen procedimientos de revocación de derechos de usuarios? ¿Se mantienen las trazas de auditoria?	No
16.5	QW	G1	¿El uso de cuentas esta monitorizado? ¿Está programado el cierre automático por inactividad?	No
16.7	QW	G1	¿El uso de cuentas inactivas o deshabilitadas está supervisado?	No
17.1	QW	G1	¿Los equipos con datos sensibles y los dispositivos móviles tienen discos duros cifrados?	No
17.3	QW	G1	¿Se ha realizado un análisis y evaluación de los datos que requieren cifrado?	No
17.4	QW	G1	¿Se revisan las prácticas de protección de datos de los proveedores de servicios cloud?	No
18.1	QW	G1	¿Existen procedimientos con personal asignado para el manejo de incidentes?	No
18.2	QW	G1	¿Están asignadas al personal las funciones relativas a la resolución de incidentes?	No
18.3	QW	G1	¿Está definido el personal de gestión que apoye la toma de decisiones en el manejo de incidentes?	No
18.4	QW	G1	¿Existen normas sobre el tiempo de reporte de incidentes?	No
18.5	QW	G1	¿Existe información a disposición de los usuarios sobre los métodos para reportar incidentes?	No
18.6	QW	G1	¿Se publica periódicamente información sobre incidentes y anomalías de seguridad?	No
1.4	V/R	G2	¿Existe un inventario extenso de dispositivos conectados?	No
2.4	V/R	G2	¿Hay herramientas de control de software e inventario en todos los equipos?	No

3.6	V/R	G2	¿Los sistemas se adquieren pre configurados de forma segura?	No
4.5	V/R	G2	¿Existen herramientas de gestión y despliegue de parches para todos los SO y aplicaciones?	No
4.6	V/R	G2	¿Existe un método de control y custodia de los registros de análisis de vulnerabilidades?	No
6.3	V/R	G2	¿Existen aplicaciones desarrolladas in-house? ¿Están documentados los flujos de datos? ¿Cumplen los requerimientos de seguridad?	No
6.4	V/R	G2	¿Se han testeado vulnerabilidades y DOS en aplicaciones in-house o de terceros?	No
12.10	V/R	G2	¿Existen registros y alertas para el movimiento o adición de cuentas privilegiadas?	No
13.3	V/R	G2	¿Se ha implementado SPF en DNS?	No

Nivel 3				
Control		M/G	Cuestiones	Si/No/No procede
20.2	QW	G1	¿Se utilizan cuentas especiales para las pruebas? ¿Se deshabilitan al acabar las pruebas?	No
9.4	V/R	G2	¿Existe algún método para evaluar la concienciación?	No
15.2	V/R	G2	¿Está establecida una auditoría detallada para datos no públicos y autenticación especial para datos sensibles?	No
16.10	V/R	G2	¿Empleados, proveedores y cuentas se concilian periódicamente?	No
16.11	V/R	G2	¿Existen auditorías y supervisión para el uso de cuentas deshabilitadas?	No
17.5	V/R	G2	¿Existen herramientas de monitorización, detección y alerta para descubrir intentos de exfiltración de datos?	No
17.6	V/R	G2	¿Se testea periódicamente la efectividad del uso del cifrado?	No
5	C/H	G3	¿La base de datos de inventario está protegida y respaldada?	No
6	C/H	G3	¿Existe un mapa de información crítica en activos HW?	No
7	C/H	G3	¿Está implementada la autenticación 802.1x?	No
8	C/H	G3	¿Está implementado el acceso NAC?	No
6	C/H	G3	¿Las herramientas de control de SW instalado y el inventario HW/SW están vinculadas?	No
7	C/H	G3	¿Está implementada alguna tecnología de listas blancas en dispositivos móviles?	No
4.7	C/H	G3	¿Existen políticas y sistemas de comprobación y aceptación de vulnerabilidades detectadas y tratadas?	No
4.8	C/H	G3	¿Se mide el GAP de parcheo de vulnerabilidades? ¿Están definidos umbrales y contramedidas?	No
6.7	C/H	G3	¿Se han utilizado herramientas de testeo para el SW desarrollado y sus entradas de datos?	No
6.8	C/H	G3	¿Se ha estudiado el proceso de seguridad de los proveedores de aplicaciones?	No
6.11	C/H	G3	¿Se incluyen herramientas de desarrollo en el entorno de producción?	No

