Trabajo de Final de Máster

Máster Interuniversitario en Seguridad de las TIC (MISTIC)

Elaboración de un Plan de Implementación de la ISO/IEC 27001:2013

Alumno
Ekaitz Astiz Martínez
Tutor
Antonio José Segovia Henares

2017 – 2018

Índice

Índice de tablas

Índice de imágenes

1. Introducción

En este proyecto se va a elaborar un Plan de Implementación de la ISO/IEC 27001:2013 para una empresa. La idea de dicho plan, es alinear los objetivos de la empresa a los principios de seguridad establecidos en la normativa ISO/IEC 27001:2013 . A través de ello se podrán definir las bases del proceso de mejora continua en materia de seguridad de la Información, posibilitando que se pueda conocer mejor el estado de la empresa y las acciones a llevar a cabo para reducir el impacto de los riesgos.

La ISO 27001 es un estándar certificable en materia de seguridad de la información. Tiene su origen en BS 7799-2:2002. Contiene las especificaciones para la implementación de un sistema de gestión de la seguridad de la información. La ISO 27001 establece un marco que permite gestionar y mejorar de forma continua la seguridad de la información, plantea la gestión de la seguridad como un proceso continuo. En ella se recogen las especificaciones para un análisis de riesgos y su gestión, para la planificación de las medidas a realizar y los recursos para ello, la implementación de controles y sobre todo en que todo eso se revise y se mejore. Este estándar, también recoge un listado de controles basado en la ISO 27002.

La ISO 27002 es una estándar que tiene la función de guía de buenas prácticas. No es un estándar certificable. En ella se plantean 114 controles, dicho de otro modo, aspectos o condiciones a tener en cuenta, y recoge un conjunto de sugerencias para cada uno de los controles. Pero no indica cuáles son prioritarias ni que todas vayan a ser necesarias, eso dependerá de cada caso.

Se puede decir, que es la ISO 27001, la que a través de sus fases, va a resultar útil para saber qué controles se seleccionar para la situación analizada y cuáles priorizar, cómo evaluar su implantación, y finalmente tratar de mejorar la seguridad continuamente. Es decir, optimizar recursos en aquello qué de verdad suponga un riesgo y no tener que intentar o no perderse ciegamente en implantar todos los controles de la ISO 27002. La ISO 27001define el SGSI, y dicho sistema de gestión significa que la seguridad de la información debe ser planificada, implementada, supervisada, revisada y mejorada. Significa que la gestión tiene sus responsabilidades específicas, que se deben establecer, medir y revisar objetivos, que se deben realizar auditorías internas, etc. Todos esos elementos están establecidos en la ISO 27001

Como conclusión, se podría decir que sin ISO 27002 sería difícil implementar los controles definidos en el Anexo A de la ISO 27001. Pero de la misma manera, sin el marco definido por la ISO 27001, implantar la ISO 27002 sería simplemente un esfuerzo aislado, ya que quedaría en algo meramente técnico y sin necesidad de la aceptación de la alta dirección y sin efectos reales sobre la empresa.

Durante la elaboración del proyecto, está claro que analizar la situación actual de la empresa, los activos, los objetivos, los riesgos, etc. requerirá de un gran trabajo en recabar información y la implicación y colaboración por parte de la empresa, ya que hará falta mucha información y documentación que pueda existir. Por lo tanto se realizarán reuniones con la dirección.

Parte la información se basa en la el estándar [ISO/IEC 27001:2013],[ISO/IEC 27002:2013].

1.1 Herramientas

Para el desarrollo del proyecto será necesario tener acceso a información relacionada con la ISO 27001, 27002 y otros materiales como los de la asignatura SGSI. Será suficiente disponer de un ordenador y software de ofimática (Word, Visio...).

1.2 Calendario de trabajo

El trabajo se realizará acorde al calendario planteado en la guía del TFM.

FASE	Comienzo	Final	Descripción
1	20/09/2017	06/10/2017	Situación actual: Contextualización, objetivos y análisis diferencial
2	09/10/2017	20/10/2017	Sistema de Gestión Documental
3	23/10/2017	10/11/2017	Análisis de riesgos
4	13/11/2017	24/11/2017	Propuesta de Proyectos
5	27/11/2017	15/12/2017	Auditoría de Cumplimiento de la ISO/IEC 27002:2013
6	18/12/2017	03/01/2018	Presentación de Resultados y entrega de Informes
	15/01/2018	19/01/2018	Presentación del trabajo

Tabla 1: Calendario de trabajo

2. Contextualización

Para la realización del TFM se ha seleccionado la empresa Secure Team Coop. Una empresa fundada en el año 2005 por 3 personas. Desde entonces esta empresa ha realizado infinidad de trabajos de diseño implementación y mantenimiento de sistemas de información.

A día de hoy Secure Team está formado por un grupo de 10 personas con amplia experiencia en diversos servicios tales como: ingeniería de redes, entornos de virtualización, gestión de sistemas de seguridad de la información y mantenimiento de los mismos basados en la ISO 27001, programación de aplicaciones web (aplicaciones de gestión pedidos, facturación, e-commerce, intranets...) y servicios de alojamiento y cloud gestionados, etc.

A día de hoy todos los empleados son socios cooperativistas.

2.1 Visión de la empresa

La visión de Secure Team es ser un referente en soluciones TIC y en seguridad de la información en el País Vasco, especialmente para clientes que buscan un trato profesional pero cercano.

Por otro lado, también quiere ser una empresa funcional pero horizontal y democrática, a través de

la participación de los socios y trabajadores e intentando satisfacer las expectativas tanto profesionales como personales.

2.2 Misión de la empresa

La empresa tiene los siguientes puntos como misión:

- Cubrir las necesidades que tienen los clientes entorno a las TIC con una ética profesional, un precio adecuado y prestando atención a la calidad y la mejora continua.
- Ofrecer asesoramiento entorno a la seguridad de la información y la privacidad y poder ofrecer los servicios teniendo en cuenta la importancia de la seguridad de la información.
- Mejorar el conocimiento y la capacidad de los empleados de Secure Team para poder ir mejorando los servicios
- Dedicar, adecuar y optimizar recursos para poder cubrir las necesidades de la empresa y hacer que los empleados se sientan realizados tanto personalmente como profesionalmente.

2.3 Organigrama

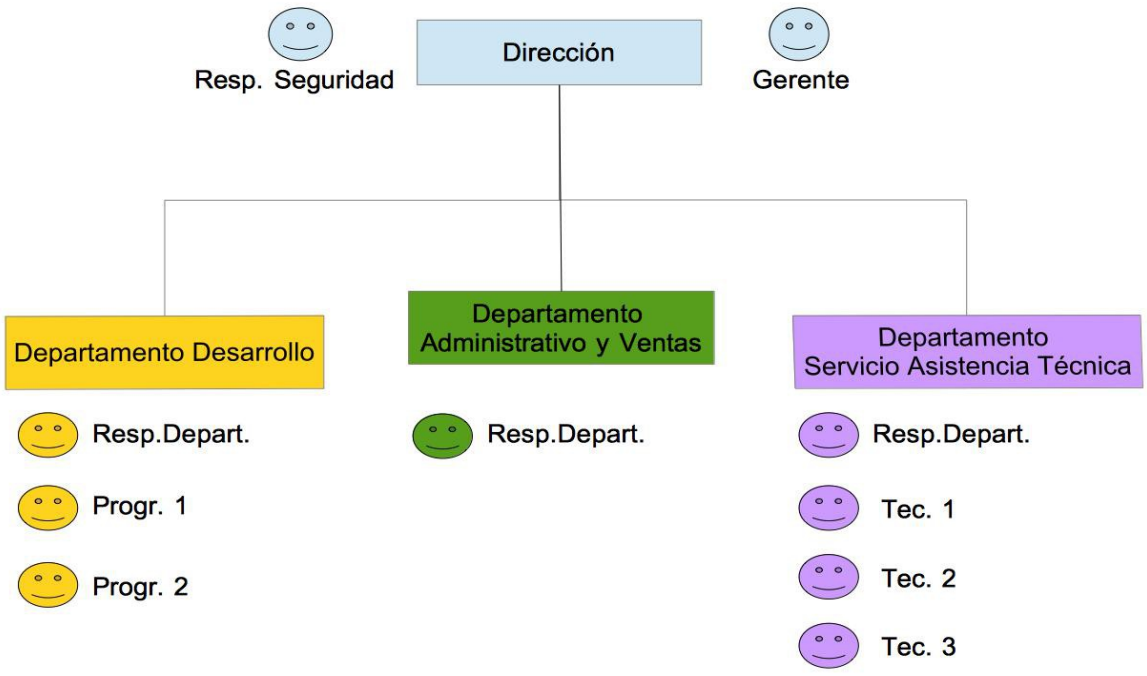

Imagen 1: Organigrama

La dirección la componen el responsable de seguridad y el gerente.

Departamento de **administración+ventas**: las funciones de este departamento las llevan

conjuntamente el gerente y otro empleado.

Departamento de servicio de asistencia técnica: Hay 4 empleados. Uno de ellos es el responsable del departamento, sobretodo se diferencia en que es el quien toma decisiones de diseño en instalaciones de redes y despliegue tecnológico de nuevos espacios de clientes. También supervisa la mayoría de mantenimientos.

Departamento de desarrollo: Hay 3 técnicos dedicados al desarrollo de software. Desempeñan las tareas de análisis, diseño e implementación de la aplicación, y luego mantienen dichas aplicaciones a nivel de programación (actualización de librerías, mejoras...). Todo ello se recoge en un contrato-convenio con el cliente. El responsable de seguridad ayuda en el despliegue de las aplicaciones y en la preparación del entorno de producción para dichas aplicaciones.

No existe por definición o con dedicación exclusiva a ello, lo que se conoce como **responsable de RRHH**. Si que se coordina entre la dirección y el responsable del departamento de servicio de asistencia técnica el tema de permisos de vacaciones, bajas y luego es el responsable del servicio de asistencia quién autoriza expresamente las solicitudes realizadas a través de una aplicación. La necesidad de trabajar con otras empresas, la necesidad de contratar a alguien o de trabajar con freelance, se contrasta primero entre los del departamento implicado y se decide entre todos los empleados-socios.

En algunos desarrollos de aplicaciones se cuenta con un **freelance** para desarrollo *frontend*. Es algo muy reciente, más o menos desde hace 1 año.

2.4 Instalaciones

La empresa se encuentra en un centro de oficinas en Andoain (Gipuzkoa), donde dispone de 140m^2 de oficina. Todos los accesos al edificio están controladas por sistemas de video-vigilancia y hay servicio de conserje-portero las 24h del día. La oficina dispone de sensores de humo, aire acondicionado. Los baños y el comedor son espacios comunes y separados de la oficina.

2.5 Diagrama de la red tecnológica

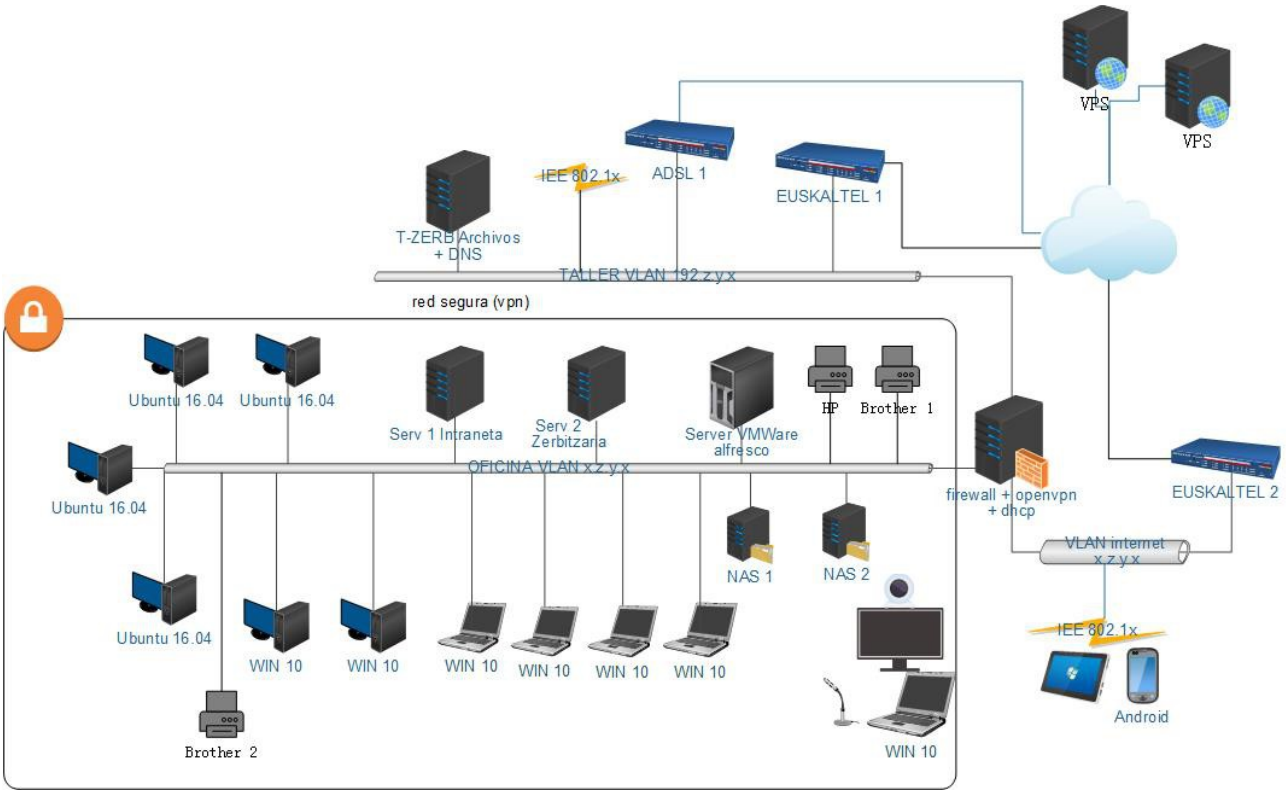

Imagen 2: Diagrama de la red tecnológica

La oficina está distribuida en varias salas, pero en dos VLAN a nivel de red. Uno es el taller, y el otro la "oficina". El taller es para que los del servicio de asistencia técnica trabajen con equipos de clientes. La oficina es para equipos propios, pero está permitido el acceso remoto usando una conexión VPN.

El taller tiene el siguiente rango de direcciones IP 192.168.x.y/24 . Dispone de una conexión a internet por fibra óptica de Euskaltel, otra conexión auxiliar ADSL de Vodafone. El router de Vodafone también permite conexiones Wifi (IEEE 802.1x). En el taller hay un switch 52 (1000/100) solamente para ofrecer puntos de conexión y gestionar tráfico (en este switch están disponibles las dos VLAN)

Hay un servidor Windows Server 2008, la cual se usa por un lado para tener un repositorio de programas que se suelen usar para instalaciones y reparaciones, y también hace la función de servidor DNS . El servidor cuenta con un SAI que también protege el switch del taller y el router de Vodafone. A día de hoy este servidor no tiene antivirus.

Por otro lado, en el taller hay 8 monitores, para conectar los equipos a reparar.

En en VLAN "oficina" (192.168.x.y), hay dos servidores NAS. En NAS 1 se guardan copias de seguridad de la información de la empresa (contenido de un alfresco,y de NAS2) y de algunas de las bases de datos de aplicaciones web de clientes.

Por otro lado, hay 4 dock stations, para los portátiles de los técnicos del departamento de servicio técnico. Los técnicos usan Windows 10 con ESET NOD32

El gerente y el responsable de facturación+ventas, tiene dos equipos con Windows 10. Los equipos de windows 10 están protegidos con ESET NOD32 .

Los programadores y responsable del departamento de desarrollo, trabajan con equipos con Ubuntu 16.04 LTS. El responsable de seguridad también trabaja con Ubuntu 16.04 LTS.

Los equipos tienen entre 3 y 4 años de antigüedad.

En la "oficina" también hay 3 servidores:

- Serv 1 "intraneta": se encuentra una WIKI y un Drupal con el fin de guardar manuales, calculadora de precios, detalles técnicos sobre proyectos... FreeBSD 9.1. .
- Serv2 "zerbitzaria": servidor de Subversion (SVN), nagios, cacti, aplicación de gestión de licencia de empleados (vacaciones, permisos...), cipher (una aplicación que guarda cifrada toda la información delicada de los CMDB de los clientes. Ofrece una API). También se descarga del servidor de correo (está en un server de OVH en territorio UE) el correo de info@secureteam.com e internet@secureteam.com usando *fecthmail* (imap) que son las direcciones más extendidas y usadas por la empresa con clientes y compartida por varios empleados de la empresa, de esas 2 direcciones hay 10 años de correo almacenado. FreeBSD 11.
- VMWare 5: Ubuntu 14.04 virtualizado: Instalado un alfresco. Se usa para ir creando y compartiendo documentación de clientes...

Firewall es un Debian 9, y tiene el servicio DHCP para asignar direcciones de todas las redes, y también hace la función de servidor VPN.

Hay un armario que alberga los 3 servidores, el firewall, los 2 NAS y el switch principal, y los 2 cable modem de Euskaltel. Hay un SAI que protege todos estos equipos.

Todos los empleados disponen de smartphone de la empresa, tanto para uso laboral como personal. El gerente también tiene una tablet.

En la sala de reuniones, conectada a la VLAN "oficina", hay una TV+webcam+micro y un portátil con win10.

También hay 3 impresoras en la vlan "oficina": 1 HP Laserjet, y 2 Brother.

Como ya se ha indicado, hay ciertos servicios que están alojadas en servidores externos contratadas al proveedor OVH. Los servidores están en países de la UE . Entre ellos se puede destacar una VPS en la cual se encuentra la aplicación de gestión de presupuestos y convenios con los clientes, incidencias, contactos de clientes, de proveedores, planificación de tareas y, CMDB de clientes haciendo uso de a la aplicación *cipher* (API de aplicación en Serv3)...

Luego también hay contratadas diferentes VPS y servers para hosting de aplicaciones web de clientes.

Hay otro VPS contratada con Euskaltel situado en el data center de Zamudio.En ella está instalada la aplicación de facturación "enbor". Hay que acceder a través de VPN.