7.4	C/H	G3	¿Se gestiona que los equipos conectados a las redes inalámbricas permitidas sean por necesidades de negocio?	No
7.5	C/H	G3	¿Se encuentran deshabilitadas los dispositivos inalámbricos sin necesidad de uso y protegidos con contraseña?	No
7.8	C/H	G3	¿Están desactivadas las capacidades P2P en todos los equipos?	No
7.9	C/H	G3	¿Están desactivadas las capacidades bluetooth en equipos sin necesidad?	No
10.2	C/H	G3	¿Las variantes de configuración están documentadas junto al responsable de negocio?	No
10.3	C/H	G3	¿Se utilizan herramientas automatizadas para el control de cambios con reporte?	No
13.9	C/H	G3	¿Se escanean periódicamente los canales con conexión de retorno no autorizados?	No

Nivel 4				Nivel
Control		M/G	Cuestiones	Si/No/No procede
19.2	C/H	G3	¿El diseño de la red permite el despliegue rápido de defensas y contramedidas (actualizaciones, listas de control de acceso, reglas firmas, etc.)?	No
20.3	V/R	G2	¿Se realizan ejercicios periódicos de Red Team?	No
20.4	V/R	G2	¿Se incluye documentación útil a los atacantes en las pruebas?	No
20.7	A	G4	¿Existe un sistema de puntuación o normalización de los resultados que permita la evaluación y el seguimiento?	No
9.5	C/H	G3	¿Existe un método de evaluación para los roles de misión crítica?	No
14.9	A	G4	¿Se monitorizan y auditan la creación de servicios o la utilización de herramientas de administración de sistemas?	No
14.10	A	G4	¿El sistema de recolección de eventos está asegurado ante la pérdida o fallo en la recolección?	No
16.13	C/H	G3	¿Están configurados perfiles de uso de cuentas y equipos por franjas horarias?	No
17.8	C/H	G3	¿Está controlado el uso de dispositivos de almacenamiento externo?	No
17.9	C/H	G3	¿Se ha implementado Data Loss Prevention para los datos y equipos sensibles?	No
17.11	C/H	G3	¿Se comprueba al menos anualmente los algoritmos y claves en el uso de información sensible?	No
17.12	A	G4	¿Se supervisa el uso de canales cifrados no autorizados?	No
17.13	A	G4	¿Se bloquea el acceso a webs de transferencia de ficheros y correo electrónico?	No
17.14	A	G4	¿Están definidas las funciones y responsabilidades relacionadas con claves de cifrado? ¿Tienen definidos ciclos de vida?	No
17.15	A	G4	¿Se utiliza Hardware Security Modules para la protección de claves privadas o de cifrado en casos necesarios?	No
18.7	C/H	G3	¿Se realizan pruebas periódicamente con el personal simulando escenarios de incidentes?	No
10	A	G4	¿Está implementada la autenticación por certificados?	No

10	A	G4	¿Se ha implementado alguna tecnología de etiquetas para la integridad del SW base?	No
5.10	A	G4	¿Se ha implementado un procedimiento de respuesta a incidentes?	No
5.11	A	G4	¿Está habilitada la detección de dominios C2 en DNS?	No
13.12	A	G4	¿Están activados la detección de detección de sesiones largas en firewalls para detectar canales encubiertos?	No

5.3.3 Fase 3: Presentación de informes

5.3.3.1 Resumen de resultados

Según los valores extraídos del análisis el tipo de empresa no necesita de un grado de protección superior al que se evalúe en las siguientes fases.

El grado de exposición del negocio a las amenazas derivadas de incidentes de seguridad en sistemas informáticos es muy alto. Existe una gran dependencia de estos sistemas para la continuidad del negocio.

El grado de madurez de los procesos de gestión de la seguridad informática es muy bajo por lo que es necesaria una mayor implicación de los órganos directivos en la mejora de estos procesos.

El grado de cumplimiento de los controles es el siguiente:

Nivel 1	61,29%
Nivel 2	60,00%
Nivel 3	50,00%
Nivel 4	51,22%

Es necesario elevar los diferentes niveles de protección además de conseguir una mayor implicación de la empresa.

Se ha realizado el cuestionario de cumplimiento de ISO 27002 con un resultado de cumplimiento inferior al 20% pero no se ha incluido en este apartado porque, en este caso, no aporta información sustancial.

5.3.3.2 Informe técnico. Puntos de control a implementar

Nivel1 Control		M/G	Controles
1	VH	M1	Inventario de dispositivos autorizados y no autorizados
1.1	QW	G1	Herramienta de descubrimiento de activos para construir un inventario. Herramientas activas (rango de ips) y pasivas

			(análisis de tráfico)
1.2	QW	G1	Implementar DHCP con registro, mejora del sistema de inventario y detección de sistemas desconocidos.
2	VH	M1	Inventario de Software autorizado y no autorizado
2.1	QW	G1	Implementar tecnología de control de software por listas blancas
2.2	QW	G1	Elaborar listas de software permitido
2.3	QW	G1	Escaneo regular de software no autorizado y generación de alertas. Proceso estricto de control de cambios.
3	VH	M1	Configuraciones seguras para Hardware y Software en dispositivos móviles, ordenadores portátiles, estaciones de trabajo y servidores
3.3	QW	G1	Limitar privilegios administrativos a muy pocos usuarios con conocimientos y necesidades de negocio.
3.4	QW	G1	Utilización de imágenes para todos los equipos y gestión de configuración estricta.
3.5	QW	G1	Custodia de las imágenes en servidores seguros y/o fuera de línea.

5	H	M2	Defensas de malware
5.3	QW	G1	Configurar equipos para impedir la ejecución automática en dispositivos externos o extraíbles así como el montado automático de unidades.
5.7	QW	G1	Limitar el uso de dispositivos externos a las necesidades de negocio. Monitorizar el uso y el intento de uso de estos dispositivos.
7	H	M2	Control de dispositivos inalámbricos
7.1	QW	G1	Asegurar que cada dispositivo inalámbrico tiene una configuración aprobada y un perfil de seguridad y denegar el acceso a dispositivos que no lo cumplan.
7.2	QW	G1	Configurar herramientas de escaneo para detectar dispositivos inalámbricos conectados a LAN. Conciliar los dispositivos detectados con permitidos y desactivar los no permitidos.
10	H	M2	Configuraciones seguras para los dispositivos de red, tales como firewalls, routers y switches
10.1	QW	G1	Definir configuraciones seguras estándar para cada dispositivo de electrónica de red. Las configuraciones deben estar comprobadas, documentadas y debe existir un control de cambios.
11	H	M2	Limitación de puertos de red, protocolos y servicios
11.1	QW	G1	Asegurarse de que solo los puertos, protocolos y servicios con necesidades de negocio validadas se ejecutan en los equipos.
11.4	QW	G1	Mantener los servicios actualizados y desinstalar los componentes innecesarios.
12	H	M2	Uso controlado de privilegios administrativos
12.1	QW	G1	Minimizar los privilegios administrativos y solo usarlos cuando se requiera. Implementar auditorías focalizadas en el uso de privilegios administrativos y monitorizar el comportamiento anómalo.
12.5	QW	G1	Asegurarse de que las cuentas de servicio cumplen los requisitos de complejidad y las periodicidades de cambio.
12.7	QW	G1	Usar listas de control de acceso para asegurar que las cuentas administrativas se usan para labores administrativas. Debe impedirse el uso de aplicaciones de correo electrónico o navegadores con cuentas administrativas.
13	H	M2	Defensa perimetral
13.1	QW	G1	Limitar las comunicaciones con listas negras o listas blancas. Se realizaran pruebas periódicas.

Nivel 2 Control		M/G	Controles
9	M	M3	Habilidades de seguridad, evaluación y formación adecuadas
9.1	QW	G1	Realizar un análisis de las habilidades que poseen y necesitan los empleados y generar una hoja de ruta.
9.2	QW	G1	Formar y capacitar a los empleados. Realizar formación jerarquizada cuando sea posible. Cubrir vacíos mediante formación online o conferencias.
9.3	QW	G1	Implementar un programa de sensibilización. 5 puntos
14	M	M3	Mantenimiento, Monitoreo y Análisis de Logs de registro
14.1	QW	G1	Incluir al menos dos fuentes de sincronización de tiempos (ej.: NTP) para cada servidor o dispositivo de red para que las marcas de tiempo sean consistentes.
14.2	QW	G1	Validar la configuración de registros para cada dispositivo hardware y para el software instalado en él incluyendo sello de tiempo, origen, destino así como descriptores de la transacción. Los registros deberán estar estandarizados o ser normalizados.
14.5	QW	G1	El personal de seguridad y sistemas debe realizar informes quincenales para identificar anomalías en los registros las cuales deben ser resueltas y documentadas.
15	M	M3	Acceso Controlado con base en la necesidad de conocer
15.1	QW	G1	Ubicar la información sensible en VLANs separadas protegiendo el tráfico entre ellas con firewalls. El tráfico a través de redes no confiables debe estar cifrado.
16	M	M3	Supervisión y control de cuentas
16.1	QW	G1	Revisar todas las cuentas de los sistemas y deshabilitar aquellas que no estén asociadas a un propietario o proceso de negocio.
16.3	QW	G1	Crear informes automáticos de los sistemas que incluyan cuentas cerradas, deshabilitadas, contraseñas sin caducidad o con duración máxima superada. El envió debe producirse de forma segura.
16.4	QW	G1	Establecer procedimientos de revocación de acceso para usuarios que finalicen su relación con la organización. Deshabilitar las cuentas permite mantener las trazas de auditoría.
16.5	QW	G1	Monitorizar regularmente el uso de todas las cuentas y programar el cierre automático de sesiones por inactividad.
16.7	QW	G1	Supervisar el uso de cuentas inactivas y deshabilitarlas si no son necesarias. Documentar y monitorizar las excepciones.
17	M	M3	Prevención de pérdida de datos
17.1	QW	G1	Implementar software de cifrado de disco duro en dispositivos móviles y equipos con datos sensibles.
17.3	QW	G1	Llevar a cabo una evaluación de los datos para identificar aquellos que requieren la aplicación de controles de cifrado e integridad.
17.4	QW	G1	Revisar las prácticas de protección de datos de los proveedores de servicios cloud.
18	M	M3	Respuesta y manejo de Incidentes
18.1	QW	G1	Asegurar que existen procedimientos escritos para el manejo de incidentes incluyendo definiciones del personal asignado. Deben definir las fases del manejo de los incidentes.
18.2	QW	G1	Asignar funciones relativas a la resolución de incidentes al personal