Los smartphone tienen cliente VPN para acceder a la VLAN de "oficina"

Se cuenta con una cuenta en *Bitbucket* y *JIRA Cloud* para trabajar con los *freelance*.

2.6 Estado inicial de la seguridad de la información

Haciendo una breve descripción de alto nivel, se podría decir que a nivel técnico hay bastantes medidas técnicas de seguridad desplegadas. Pero se podría decir, que dichas medidas se han desplegado con el paso del tiempo y porque hay una persona que tiene un amplio conocimiento de las redes y que ejerce de "responsable de seguridad". Resumiendo, se han desplegado medidas pero no de una manera planificada y con un respaldo general, más bien, según venían problemas o nuevas necesidades y de manera bastante improvisada o sin seguir un plan. No hay un marco establecido o políticas que indiquen como se debe de trabajar en el departamento con la información. Hubo unos intentos de implantar ciertas políticas y ciertos procedimientos, pero se quedaron más a nivel del departamento de asistencia técnica y luego no se han trabajado con la totalidad de los técnicos para que estos pudieran concienciarse en la importancia y pudieran y debieran aplicarlos. Por lo tanto, se puede decir que las medidas organizativas son casi nulas, y que no existen políticas y procedimientos implantados.

2.7 Alcance

Para poder elaborar el plan de implementación, hay que definir un alcance, de esa manera no se abarcará más de lo necesario y el proceso estará enfocado a aquello en lo qué más prioridad se le ha dado.

Por lo tanto, y después de tener una reunión con la dirección de la empresa, tanto por importancia y prioridad y teniendo en cuenta la disponibilidad de recursos y tiempo que se puede dedicar de manera realista, el alcance del presente sistema de gestión de la seguridad de la información basado en la vigente norma ISO 27001 queda definido a los sistemas de información que soportan los servicios técnicos informáticos del departamento de desarrollo. Con ello se entiende desde los equipos y servidores usados del departamento, hasta los datos tratados en todo el proceso de desarrollo y posterior mantenimiento de las aplicaciones.

3. Objetivos del plan director

Cuando se quiere abordar aspectos de la seguridad de la información es importante contar con el compromiso de la dirección de la empresa, y que las tareas (técnicas y organizativas) o actividades a llevar a cabo estén planificadas. El plan debe marcar las prioridades y debe de contemplar los responsables y los recursos que se van a dedicar para mejorar la seguridad como se hace mención en la wiki de la asignatura de SGSI de la UOC http://www.uoc.edu , y en diferentes apartados de la web de Incibe (Instituto Nacional de Ciberseguridad) [Incibe, Plan Director de Seguridad],[Incibe, Plan Director de Seguridad - Un caso práctico]

Los objetivos del Plan Director deben ir alineados a los objetivos de negocio de la empresa. Luego, teniendo en cuenta la misión de la empresa y acotándolo al alcance definido, se han definido los siguientes objetivos:

- **Concienciar y formar a los técnicos** del departamento de desarrollo de la importancia de la seguridad de la información. Más allá de programar código seguro, hacerles ver que tanto el proceso de desarrollo como en el mantenimiento de la aplicación se gestiona información que requiere una gestión segura (confidencialidad,integridad,disponibilidad).
- **Definir políticas, procedimientos y normas para la gestión segura de la información** y datos de los clientes en las aplicaciones y su proceso de desarrollo. En algunos casos será más formalizar, comunicar y revisar aquellas decisiones que ya están establecidas de forma improvisada.
- **Dedicar recursos** por parte de la empresa para poder disponer de **herramientas que sirvan para evaluar y mejorar la gestión de la seguridad de la información.**.
- **Definir nuevas medidas organizativas y nuevas funciones** para poder **evaluar y poder mejorar la seguridad y la eficiencia**.

Todos esos objetivos como se ha dicho responde a la misiones que tiene la empresa, es decir, la de pretender ser más cercana y poder dar mejor asesoramiento en todos sus servicios, también en la de desarrollo, que es la que cubre el alcance. Eso requiere conocer mejor la empresa y eso requiere información y tener mayor disponibilidad para poder atender y ofrecer un servicio más eficiente. Pero para ello es importante garantizar la seguridad de toda esa información consiguiendo los objetivos definidos y trasmitiéndole esa profesionalidad y los valores de que se toman en serio los aspectos de la seguridad de la información.

4. Análisis diferencial

Análisis del estado actual de la organización, en relación a los requerimientos del anexo A del 27001:20013 o controles de ISO 27002, es bastante negativo. Aquí se recoge un resumen del análisis diferencial que está recogido en el documento **GAP 27002_2013_secure_team.xls** . La valoración es sobre 5 en base a la siguiente tabla.

ID	Nivel	Descripción
0	No existente	La organización no es consciente de que debe gestionar la seguridad. Ausencia total de procesos reconocibles
1	Inicial	La organización ha reconocido que existe la necesidad. Las actividades de los procesos se basan en el esfuerzo personal. Los planteamientos son a medida o "ad hoc", no existen procesos estandarizados o formalizados.
2	Repetible	Existe un grado de confianza en el conocimiento de los individuos y las tareas son llevadas cabo de manera similar por diferentes individuos. Los procesos no están documentados, ni las decisiones, ni procedimientos ni nada se comunican de manera formal y siguiendo un criterio establecido.
3	Definido	Hay una implicación colectiva y corporativa de toda la organización. Los controles están documentados, comunicados e implantados.
4	Gestionado	Es posible medir y monitorizar los procedimientos y controles, y se pueden tomar decisiones en base a esas mediciones.
5	Optimizado	Los procesos se pueden medir, están bajo constante mejora y además, IT son usadas de manera integrada para automatizar los workflows, proporcionando herramientas para mejorar la calidad y la eficiencia, haciendo que la organización se adapte rápidamente.

Tabla 2: Valores usado en el análisis diferencial

	Valor
A.5 Information security policies	0,5
A.6 Organization of information security	0,2
A.7 Human resource security	0,5
A.8 Asset management	1,194
A.9 Access control	0,6
A.10 Cryptography	0
A.11 Physical and environmental security	0,778
A.12 Operations security	0,524
A.13 Communications security	0,833
A.14 System acquisition, development and maintenance	0,222
A.15 Supplier relationships	0,5
A.16 Information security incident management	1,429
A.17 Information security aspects of business continuity management	1
A.18 Compliance	0,767

Imagen 3: Resumen del análisis diferencial

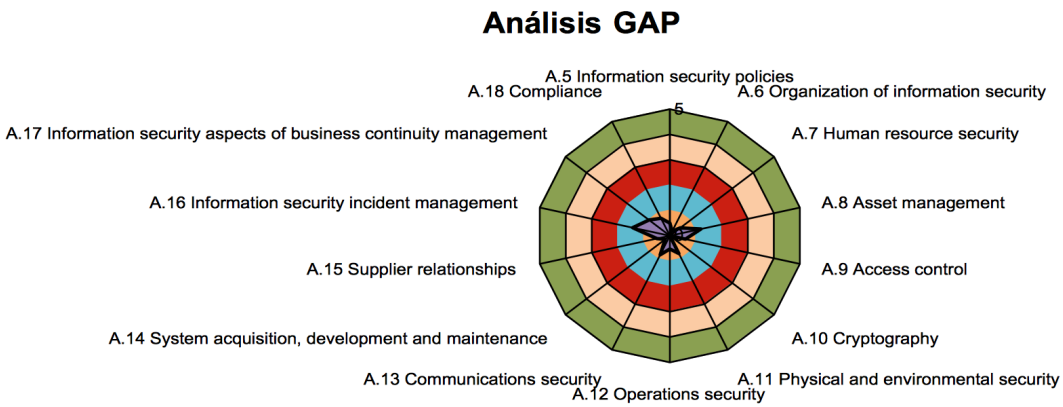

Imagen 4: Radar análisis GAP

En cuanto a los apartados de la ISO 27001:2013, todas se encuentran a 0 en este momento:

4. Contexto de la organización	No existe	No hay un estudio del entorno elaborado. No hay nada sobre SGSI, ya que a día de hoy no existe.
5. Liderazgo	No existe	La dirección no se asegure de de forma periódica y siguiendo unos criterios de que los roles y funciones se estén cumpliendo, y que la asignación de ellas se comunique. Se confía en que cada uno más o menos hace bien las cosas, se asignan trabajos y proyectos pero no hay unos perfiles, roles y tareas muy definidas, y cuando se designa algo no se comunica expresamente. Como tampoco existe una política la dirección no tiene ningún que hacer relacionado con ella.
6. Planificación	No existe	No hay objetivos de seguridad y una planificación para conseguirlos.
7. Soporte	No existe	Hay muy poca concienciación y no hay suficiente personal formado o competente en materia de seguridad. Las cosas no se comunican de manera formal ni siguiendo procedimientos. Y la información documentada no está demasiado organizada ni controlada.
8. Operación	No existe	No hay valoración ni tratamiento de riesgos.
9. Evaluación del desempeño	No existe	Como no hay nada establecido como política ni procedimientos formalizados ni normalizados. No se audita ni se revisan las cosas en base a un procedimiento y/o un proceso.
10. Mejora	No existe	Al no haber auditoría, no hay un informe de no conformidades ni de sus

		correcciones... las mejoras o nuevas medidas se hacen de forma improvisada

Tabla 3: Análisis sobre 27001:20013

Como se recoge en la tabla, se hacen cosas de manera improvisada, sin seguir unas normas establecidas. Luego no hay un plan que llevar a cabo, no hay nadie que lo tenga que tirar de ese carro, ser referente o aportar una compromiso con ello. No hay tampoco algo que se pueda evaluar de manera periódica y seria, por ejemplo, con una auditoría, y de la mimas manera no hay nada planteado para mejorar que no planteamientos para responder a problemas de cada momento.

4.1 Conclusiones

Hay una cultura establecida en la que se confía y se deja en manos del responsable de seguridad casi todo lo relativo a la seguridad de la información. No hay una cultura de implicar a toda la plantilla en dicho trabajo. Todas las medidas se implantan de manera improvisada, a base de esfuerzo técnico y sin darle importancia a las medidas organizativas.

Las mejores valoraciones son la de los controles del apartado 11.2 Seguridad de los equipos. Que aún así tiene mucho que mejorar, ya que recae prácticamente en el acierto por parte del responsable de seguridad y en el conocimiento que se adquiere con el paso tiempo. Hay que formalizar y normalizar los procedimientos y políticas. Pero por lo menos hay una concienciación sobre ello y se repiten ciertos criterios.

También hay que decir que la gestión de activos no está tan mal ya que tienen un software para llevarlo al día y bien etiquetado, y también tienen definida que es responsabilidad del gerente y del responsable de seguridad. De la misma manera, la gestión de incidentes también está bastante bien, ya que están usando un software y se hace un seguimiento en reuniones y se establecen prioridades, es decir, que se gestiona y está bastante establecido. Pero habría que formalizar los procedimientos.

La mayoría de los controles brillan por su ausencia o por su baja nota en toda la organización, luego es normal que en el departamento de desarrollo también esté al nivel general de la organización. Pero si tenemos en cuenta que el alcance está enfocado al departamento de desarrollo, hay que remarcar la baja valoración que hay para los controles dedicados a las actividades de desarrollo en sí, es decir, las 14.2 Seguridad en el desarrollo y en los procesos de soporte . Esto se debe a la falta de concienciación por parte de los empleados, falta de compromiso y falta de revisión por parte de la dirección, es imprescindible establecer procedimientos y políticas, que mínimamente vayan a cumplirse y revisar, no sirve de nada que la dirección tenga una idea y solo se quede en la idea, mientras que la falta de políticas y la aplicación de estas por parte de los técnicos de departamento no exista.

De todas formas, hay que tener en cuenta lo que se decía en la introducción, la ISO 27001 va a ser un marco que va a servir para decidir qué controles priorizar, cuáles no en base a un análisis. El estado actual, la mayoría de los controles no están implantados pero porque ni se han contemplado o la dirección no le ha dado importancia o no los ha valorado. Si no se va a implantar que no se implante, pero que sea sobre una base y siendo conscientes de lo que ello supone.

5. Esquema Documental

5.1 Política de Seguridad

La política de seguridad es una normativa interna que debe de conocer el todo el personal de la organización. La dirección de Secure Team. ha decidido adoptar un conjunto de medidas para proteger los activos estratégicos de la compañía. Entre estos activos se encuentra la información, los documentos y los sistemas de información que permiten su tratamiento, almacenamiento, comunicación y explotación, necesarios para el desarrollo de las actividades de negocio y futuro de la organización. Esas normas y directrices establecen ciertas normas para la seguridad del uso de recursos de la empresa, del tratamiento de la información de la empresa y de los proyectos y tienen el objetivo de garantizar su confidencialidad, integridad y disponibilidad.

A su vez, establecer unas normas hace que la empresa opere bajo un mismo código y que las deficiencias se puedan detectar mejor y también que puedan tomar ciertas medidas al respecto, siendo todo ello muestra de una empresa seria, con espíritu de mejora y con una aspiración a ofrecer un servicio de calidad y segura.

5.1.1 Política de Alto Nivel

La Dirección de Secure Team, consciente de la importancia que la seguridad en el tratamiento de la información tiene para toda la compañía y los clientes, ha considerado fundamental establecer el tipo de tratamiento que debe darse a la información de la que es propietaria o depositaria, durante todo su ciclo de vida y con el fin de garantizar su confidencialidad, integridad y disponibilidad, y cumpliendo escrupulosamente con todos los requerimientos legales que sean de aplicación en cada momento.

El objetivo prioritario de esta política es disponer de un sistema eficiente y eficaz para la gestión de la seguridad de la información, y como consecuencia de ello obtener el más alto nivel de garantía en su tratamiento dentro del departamento de desarrollo de Secure Team y que redunde en una mejora continua en nuestra relación interna y externa, logrando con ello que nuestros clientes perciban el compromiso de la empresa con respecto a la seguridad y a la satisfacción de los servicios ofrecidos.

Para lograr estos objetivos, la dirección se compromete a facilitar, por todos los medios a su alcance y de forma proporcional a los riesgos detectados, los recursos necesarios para que el departamento disponga de un entorno alineado con los objetivos de negocio y los objetivos de seguridad plasmados en toda la documentación desarrollada a partir de esta política. Esta política y toda la documentación relacionada serán distribuidas por canales adecuados y en base a la necesidad del conocimiento a todos las partes interesadas.

Todas las partes implicadas se comprometen a cumplir y a hacer cumplir todos los principios de seguridad que la dirección ha establecido, garantizando la protección de la información en todo momento, y evitando y colaborando a que la seguridad de la información sea mantenida de forma permanente.

La dirección cuenta con la colaboración de todos sus empleados y asume la responsabilidad de motivar y formar adecuadamente a todos ellos. Éstos están en la obligación de alertar, de manera

oportuna y adecuada, cualquier incidente que atente contra lo establecido en esta política.

Las actividades deliberadas contra los objetivos de esta política serán tratadas de acuerdo a la legislación y a la relación contractual existente en cada momento.

Esta política de seguridad entra en vigor el mismo día de su publicación y será revisada anualmente por el responsable de seguridad y la dirección de Secure Team.

5.1.2 Política de uso de correo electrónico

La política de uso de correo electrónico tendrá la finalidad de que todas las comunicaciones relacionadas con la actividad se hagan con un carácter oficial, y que se hagan desde este recurso propio sin hacer uso de otras herramientas externas que puedan quedar fuera del marco de la LOPD.

- El personal debe saber que el los mensajes que envía o recibe en el correo electrónico de la compañía no son ni personales ni privados. La empresa puede supervisarlo a partir de que se reserva y comunica este derecho en esta misma política.

- Cada empleado es el responsable de proteger el correo con una contraseña adecuada y siguiendo los criterios definidos en la política de contraseñas.

- No está autorizado el uso del correo electrónico de la compañía para asuntos personales

5.1.3 Política de contraseñas

La política de contraseñas tiene el objetivo de proteger los recursos frente a accesos no autorizados.

- La contraseña debe ser modificada semestralmente. No está garantizado la configurarán en los sistemas para que fuerce a dicho cambio, por lo tanto, será responsabilidad del empleado acordarse y cada 6 meses recibirá una notificación del Responsable de Seguridad vía correo electrónico como recordatorio.

- Cada empleado es responsable de proteger en secreto su contraseña.

- Esta prohibido revelar o comunicar la contraseña, no hay que hacerlo bajo ningún caso, ni a petición de la dirección.

- No se debe anotar dicha contraseña en ningún papel ni recurso accesible y/o que no esté cifrada y protegida bajo otra contraseña.

- La contraseña debe ser distinta a usada en recursos personales

5.1.4 Política de uso de los servicios en red

La política de uso de servicios de red afecta tanto a empleados internos como a externos, y tiene como objetivo que el uso de la red se con garantías de preservar la confidencialidad y hacer un buen uso de cara a evitar incidentes de seguridad.

- No se revelará ninguna clave de redes inalámbricas a personal ajeno a la empresa.
- Solo se podrán conectar a las red de la empresa dispositivos propiedad de la propia empresa o autorizadas por el responsable de seguridad.
- No se visitarán páginas que puedan contener malware, ni se podrán descargar ficheros no necesarias para el desarrollos de actividades de la empresa.
- Todos los dispositivos con conexión a la red deben de tener el antivirus seleccionado por el responsable de seguridad.
- Para conectarse a la VLAN "oficina" desde el exterior, hay que usar VPN.Para ello, será la dirección quien lo autorice y proporcione un usuario y contraseña.

5.1.5 Política de uso de los recursos de comunicación

La Política de uso de los recursos de comunicación de Secure Team tiene como finalidad el promover el uso responsable de los sistemas de comunicación electrónica, en particular: el teléfono, el correo de voz, el correo electrónico y el fax, por parte de la compañía.
Los sistemas de comunicación y los mensajes generados y procesados por tales sistemas, incluyendo las copias de respaldo, se deben considerar como propiedad de Secure Team y no propiedad de los usuarios de los servicios de comunicación.