18.3	QW	G1	Definir personal de gestión que apoye la toma de decisiones en el manejo de incidentes informáticos.
18.4	QW	G1	Elaborar normas en toda la organización para el tiempo de reporte, tipo de información y forma de reportar eventos. Debe haber conformidad a las normativas legales.
18.5	QW	G1	Montar y mantener información así como modo de contacto sobre incidentes de seguridad.
18.6	QW	G1	Publicar información para todo el personal sobre incidentes o anomalías de seguridad. Debe estar incluido en las actividades de concienciación.

1	VH	M1	Inventario de dispositivos autorizados y no autorizados
1.4	V/R	G2	Inventario extenso de los dispositivos conectados.
2	VH	M1	Inventario de Software autorizado y no autorizado
2.4	V/R	G2	Implementar herramientas de inventario de software en todos los equipos en todas sus versiones.
3	VH	M1	Configuraciones seguras para Hardware y Software en dispositivos móviles, ordenadores portátiles, estaciones de trabajo y servidores
3.6	V/R	G2	Adquisición de sistemas preconfigurados de forma segura.
4	VH	M1	Evaluación continua y corrección de vulnerabilidades
4.5	V/R	G2	Implementar herramientas de gestión de parches para SO y aplicaciones para todos los sistemas.
4.6	V/R	G2	Control y custodia de los registros asociados a los análisis y exploraciones.

6	H	M2	Seguridad en aplicaciones software
6.3	V/R	G2	Para aplicaciones desarrolladas in-house comprobar que las entradas de datos están documentadas y cumplen requerimientos de seguridad.
6.4	V/R	G2	Testear vulnerabilidades y DDOS en aplicaciones desarrolladas in-house y de terceros.
12	H	M2	Uso controlado de privilegios administrativos
12.10	V/R	G2	Configurar registros y alertas cuando se añadan cuentas con privilegios o se muevan cuentas a/desde grupos privilegiados.
13	H	M2	Defensa perimetral
13.3	V/R	G2	Implementar SPF en DNS para disminuir la posibilidad de recibir correos falsificados.

Nivel 3 Control		M/G	Controles
20	L	M4	Pruebas de penetración y RedTeam
20.2	QW	G1	Las cuentas de sistema o de usuario utilizadas para las pruebas deben ser controladas y supervisadas así como deshabilitadas tras su uso.

8	M	M3	Capacidad de recuperación de datos
9	M	M3	Habilidades de seguridad, evaluación y formación adecuadas
9.4	V/R	G2	Establecer un método para validar la concienciación (enlaces de correo, datos telefónicos, etc.) principalmente a

			víctimas potenciales.
15	M	M3	Acceso Controlado con base en la necesidad de conocer
15.2	V/R	G2	Establecer auditoría detallada en datos no públicos y autenticación especial en datos sensibles.
16	M	M3	Supervisión y control de cuentas
16.10	V/R	G2	Conciliar empleados activos y proveedores con cuentas y desactivar las no asignadas.
16.11	V/R	G2	Registro de auditoría y supervisión del uso de cuentas deshabilitadas.
17	M	M3	Prevención de pérdida de datos
17.5	V/R	G2	Implementar una herramienta automatizada para monitorizar información sensible o palabras clave para descubrir intentos no autorizados de exfiltración. Configurar bloqueo y alertas.
17.6	V/R	G2	Controlar mediante herramientas la efectividad de uso del cifrado de datos sensibles. Buscar e identificar patrones, ficheros en texto plano con información sensible.
18	M	M3	Respuesta y manejo de Incidentes