- Está prohibido el uso de los sistemas de comunicación para propósitos de entretenimiento y diversión.
- Todas las comunicaciones de correo electrónico o de cuentas de la empresa, se consideran oficiales, por lo que no se pueden hacer públicas las comunicaciones por parte de alguien que no tenga expresa autorización para ello por parte de la dirección. Por ejemplo, escribir en foros.
- Cualquier clave o contraseña que se tenga que comunicar o información confidencial, deberá ser usando medios seguros, es decir, firmados y cifrados por claves asociadas a correos de la compañía.
- Queda prohibido el uso de servicios de mensajería instantánea y correos de servicios externos para comunicaciones con información de actividad de la empresa.

5.1.6 Política de dispositivos móviles

El objetivo es el correcto uso de los activos móviles de la compañía.

- Cada empleado dispone de un smartphone para uso laboral y privado. Pero el dispositivo es propiedad de la empresa.
- Los portátiles de las instalaciones solo saldrán para uso laboral, así como, reuniones con los clientes, presentaciones...
- No se podrá llevar a casa ningún portátil de la empresa, a menos que se tenga autorización por parte de la dirección. Y siempre deberá de devolverlo en el plazo indicado.
- Cuando se saque un portátil de las instalaciones, se llevará en una bolsa o mochila protegida.

5.1.7 Política de software

Todos los empleados deben saber que el software que se use en los equipos de la empresa serán de fuentes y fabricantes seguras, con licencias legales en caso de tenerla, y siempre supervisadas por el responsable de seguridad.

- No podrán usarse servicios ni instalarse programas o software que no estén en la lista elaborada por el Responsable de Seguridad o sin la autorización expresa por parte del Responsable de Seguridad.
- Cada empleado será responsable de actualizar su sistema y software cuando así se le comunique por correo desde la dirección o por parte del Responsable de Seguridad.

5.1.8 Política de desarrollo de software y propiedad intelectual

Esta política es para los empleados del departamento de desarrollo, definiendo los mínimas normas de generación de documentación en proyectos y sobre su propiedad, de tratamiento de información de clientes en las aplicaciones desarrolladas.

- Los programadores deberán de llevar el control de versiones a través de los recursos de la empresa (servidor subversion)
- Se documentarán todos los desarrollos y se almacenarán en el servidor de Alfresco en la carpeta correspondiente al cliente-aplicación, el responsable de desarrollo deberá de contemplar un plazo o un tiempo para ello en cada proyecto. Se añadirá un enlace en la Wiki o una referencia de lo que se documente en Alfresco.
- Cualquier truco, observación o aspecto técnico a destacar, se documentará en la Wiki de la empresa, bajo el apartado de "programación".

- Todo el código, documentación y comunicación de los desarrollos realizados por los empleados en la compañía y para clientes de la empresa son propiedad de la empresa y/o del cliente según el contrato acordado entre ambas partes, nunca serán propiedad de los empleados.

- Las contraseñas de acceso a aplicaciones de clientes deberán de almacenarse en *Cipher* y etiquetarlas correctamente

- Se comunicará al responsable del departamento de desarrollo y al responsable de seguridad, cuando ya se obtenga algún dato del cliente para cargar, o se tenga que pasar a fase de producción, para que estos preparen e implanten los procedimientos adecuados tanto a nivel de configuración de servidores como a nivel de copias de seguridad.

- Queda prohibido la revelación de información de clientes y de la empresa a ajenos de la empresa.

- Solo se podrá crear usuarios con privilegios de administración a un cliente para una aplicación si la dirección lo autoriza.

- Los cambios y desarrollos se harán en el entorno de desarrollo, nunca en producción.

- La aplicaciones en entorno de producción y que usen información sensible, datos personales o contraseñas o que presten servicios de comercio electrónico (ventas, reservas...) irán bajo protocolos seguros (SSL/HTTPS...) y con medidas de no duplicidad, identificación, etc.

- Se testearán, probaran o se revisarán los cambios en entorno de desarrollo y en producción.

5.2 Procedimiento de Auditorías Internas

Documento que debe incluir una planificación de las auditorías que se llevarán a cabo durante la vigencia de la certificación (una vez se obtenga), requisitos que se establecerán a los auditores internos y se definirá el modelo de informe de auditoría.

El objetivo de este procedimiento es definir los procesos y aspectos para realizar auditorías internas en Secure Team que comprueben la idoneidad del diseño e implementación del SGSI.

5.2.1 Alcance

Lo dispuesto en esta instrucción sobre auditorías es aplicable a todos los procesos del Departamento de Desarrollo de Secure Team.

5.2.2 Planificación de auditorías

Las auditorías internas se realizan por iniciativa del Comité de Seguridad una vez al año. Para

realizar la auditoría hay que planificar cuándo, sobre qué y qué recursos se necesitarán. El Comité de Seguridad será el responsable de definir el alcance, el objetivo y la duración de cada auditoría, aprobar los recursos a destinar, y aprobar la composición del equipo auditor. En dichas planificaciones es conveniente tener en cuenta las siguientes consideraciones:

- Las fechas deben ser establecidas de forma que perturben lo menos posible la actividad normal de la Empresa.

- La frecuencia con la que se deben realizar las auditorías del Sistema depende sobre todo, del grado de implantación del Sistema y de la importancia de los cambios que se hayan producido en los procesos. Aunque se ha decidido que sean anuales, podrían variar por necesidades o cambios que puedan surgir en la empresa o en sus políticas.

- Los requisitos de las Normas de referencia y la legislación vigente y todos los procesos deben ser auditados como mínimo una vez cada 3 años.

- La empresa pondrá a disposición de los auditores entre otros recursos para la realización de pruebas técnicas, y documentación de la ISO 27007 que ofrece una guía para las auditorías de SGSI (internas, externas, programa de auditorías) y establece las competencias del auditor.

- Por motivos de recursos y por interrumpir lo mínimo la actividad habitual de la empresa, el Comité de Seguridad a decidido distribuir la auditoría de controles de la siguiente manera para ciclos de 3 años (teniendo en cuenta que la revisión de requisitos del 4 al 10 de ISO 27001 hay que hacerlo todo los años):

    - 1. año: auditar requisitos ISO/IEC 27001:20013 apartado 4 al 10, y controles de ISO/IEC 27002:20013 del A.5 al A.9
    - 2. año: auditar requisitos ISO/IEC 27001:20013 apartado 4 al 10 y controles de ISO/IEC 27002:20013 del A.10 al A.14
    - 3. año: auditar requisitos ISO/IEC 27001:20013 apartado 4 al 10 y ISO/IEC 27002:20013 del A.15 al A.18

Por lo tanto, planificación de cada auditoría por lo tanto tendrá que tener en cuenta esa distribución.

5.2.3 Aprobación del Plan de Auditorías

La planificación de Auditorías deberá se aprobada por la dirección de la Empresa.

5.2.4 Comunicación del Plan de Auditorías

Una vez aprobada el Plan de Auditoría, habrá que comunicarle a través del correo y con un mes de antelación al responsable del departamento afectado, en este caso al responsable del Departamento de Desarrollo. Asimismo, se le comunicarán las revisiones o posteriores modificaciones significativas del Plan. De todas formas, el Plan estará disponible para toda la empresa en el servidor de Alfresco, en el directorio de Secure Team.

5.2.5 Designación del equipo auditor

Antes de realizar la auditoría, se designará un equipo auditor, que será quien lo lleve a cabo.
Este equipo debe cumplir con las siguientes características:

- Será liderado por el coordinador del Comité de Seguridad

- Para que la auditoría de buenos resultados, se tendrá en cuenta el principio de independencia en la medida posible, objetividad e imparcialidad. Por lo que no habrá nadie del departamento auditado en el equipo auditor que audite dicho departamento.

- El equipo auditor, al ser un departamento pequeño, estará formada por dos personas.

- Tener una experiencia mínima de seis meses en actividades de gestión seguridad de la información y formación en su auditoría (por ejemplo título del curso de Lead Auditor). La empresa asumirá los gastos de dicha formación.

5.2.6 Ejecución de la auditoría

La auditoría se dividirá en 4 fases:

- **Recolección de información previa**: esta información servirá para preparar las pruebas de auditoría con un mejor entendimiento de los procesos, cargos/roles y políticas y procedimientos que afectan al departamento y a los procesos a auditar.

- **Ejecución de la pruebas de auditoría**: habiendo recopilado y estudiado la información necesaria del entorno y los procesos a auditar, habrá que llevar a cabo las pruebas recogidas en el plan de auditoría. Las prácticas serán la **revisión de documentación**, **realización de entrevistas** y **ejecución de pruebas técnicas**.

- **Análisis de la información**:En realidad, el proceso de análisis se inicia desde el mismo momento en que comienza la ejecución de la auditoría y únicamente finaliza con la aceptación por parte del auditado de la última revisión del informe de auditoría. Pero el equipo auditor deberá llevar paralelamente la ejecución de ciertas pruebas con el análisis de la información que extraiga de ellas. Uno de los aspectos que el auditor deberá ir evaluando es la importancia relativa o el riesgo de no conformidad del problema que detecte.

- **Reporting de la auditoría**: Una vez realizadas las distintas pruebas y el análisis de la información obtenida, el equipo auditor trasmitirá sus conclusiones en a través de un informe al Comité de Seguridad, que es quien promueve estas auditorías, y también a la dirección de la empresa y al responsable del Departamento de Desarrollo. El informe será elaborado por parte del líder del equipo auditor.