1	VH	M1	Inventario de dispositivos autorizados y no autorizados
1.5	C/H	G3	Base de datos de inventario protegida y con copia de seguridad.
1.6	C/H	G3	Mapa de información crítica en activos hardware.
1.7	C/H	G3	Autenticación 802.1x
1.8	C/H	G3	Implementar control de acceso NAC.
2	VH	M1	Inventario de Software autorizado y no autorizado
2.6	C/H	G3	Integración de la herramienta de inventario con el control de software así como la instalación de SW legítimo en equipos no autorizados.
2.7	C/H	G3	Despliegue de tecnología de listas blancas en dispositivos móviles.
4	VH	M1	Evaluación continua y corrección de vulnerabilidades
4.7	C/H	G3	Sistema de comprobación y/o aceptación de vulnerabilidades detectadas y tratadas.
4.8	C/H	G3	Medición del GAP de parcheo de vulnerabilidades, definición de umbrales y contramedidas.

5	H	M2	Defensas de malware
6	H	M2	Seguridad en aplicaciones software
6.7	C/H	G3	Utilizar herramientas de testeo para el software desarrollado tanto para el código como para los valores de entrada/salida.
6.8	C/H	G3	Estudiar el proceso de seguridad de los proveedores de aplicación como parte del proceso global de la empresa.
6.11	C/H	G3	Asegurarse de que las herramientas de desarrollo (scripts, debug code, tools) no se incluyen en el entorno de producción.
7	H	M2	Control de dispositivos inalámbricos
7.4	C/H	G3	Configurar equipos para que accedan solo a las redes inalámbricas permitidas y que sean necesidades de negocio.

7.5	C/H	G3	En aquellos equipos que no haya necesidad de uso de dispositivos inalámbricos, deshabilitarlos y proteger las configuraciones por contraseña.
7.8	C/H	G3	Desactivar las capacidades p2p en equipos a menos que haya una necesidad de negocio documentada.
7.9	C/H	G3	Desactivar las capacidades bluetooth en equipos a menos que haya una necesidad de negocio documentada.
10	H	M2	Configuraciones seguras para los dispositivos de red, tales como firewalls, routers y switches
10.2	C/H	G3	Todas aquellas configuraciones que difieran de la línea base endurecida de configuraciones debe quedar documentada junto a la razón y el responsable de negocio.
10.3	C/H	G3	Utilizar herramientas automatizadas para comprobar configuraciones y controlar cambios. Las modificaciones deben ser reportadas al personal de seguridad.
13	H	M2	Defensa perimetral
13.9	C/H	G3	Escanear periódicamente los canales con conexión de retorno a internet no autorizados (VPN, DialUp, Wifi).

Nivel 4 Control		M/G	Controles
19	L	M4	Ingeniería de red segura
19.2	C/H	G3	Diseñar la red permitiendo métodos de respuesta rápida para el rápido despliegue de nuevas listas de control de acceso, reglas, firmas, bloqueos, blackholes u otras medidas defensivas.
20	L	M4	Pruebas de penetración y RedTeam
20.3	V/R	G2	Realizar ejercicios periódicos de Red Team para evaluar ataques y respuestas.
20.4	V/R	G2	Incluir en las pruebas información o documentación que podrían ser útiles a los atacantes, diagramas de red, PenTest antiguos, emails o documentos de contraseñas, etc.
20.7	A	G4	Idear un sistema de medida o puntuación para la comparación de resultados en el tiempo.

9	M	M3	Habilidades de seguridad, evaluación y formación adecuadas
9.5	C/H	G3	Evaluar las habilidades de seguridad para cada uno de los roles de misión crítica. Utilizar ejemplos prácticos.
14	M	M3	Mantenimiento, Monitoreo y Análisis de Logs de registro
14.9	A	G4	Monitorizar la creación de servicios y auditar determinados procesos. La utilización de procesos como psexec o la creación de nuevos servicios es algo inusual.
14.10	A	G4	Asegurar que el sistema de recogida no pierde eventos incluso en periodos de gran carga, desconexiones o ancho de banda limitado.
15	M	M3	Acceso Controlado con base en la necesidad de conocer
16	M	M3	Supervisión y control de cuentas
16.13	C/H	G3	Definir y controlar perfiles de uso de las cuentas de usuario por franjas horarias y por equipos. Registrar y alertar los usos inapropiados.
16.16	A	G4	Utilizar canales cifrados para la transmisión de contraseñas.
17	M	M3	Prevención de pérdida de datos
17.8	C/H	G3	Si no hay necesidad deshabilitar el uso de dispositivos USB. En caso de necesidad controlar el uso por identificación de