5.2.7 Informe de auditorías

El informe que se elaborará en la 4 fase de la ejecución de auditoría, debe ser claro, simple y lo más directo posible y siempre facilitando la información relevante. Al mismo tiempo, debe facilitar de

manera sencilla la forma de resolver las deficiencias halladas o por lo menos recomendar ciertas acciones o medidas correctivas.

El informe debe incluir los siguientes puntos:

- **Resumen ejecutivo**: En ella se reflejará de manera resumida el contenido del informe. Incluirá, por tanto, una introducción, una visión general de la metodología empleada, las principales conclusiones que se hayan obtenido y las recomendaciones más relevantes que el equipo auditor pueda dar. El lenguaje empleado será lo más directo y comprensible para un público amplio ya que debe ser leído por parte de responsables de poco conocimiento técnico. Además, empezar con este apartado, puede servir para poder ofrecer un pequeño adelanto a los cargos interesados que requieran cuanto antes el informe.

- **Metodología empleada**: una explicación de la metodología empleada.

- **Listado detallado de los hallazgos**: No hay que confundirlos con los resultados de las pruebas. Este apartado recoge las los hallazgos de no conformidades o de aspectos a mejorar.

- **Anexos**: Se recogerá la información que ha dado lugar a los hallazgos, es decir, resultados de pruebas técnicas, resultados de las entrevistas ...

En un plazo de dos semanas después de la emisión del informe, el responsable del Departamento de Desarrollo deberán de emitir un informe al Comité de Seguridad con acciones correctivas correspondientes a resolver o a responder a las no conformidades detectadas en la auditoría a su departamento indicando la fecha de la aplicación de estas. Para ello se utilizará un documento Excel que tendrá dos columnas, una "Informe de No Conformidad" y otra "Acción Correctiva o Preventiva", y está se guardará en Alfresco, bajo el directorio de Secure *Team / Auditorías / Acciones Correctivas*, una vez subido, se le notificará al Comité de Seguridad por correo electrónico.

El Coordinador del Comité de Seguridad verificará que las acciones correctivas propuestas sean coherentes con las no conformidades detectadas en la auditoría, requiriendo su modificación, si fuera preciso. Las fichas correspondientes a todas las acciones correctivas previstas darán lugar al Plan de Acciones Correctivas.

En cuanto a las acciones preventivas, el Comité de Seguridad decidirá de acuerdo con el contenido del Informe de Auditoría, la necesidad de implantar acciones preventivas.

Se ha utilizado documentación de la asignatura de Auditorías Internas de la UOC para la redacción del procedimiento de auditorías internas [Estevan de Quesada,2017].

5.3 Procedimiento de comunicaciones relativos al SGSI

En este procedimiento se define quién realiza los comunicados internos/externos relativos al SGSI, a través de qué canal y formato de los mensajes.

- Los mensajes se escribirán desde el correo sgsi@secureteam.com .

- Será el Responsable de Seguridad quién haga estas comunicaciones, es responsabilidad del Responsable de Seguridad no revelar la contraseña de dicho correo a ningún otro miembro de la empresa, ni al gerente. Si el responsable no pudiera emitir un comunicado (baja, vacaciones...), lo hará el gerente desde su cuenta corporativa.
- En caso de que el envío lo haga el gerente, deberá incluir como receptor (copia carbón) siempre a sgsi@secureteam.com .
- Los mensajes en el campo “asunto” empezarán con “SGSI”
- El mensaje deberá ir firmado

5.4 Gestión de indicadores

Es necesario definir indicadores para medir la eficacia de los controles de seguridad implantados. A continuación se recoge una tabla en la que establece indicadores para cada control, detallando el objetivo del control, la frecuencia a revisar el control, la formula para medirlo y el margen de tolerancia que se permite y quien es el responsable de la medición.

Control	Objetivo	Frecuencia	Fórmula/Tolerancia	Responsable
Política de Seguridad	Comprobación anual de dirección	Anual	Mínimo consta un acta sobre revisión	Responsable Seguridad
Organización de seguridad de información	75% de responsabilidades asignadas	Anual	Comprobar organigrama y contratos 50% o menos no es tolerable	Responsable Seguridad
Procedimiento de contratación y condiciones	0 screening 0 empleados con contratos sin condiciones bien definidas (durante,cese...)	Anual	Revisar contratos No se tolera ningún contrato mal	Gerente
Gestión de activos	100% activos etiquetados y asignados 0 incidentes de usos no autorizados	Anual	Revisar el CMDB actualizado. No se tolera menos de 80% activos gestionados. Existen quejas o parte de algún responsable de activo. Se tolera una por empleado cada 6 meses.	Responsable Seguridad
Gestión de accesos	Existencia y comunicación de política. 100% equipos con contraseña	Semestral	Entrevistar y comprobar o revisar resultados de auditoría libre de no conformidad en estos puntos. Y plan de corrección sin dichos temas. No se tolera ningún empleado no informado desconozca. Ningún equipo sin contraseña.	Responsable Seguridad y Responsable de departamento.
Criptografía	El 100% de copias de seguridad con datos personales encriptados. Claves de acceso a servidores y administradores guardados cifrados 100%	Semestral	0 ficheros en servidor de copias clientes que no terminen en .gpg Buscar palabras contraseña,password,pasahitza,clave en la base de datos de la WIKI, en alfresco, y equipos. No se tolera ni una sola clave almacenada sin cifrar, excepción en ficheros de configuración.	Responsable Seguridad

Seguridad física y perimetral	Extintores, aire acondicionado y detector de humos revisados anualmente.	Anual	Constancia del acta de revisión de la revisión aire, detector humos y extintores en copia No se tolera que pase más de un año sin revisar	Gerente
Seguridad operacional	100% equipos con IDS Solo programas autorizados Hacen copias de servidores y servicios	Semestral	Comprobar compra licencias Elaboración lista programas actualizada y enviado por correo a empleados al menos cada 2 meses. Comprobar fechas registro de copias. No se tolera más de una semana sin copias.	Responsable seguridad
Seguridad en comunicaciones	0 intrusiones en la red 0 denuncias o avisos recibidos	Trimestral	No se tolera ninguna denuncia. Se tolera un aviso/advertencia interna mensual	Responsable seguridad Gerencia
Cumplimiento	Cumplimiento total de política Cumplimiento de recomendaciones de la asesoría jurídica	Anual	Revisar conclusiones de la auditorías. Por lo menos cumplir 80% de política. Por lo menos cumplir un 90% de recomendaciones de asesoría	Responsable Seguridad Gerente
Concienciación y compromiso con la seguridad	0 empleados que desconozcan la política Reunión quincenal (o 2 reuniones mensuales) de comité de seguridad	Trimestral	Checklist/test sencillo a empleados y resultados de auditoría Se tolera que un empleado que lleva menos de un año conozca solo e 30% de política. Comprobar fechas de actas de comité de seguridad. Por lo menos 1 reunión mensual.	Responsable Seguridad

Formación en seguridad	Responsable y miembros del comité formados y al día	Anual	Existen justificantes, títulos, facturas de cursos, libros... Por lo menos un curso o un libro al año.	Gerente

Tabla 4: Indicadores

5.5 Procedimiento de Revisión por Dirección

Este procedimiento tiene por objeto establecer el criterio de revisión del Sistema de Gestión de Seguridad de la Información (SGSI) que debe llevar a cabo la Dirección de la Secure Team. Esa revisión debe ser periódica, por lo menos debe hacerse una vez al año. La dirección debe usar medios para medir los controles y hacer un correcto seguimiento del sistema, para así poder tomas decisiones en la buena dirección de mejorar la gestión.

Para ello la dirección, junto a por miembros del comité de seguridad deberá de conocer el cumplimiento de las política de Seguridad los resultados de las auditorias, las acciones correctivas y preventivas que se están llevando a cabo. El SGSI debe estar alineado a los objetivos de negocio, luego también tendrá que contar con el feedback de los clientes, los resultados económicos de la empresa, noticias e información publicada sobre la empresa, propuestas y quejas del personal... Con todo ello deberá de adoptar decisiones para la mejora de la gestión, como puede ser destinar más recursos económicos y/o humanos, proponer modificaciones en la política de seguridad...

5.6 Gestión de Roles y Responsabilidades

El Sistema de Gestión de Seguridad de la Información tiene que estar compuesto por un equipo que se encargue de crear, mantener, supervisar y mejorar el Sistema. Este comité debe de contar al menos con un miembro de la dirección, con ello se consigue que la dirección esté al corriente y que las decisiones de seguridad se contrasten con la dirección y se ajusten a los objetivos de negocio de la empresa.

5.6.1 Propuesta de Comité de Seguridad y aprobación

Este equipo lo propone la dirección de la organización en el que ya está el responsable de la seguridad y es presentado y aprobado por la junta de socios, con lo que le reconoce una autoridad en materia de gestión de seguridad.

5.6.2 Miembros del Comité de Seguridad

En Secure Team el comité de seguridad será bastante reducido, ya que la empresa está compuesta solo por 10 empleados-cooperativistas compuesta por 3 departamentos. Por lo tanto con un número reducido ya estarían representadas los departamentos y cubiertos los perspectiva de todos los procesos. Hay que tener en cuenta, que el alcance de la implementación se limita al Departamento de Desarrollo. Por lo tanto, el Comité de Seguridad de Secure Team estará compuesta por los siguientes cargos:

- Responsable de Seguridad
- Responsable de Departamento de Desarrollo
- Gerente

En el caso de Secure Team, los dos miembros de la dirección toman parte en el comité de

Seguridad, lo cual hará que ciertas decisiones que se tengan que aprobar por parte de la dirección se puedan tomar en la misma reunión si así lo quieren.

5.6.3 Funciones del Comité de Seguridad

Las funciones designadas al comité de Seguridad son las siguientes:

- Presentar a la dirección las políticas, normas y responsabilidades.
- Aprobar roles y funciones en materia de seguridad de la información.
- Aprobar el Plan Director de Seguridad.
- Elaborar los planes de auditoría.
- Analizar los informes de auditoría.
- Revisar y aprobar el plan de medidas correctivas.
- Revisar las incidencias destacadas.
- Proponer a la Dirección la destinación de recursos para la gestión de seguridad.
- Velar por el cumplimiento de la legislación en materia de información.
- Hacer seguimiento del sistema de gestión. Y promover la formación e concienciar a los miembros de la empresa, y especialmente del Departamento de Desarrollo.

5.6.4 Responsable de Seguridad

Para poder tener una perspectiva global y que tenga información de toda la gestión de la seguridad de la información nombra a un responsable de seguridad. Siendo Secure Team una empresa pequeña, y sabiendo que los empleados no solo tienen un rol asignado, a continuación se definen las funciones mínimas que debería de desempeñar el responsable:

- Revisar periódicamente el estado de la seguridad en cuestiones organizativas, técnicas o metodológicas. Para ello basándose en la tabla de indicadores definidos.
- Actuar como referente en materia de seguridad de la información, lo cual incluye una actitud atenta, sensible y activa sobre cuestiones de seguridad, y una actitud ejemplar en el cumplimiento de las políticas.
- Estar formado y conocer aspectos técnicos de la seguridad.
- Diseñar la seguridad de los sistemas de información, monitorizar y hacer un seguimiento la seguridad a nivel tecnológico (gestión activos, estado de la red, vulnerabilidades...).

- Distribuir información interesante, visión, cultura y aspectos técnicos en torno a la seguridad en coordinación con el Responsable del Departamento.

- Contribuir en la estimación de costes de inversiones en seguridad y aclaración de aspectos de seguridad frente a la dirección y en el Comité de Seguridad.

5.6.5 Gerente

A continuación se detallan las funciones del gerente en cuanto a materia de seguridad y lo que debería de aportar en el Comité de Seguridad:

- Analizar los objetivos de la seguridad desde la perspectiva de negocio.

- Velar por el cumplimiento de la ley relativa a la información (LOPD, LSSI...). Ser el contacto y responsable para trabajar junto a la asesoría jurídica.

- Aportar aspectos decisivos para la dedicación de recursos tanto humanos como económicos que se destinarán a de forma explicita y directa a la gestión de la seguridad.

- Hacer labores de comunicación en juntas de socios, presentando los aspectos más relevantes, los resultados de auditorías y una valoración general del estado de la seguridad en la empresa.

5.6.6 Responsable del Departamento de Desarrollo

El alcance de la implementación del SGSI está limitado al Departamento de Desarrollo, por lo que las funciones del responsable de dicho departamento serán muy importantes de cara a que en ese departamento se tomen en cuenta los aspectos de seguridad de la información.

- Hacer seguimiento del cumplimiento de procedimientos por parte de los miembros del departamento.

- Hacer seguimiento de las políticas por parte de los miembros del departamento.

- Tratar cualquier propuesta, incidente o problema relativo a la seguridad (técnico, organizativo, procedimiento, política) en el Comité de Seguridad.

- Fomentar concienciación en torno a la seguridad de la información en los miembros del departamento.

- Coordinar con el responsable de seguridad para

5.6.7 Responsable RRHH

Su función básicamente es la siguiente:

- Hacer seguimiento de la licencia de horas de los trabajadores y gestionarla de manera que ningún proceso o departamento se paralice.
- Informar de cambio, problemas y de permisos a la dirección.
- Colaborar a petición del Comité de Seguridad para la planificación de ciertas tareas como la de auditorías internas para que dichas labores de puedan dar afectando lo mínimo al funcionamiento diario de la empresa.
- Tratar las posibles sanciones o medidas disciplinarias junto al Comité de Seguridad cuando este le informe de algún suceso grave y si no, por norma reunirse una vez al año para las no graves.

5.6.8 Personal del Departamento de Desarrollo

Son el personal del departamento en el que les afecta el Plan de Implementación del SGSI, por lo que deben deben de llevar cabo las siguientes funciones:

- Cumplir con la Política de Seguridad.
- Usar correctamente los recursos de la empresa.
- Valorar los aspectos de la seguridad de la información, cumpliendo y respetando los procedimientos establecidos.
- Tener una actitud activa para la mejora en gestión de seguridad, proponiendo mejoras y haciendo aportaciones de forma constructiva en una mejor gestión de la información y de soluciones técnicas.
- Informar de problemas, incidentes, ataques o vulnerabilidades que detecte.
- Preservar el secreto profesional y la confidencialidad.
- Cumplir la ley relacionada al tratamiento de la información (LOPD) y a algunos desarrollos de aplicaciones (LSSI) entre otras.

5.7 Metodología de Análisis de Riesgos

El objetivo de este apartado es definir la metodología que se aplicará para el análisis y gestión de riesgos. Secure Team ha decidido basarse en la metodología de SP800-30 de NIST. Es una metodología elaborada por el Instituto Nacional de Estándares y Tecnología de Estados Unidos (National Institute of Standards and Technology). Por lo tanto, una metodología de origen americano, y las valoraciones que se realizan no son económicas, sino que son más cualitativas.

Siendo Secure Team una empresa pequeña, la cual no puede destinar demasiados recursos humanos a realizar un estudio tan detallado de los activos como la establecida por MAGERIT (tratar los activos sobre la base de su valoración económica hace que el método sea más costoso), se ha decidido adoptar la metodología NIST.

En NIST hay que abordar **dos fases principales**, por un lado está el **prepararse para el análisis de riesgos**, y por otro llevar a cabo **el análisis en sí**. Es decir, en la primera, se define el objetivo o lo que se espera obtener del análisis, el alcance, referencias o qué tipos de fuentes de información se usarán, modelo, enfoque, modo de cuantificación... Y en el segundo, se van rellenando ciertas tablas en base a lo definido en la primera fase.

La información relativa a la primera fase, se desarrollará a continuación:

Dentro de NIST diferentes enfoques para abordar el análisis de riesgos. Está el orientado a activos/impacto (assets/impact oriented), orientado a vulnerabilidades (vulnerability oriented), y el orientado a amenazas (threat oriented). Se ha decidido seguir un modelo orientado a amenazas. Eso quiere decir, que las tareas o pasos que se llevarán a cabo girarán en torno a amenazas identificadas.

Por otro lado, la cuantificación del riesgo puede ser cualitativa, cuantitativa, semi-cuantitativa (qualitative, quatitative, semi-cuantitative). La cualitativa tiene la ventaja de que está en lenguaje transmitible y reflejable como tal en los resultados a entregar (por ejemplo: alto, bajo, etc.), hay que remarcar que da lugar a interpretaciones incluso tratando de expertos, ya que cada cual interpretará el valor en base a sus experiencias. Por otro lado, dificulta la priorización dentro de los elementos valorados con el mismo valor. La cuantitativa ofrece precisión aunque a posteriori también puede generar dudas en cuanto a la interpretación de esas cuantificaciones, pero como desventaja habría que remarcar que no sirve o no refleja demasiado para quién no lo entienda, y además para poder hilar fino y precisar un número y asignarlo correctamente hay que tener mayor capacidad o conocimientos, más información, recursos y tiempo, lo cual supone un mayor coste. La semi-cuantitativa ofrece una solución intermedia, pero se sigue necesitando capacidad y más tiempo que en la cualitativa. Por lo tanto, y atendiendo a un primer análisis y a los recursos económicos de Secure Team y el tiempo disponible para el análisis, se empleará el **modo cualitativo.**

A continuación se enumerarán las tareas o pasos que se seguirán para obtener finalmente el resultado o la identificación/cuantificación del riesgo. En cada paso se definirá qué información o fuentes de información se usarán o se podrán usar para completarlo, y también los rangos o los valores.

Se han usado tanto el propio documento de NIST SP 800-30 [NIST, 2012] como material de la asignatura de SGSI de la UOC [Cruz, 2007] para la definición y redacción de la metodología de análisis de riesgos que se recoge en este apartado 5.7.

5.7.1 Identificación fuentes de amenaza

Se identificarán las diferentes fuentes de amenazas y se clasificarán en dos categorías. Por un lado, fuentes de amenazas provocadas o intencionadas, resumiendo, atacantes, enemigos o adversarios. Y por otro las no provocadas o no intencionadas. Dentro de esta segunda categoría se encuentran las son medioambientales, accidentes, personas como fuente de despistes o errores humanos, etc. Por ejemplo, una tormenta, o una ola de calor.