			dispositivo y mantener un inventario.
17.9	C/H	G3	Utilizar soluciones DLP basadas en red. Detectar y gestionar las anomalías.
17.11	C/H	G3	Llevar a cabo una revisión anual de algoritmos y longitudes de clave en el uso de la protección de datos sensibles.
17.12	A	G4	Supervisar todo el tráfico que sale de la organización y detectar usos indebidos de canales cifrados. Los atacantes suelen cifrar los canales de extrusión de datos. Hay que detectar y bloquear las conexiones no autorizadas.
17.13	A	G4	Bloquear el acceso a webs conocidas de transferencia de ficheros y correo electrónico.
17.14	A	G4	Definir funciones y responsabilidades relacionadas con claves de cifrado de datos así como definir los ciclos de vida.
17.15	A	G4	En su caso aplicar Hardware Security Modules (HSM) para la protección de claves privadas o de cifrado.
18	M	M3	Respuesta y manejo de Incidentes
18.7	C/H	G3	Llevar a cabo sesiones periódicas con escenarios de incidentes para asegurarse de que las personas del equipo de gestión conoce y entienden las amenazas, los riesgos y las responsabilidades.

1	VH	M1	Inventario de dispositivos autorizados y no autorizados
1.10	A	G4	Validación y autenticación por certificado.
2	VH	M1	Inventario de Software autorizado y no autorizado
2.10	A	G4	Software con etiquetas de identificación
5	H	M2	Defensas de malware
5.10	A	G4	Implementar un procedimiento de respuesta a incidentes.
5.11	A	G4	Habilitar detección de dominios C2 en DNS.
13	H	M2	Defensa perimetral
13.12	A	G4	Para ayudar a identificar canales encubiertos, activar los mecanismos integrados de detección de sesiones largas en firewalls.

5.3.4 Fase 4: Implementación

Se deberán implementar los puntos de control necesarios para adquirir los diferentes niveles siguiendo el orden especificado en las figuras de la Fase 4 con la ayuda de las tablas presentadas en el apartado anterior.

6 Conclusiones

6.1 Objetivos cumplidos

Se ha conseguido reducir o eliminar las barreras que se han identificado como las responsables de la baja adopción de medidas de protección efectivas en el entorno de las pymes españolas.

Se ha desarrollado un método rápido y sencillo que permitirá a empresas de muy diferente tipología alcanzar la protección que necesitan sus sistemas de información.

Se ha conseguido basar el método en normas y estándares aceptados para darle robustez y fiabilidad.

6.2 Bondades del método

Este método permitirá alcanzar un nivel de protección de los sistemas informáticos, adecuado a las particularidades de cada empresa.

Permitirá alcanzar un alto grado de concienciación de los niveles efectivo y adecuado de protección y servirá como guía de autogestión de la seguridad.

Este método se ha basado en normas y estándares ampliamente aceptados por lo que hereda las prácticas ampliamente aceptadas y contrastadas.

El sistema consigue un alto grado de mitigación de amenazas priorizando la rapidez de la ganancia que aporta cada punto de implementación. Con esto se consigue desplazar la consecución de los mayores beneficios a las primeras etapas de implantación. Esto maximiza el resultado en el tiempo.

El análisis y la evaluación mediante cuestionarios suponen una forma sencilla y ligera de filtrar todos los puntos de control innecesarios. Esto reduce el número de soluciones, herramientas o proyectos de seguridad necesarios e identifica las amenazas con las soluciones prácticas. Esto reduce considerablemente la inversión en seguridad.

El método de implementación por niveles reduce el tiempo de implantación maximizando los resultados.

7 Nuevas líneas de trabajo y propuestas

7.1 Dotar al método de flexibilidad para adoptar nuevas normas o actualizaciones

Para que el método presentado sea durable en el tiempo debe poder adaptarse a los cambios. La constante evolución de la tecnología produce cambios en las amenazas por lo que las normas y estándares se adaptan y actualizan constantemente a ellos. Habría que dotar al método de un proceso de actualización que siga las directrices y objetivos principales que son baja complejidad y bajo coste.

7.2 Creación de un sello

En el entorno de estudio, existe la visión, tanto de empresas como de profesionales de que la seguridad solo está relacionada con las amenazas. Las empresas y consultoras de seguridad venden el miedo al daño que pueden generar estas amenazas y por lo tanto las empresas españolas identifican la seguridad como un mal necesario, un coste que no produce ningún beneficio.

En otros países y en otros mercados es común encontrar sellos con los cuales un cliente identifica unos niveles de calidad en un producto que los diferencia de otros que no lo tienen.

El desarrollo de un sello de calidad que demostrara, mediante el cumplimiento de la metodología presentada, que una empresa cumple con una serie de normas y estándares aportaría confianza a los usuarios o clientes finales. Como ejemplo, es conocida la baja implantación del comercio electrónico en las pymes españolas así como el bajo uso en diferentes sectores de población. Pienso que la falta de confianza es la causa de esto y produce una gran desventaja competitiva entre las grandes empresas con grandes sistemas de seguridad y certificaciones y las pequeñas y medianas empresas.

Un sello de cumplimiento en seguridad añadiría valor a las empresas y permitiría ver la seguridad como algo positivo que permite a un sector principal en el mercado español, derrumbar las diferencias competitivas y alcanzar mercados emergentes.

7.3 Mejorar el catálogo de soluciones y herramientas

Se ha desarrollado un trabajo de identificación de los diferentes controles del estándar con los controles de la norma SANS. A su vez se ha catalogado las diferentes soluciones y herramientas para implementar los controles de ambas.

Se ha detectado que muchas soluciones o herramientas cubren diferentes controles o puntos de implementación de estos y se está realizando un proceso de identificación de todos ellos. La idea de este trabajo es poder realizar un catálogo o base de datos con todas las herramientas y soluciones del mercado en donde se identifique en cada una de ellas los puntos que cubre e incluso poder generar un baremo para medir la calidad.

Se ha comprobado la existencia de diferentes grupos y comunidades que desarrollan proyectos similares como el ClubISO2700 en Francia donde una comunidad de profesionales evalúan diferentes soluciones para implementar un SGSI.

Para ello se propone crear un site web y contactar con diferentes comunidades, profesionales y organismos que quieran participar en el proyecto.

7.4 Mejorar la integración entre estándares y normas base

Actualmente la aplicación de la metodología está orientada a permitir a las empresas alcanzar el nivel adecuado de protección conforme a las normas y guías. Los cuestionarios que hacen referencia al estándar ISO 27000 pretenden identificar el nivel de cumplimiento pero no es objetivo de este trabajo el implementar los controles de la norma ni conseguir la certificación.

Se plantea la posibilidad de adaptar o mejorar la metodología de forma que simplemente alcanzando el nivel adecuado de protección se asegurara el cumplimiento del estándar y posibilitara la certificación.

Se plantea también realizar una identificación entre los controles, normativas y necesidades de los diferentes tipos de empresas para realizar una adaptación de grado más fino del método.

8 Referencias

1. *Controles ISO27002:2005*, ISO27000.es (2013)
2. *Estudio sobre seguridad de la información y continuidad de negocio en las pymes española,* Inteco (2012)
3. *ISO 21827 - Systems Security Engineering – Capability Maturity Model*, ISO (2001)
4. *Maturité SSI – Approche méthodologique,* ANSSI (2007)
5. *The Critical Security Controls for Effective Cyber Defense, SANS (2013). Publicado en* http://www.sans.org/critical-security-controls/
6. *Norma ISO 27000,* Coord. Galupe Monge, E. Universidad de El Salvador (2009)

9 Bibliografía

9.1 Conceptos previos

7. *Advanced Persistent Threats: A Decade in Review, COMMAND FIVE PTY LTD. (2011)*
8. *El Estado del Arte de la Seguridad Informática, Julio C. Ardita, Cybsec (2004)*
9. *Seguridad por niveles, DarFE, Alejandro Corletti Estrada (2011)*
10. *Alineando COBIT® 4.1, ITIL® V3 e ISO/IEC 27002 en beneficio de la empresa, IT Governance Institute (2008)*
11. *Becoming Resilient: The Definitive Guide to ISO 22301 Implementation, Kosutic D., EPPS Services Ltd (2013)*
12. *OSSTMM 2.1. Manual de la Metodología Abierta de Testeo de Seguridad ,Pete Herzog, ISECOM(2003)*
13. *El atacante informático, IT Forensic Ltda (2013)*
14. *Introducción a la seguridad informática, kioskea.net (2014)*
15. *An in-depth perspective on software vulnerabilities and exploits, malware, potentially unwanted software, and malicious websites,Microsoft (2013)*
16. *Microsoft Security Intelligence Report, Microsoft (2013)*
17. *Mejores Prácticas para Aplicaciones de Gobierno y Defensa, Oracle (2007)*
18. *ANÁLISIS Y GESTIÓN DE RIESGOS DEL SERVICIO IMAT DEL SISTEMA DE INFORMACIÓN DE I.C.A.I., Eduardo Ferrero Recaséns, PROYECTO FIN DE CARRERA (2006)*
19. *El Sistema de Gestión de Seguridad de la Información - La nueva Norma UNE 71502, S2 Grupo (2004)*
20. *"Metodología para el Aseguramiento de Entornos Informatizados" – MAEI, María Victoria Bisogno, Tesis de Grado (2004)*
21. *Les Preuves de Connaissance et leurs Preuves de Sécurité, David Pointcheval, Thèse de Doctorat Université de Caen (1996)*
22. *Security Configuration Management for Dummies, Steve Piper, Tripware (2013)*
23. *SEGURIDAD INFORMATICA, Jean Polo Cequeda Olago, UFPS (2012)*
24. *Aspectos avanzados de seguridad en redes, Jordi Herrera Joancomartí, UOC (2004)*
25. *Seguridad de los sistemas de la información, Antonio Villalón Huerta, UPV (2005)*
26. *Apuntes de: Seguridad en los Sistemas Informáticos (SSI), José Ismael Ripoll Ripoll, UPV (2012)*

9.2 Bases de investigación

27. *Annual Security Report , Cisco (2014)*
28. *Livre BLANC BENCHMARK DES OUTILS SMSI, Club 27001 (2013)*
29. *Blurring the lines 2013 TMT Global Security Study, Deloitte (2013)*
30. *Implantación de un SGSI en la empresa , Inteco (2012)*
31. *Resumen ejecutivo del Estudio sobre seguridad de la información y continuidad de negocio en las empresas españolas, Inteco (2012)*
32. *IAD's Top 10 Information Assurance Mitigation Strategies, NSA (2013)*
33. *internet security THREAT REPORT , Symantec (2013)*
34. *TECHNOLOGY PRIORITIES FOR 2013, TechTarget (2013)*
35. *Análisis de Riesgos de Seguridad de la Información, Juan Manuel Matalobos Veiga, TFC-UPM (2009)*
36. *How to Define SIEM Strategy, Management and Success in the Enterprise, Jean Polo Cequeda Olago, UFPS (2013)*
37. *DATA SECURITY: LEADERS VS. LAGGARDS, Unisphere (2013)*

9.3 Metodología

38. *Benefits of ISO 27001, 27001 Academy (2011)*
39. *Diagram of ISO 22301 Implementation Process , 27001 Academy (2012)*
40. *Diagram_of_ISO_27001_2013_Implementation_Process_ES , 27001 Academy (2013)*
41. *Lista de documentación obligatoria requerida por ISO/IEC 27001 (Revisión 2013), 27001 Academy (2013)*
42. *Twelve-step transition process from ISO 27001:2005 to 2013 revision, 27001 Academy (2013)*
43. *Checklist of ISO 22301 Mandatory Documentation, 27001 Academy (2014)*
44. *ISO 27001 Case Study for Data Centers, 27001 Academy (2014)*
45. *Project Checklist for ISO 27001 Implementation , 27001 Academy (2014)*
46. *White paper: How online tools are revolutionizing ISO 27001 and ISO 22301 implementation, 27001 Academy (2014)*
47. *Implantacion del ISO 27001:2005, Alberto G. Alexander, Centrum (2006)*
48. *Critical Controls for Effective Cyber Defense Version 4.1 , SANS (2013)*
49. *An Early Malware Detection, Correlation, and Incident Response System with Case Studies , SANS Institute (2013)*
50. *Critical Security Controls Survey: Moving From Awareness to Action, SANS Institute (2013)*
51. *Free and Open Source Project Management Tools, SANS Institute (2013)*
52. *Home Field Advantage: Employing Active Detection Techniques , SANS Institute(2013)*
53. *Tools and Standards for Cyber Threat Intelligence Projects, SANS Institute (2013)*
54. *Calculating Total Cost of Ownership on Intrusion Prevention Technology, SANS Institute (2014)*
55. *Seguridad de la Información en Latinoamérica Tendencias 2009, Jeimy J. Cano, SegurInfo (2009)*
56. *THE SANS 20 CSC AND TRIPWIRE SOLUTIONS DETAILED MAPPING OF THE SUB-CONTROLS, Tripware (2013)*

57. *NORMA ISO 27000 SISTEMAS DE GESTION DE SEGURIDAD INFORMATICA, GUADALUPE MONGE E., UNIVERSIDAD DE EL SALVADOR (2009)*
58. *ANÁLISIS DE ISO-27001:2005, Alejandro Corletti Estrada (2006)*
59. *ISO-27001: LOS CONTROLES, Alejandro Corletti Estrada (2006)*