En un principio la identificación de fuentes de amenaza se basará en la taxonomía marcada por NIST, la cual está definida en el la tabla **D-2** y también recogidas y traducidas en el anexo de metodología de análisis de este documento. Aunque podrán darse pequeñas adecuaciones o adaptaciones en base a la necesidad de quien realice el análisis.

En las amenazas provocadas se valorará la capacidad del atacante, la intención y la motivación de selección del objetivo. No es lo mismo, la capacidad de un grupo de hackers o la que tiene alguien que se guía por un manual de internet sin entender lo que hace, como tampoco es lo mismo, si el atacante es un grupo de hackers de USA que elige por motivos técnicos o al azar el objetivo, o alguien que a seleccionado explícitamente el objetivo y si lo conoce. La escala de valores para determinar esos factores serán las definidas por NIST en la tabla **D-3, D-4 y D-5** y también recogidas y traducidas en el anexo de metodología de análisis de este documento.

Del mismo modo, en las que no son intencionadas, habrá que determinar el rango de efectos. Es decir, no es lo mismo, un huracán que podrá afectar a todo los recursos o que la temperatura sea alta.

Se definirán fuentes de amenaza creíbles. Por ejemplo, no se ve creíble contemplar una guerra en este momento en Gipuzkoa, o un ataque nuclear, o huracanes por donde se ubica Secure Team.

Por lo tanto, entre otros, se necesitará información por parte de algunos miembros del comité de seguridad, que se aportará información sobre posibles adversarios que pudieran tener o de qué tipo (competencia, empleados descontentos, despedidos...) , también consultar en webs o recursos dedicados a la seguridad la tendencia de tipo de adversarios, consultar en base a la ubicación condiciones meteorológicas y medioambientales, etc.

5.7.2 Identificación de amenazas

En esta fase se identificarán las amenazas, su relevancia y las fuentes que puedan originarlo. Por ejemplo, una inundación la puede producir alguien de forma intencionada, alguien que por despiste se ha dejado un grifo abierto, o una tormenta. Por lo tanto, una amenaza puede ser generada o puede venir de varias fuentes de amenaza.

NIST ofrece una una lista para amenazas intencionadas y de no intencionadas. Es dos listados bastante generales (**tablas E-2 y E-3**), y en la que hay que determinar la relevancia y la fuente de amenaza. Aún así, hay que tener en cuenta que puede que haya amenazas que no es que no sean aplicables en un cierto momento, que también no tengan sentido o no resulten identificables para la realidad de la organización. Por lo que puede haber cierta adaptación de estas.

La escala de valores para la relevancia será la definida por NIST en la **tabla E-4** y también recogidas y traducidas en el anexo de metodología de análisis de este documento.

Si se determina que una amenaza es "no aplicable" (N/A), no se seguirá valorando esa amenaza en los siguientes pasos.

Como fuente de información, se usará por un lado la información generada en el paso anterior, y para determinar el valor de la relevancia, se consultará fuentes del mundo de la seguridad y también con algún miembro del Comité de Seguridad.

5.7.3 Identificación de vulnerabilidades y de condiciones predispuestas

Una vulnerabilidad se considera como una debilidad en un sistema de información, o en un procedimiento o control que pueda ser explotado por una amenaza.

Por ejemplo, tener sistemas operativos muy antiguos es una vulnerabilidad que un atacante a través de un ataque puede explotar. O no tener un sistema de ventilación puede ser una vulnerabilidad frente a situaciones o climas de calor para la amenaza de deshidratación. Es decir, se podría entender que está asociado a la falta de control o a deficiencias en controles o el grado en el que un control o salvaguardas esta desplegado. La escala de valores que plantea NIST, recogidos en la **tabla F-2** y también también recogidas y traducidas en el anexo de metodología de análisis de este documento, se basa en la gravedad de los impactos que podrían derivar la explotación de los mismos y del grado de despliegue de control.

En cuanto a las condiciones, son condiciones por defecto o que están asociadas de por sí a ciertas actividades, condiciones técnicas o tipo de negocios, en las que hacen que una amenaza iniciada o ya ocurrida tenga mayor o menor probabilidad de causar un impacto adverso. Por ejemplo, la ubicación en una zona rural una vez se valla la conexión seguramente también tardará más en repararse y eso hace que el impacto pueda ser mayor. O explicado de manera simple, ciertos tipos de actividades, conllevan ciertas condiciones las cuales hacen que se tengan que hacer las cosas de una manera especifica, por ejemplo, una clínica conlleva sí o sí a la existencia de datos muy sensibles, por lo que una intrusión en sus sistemas puede tener mayor impacto que en otra empresa de otro tipo de actividad. La escala de valores que plantea NIST, recogidos en la **tabla F-4** y también también recogidas y traducidas en el anexo de metodología de análisis de este documento

Como fuente de información se usarán datos que pueda aportar la empresa, información de pasos anteriores, información ya recogida sobre salvaguardas en este documento, y fuentes de páginas relacionadas con la seguridad de la información e informática.

5.7.4 Determinación de la probabilidad

La probabilidad que se plantea no es un mero número estadístico. Se basa en tres pasos. Primero se determina la probabilidad de ocurrencia o de que una amenaza se inicie, segundo , se evalúa si la amenaza ya iniciada u ocurrida qué impacto adverso puede causar. Finalmente, se calcula una

media partiendo de los dos aspectos mencionados.

Para las amenazas no intencionadas, la probabilidad de ocurrencia se puede guiar tanto de la experiencia, datos e informaciones para determinar de que pueda ocurrir, o también se determina la cantidad de veces que pueda ocurrir. Es decir, cuantas más veces pueda ocurrir mayor valor adquiere. Recogido por NIST en la **tabla G-3** y también también recogidas y traducidas en el anexo de metodología de análisis de este documento. En la intencionadas se puede guiar tanto de la experiencia, datos e informaciones para determinar de que pueda ocurrir.

Es necesario tener conocimiento de los controles que están desplegados ya que estos influyen tanto en la probabilidad de ocurrencia como en la probabilidad de que una vez ocurrida la amenaza tenga impactos adversos.

Como fuente de información se usarán datos que pueda aportar la empresa, información ya recogida sobre salvaguardas en este documento, y fuentes de páginas relacionadas con la seguridad de la información e informática.

En el documento de NIST no hay una tabla separada definida para estos parámetros. Están recogidas en la tabla donde se define el riesgo. En este caso, se añadirán 3 columnas en el lado derecho de las tablas de amenazas.

5.7.5 Análisis del impacto

Éste análisis define el impacto adverso en términos del daño que se causa a la propia organización y su actividad, sus activos, personal, y otras organizaciones. Por lo tanto NIST propone un listado (tabla H-2), pero podrá adecuarse en cierto modo a las necesidades o formas que requiera cada análisis. Junto a cada impacto, se detallará a qué activos afecta. Para ello, aunque NIST no lo menciona, o por lo menos, no de manera explicita en el análisis con enfoque orientado a amenazas, se hará un inventario de activos.

5.7.6 Determinación del riesgo

Partiendo de todos los pasos anteriores, se establece un cuadro de cruces que serán los riesgos que resultan de este estudio.

NIST también contempla un paso para hacer recomendaciones de controles. Pero ese apartado o esa esa tarea se recogerá en el apartado de “propuestas de proyectos”.

5.7.7 Fuentes de información

Es un breve listado de posibles fuentes de información que podrán usarse para la realización del análisis de riesgos.

- Por un lado se usará la información que se recoge en apartados de este documento, por ejemplo, organigrama de la empresa, diagrama de la red tecnológica, instalaciones, misión.

- Por otro lado, se solicitará a la empresa una serie de reuniones para poder tratar y estudiar

amenazas en base a experiencia e histórico que puedan tener o experiencias que puedan aportar. También logs, informes, etc.

- El alcance es el departamento de desarrollo, y por un lado será interesante usar referencias o fuentes de información relacionadas con la seguridad de desarrollo de aplicaciones y seguridad de la información en aplicaciones. Pero el departamento también hace uso de sistemas, redes, oficinas, software para poder llevar a cabo su actividad. Por lo que habrá que es interesante buscar información relativa a seguridad de la información, informática y sistemas de la información en general en fuentes o referencias fiables (por ejemplo: OWASP, NIST, ISO 27002, INCIBE, CERT-s (FIRST), CAPEC, CVE, etc)

5.8 Declaración de Aplicabilidad

La Declaración de Aplicabilidad es un documento que describe los controles de la ISO/IEC 27002:20013 que son objetivos, relevantes y aplicables al SGSI de la organización, basado en los resultados y conclusiones de la valoración y el tratamiento del riesgo. Por lo que aquí en la siguiente tabla habría que completarla en cada ciclo después de obtener los resultados de la valoración y tratamiento de riesgo. En la justificación se indica con que política, proceso, norma o procedimiento esta asociado.

Control	Aplica	Justificación	Origen
A.5 Information security policies			
A.5.1 Management direction for information security			
A.5.1.1 Policies for information security	si	Es la norma para todos los empleados, un documento exigido por ISO 27001	ISO 27001
A.5.1.2 Review of the policies for information security	si	Los cambios en la política requiere la revisión	ISO 27001
A.6 Organization of information security			
A.6.1 Internal organization			
A.6.1.1 Information security roles and responsibilities	si	Existe una necesidad derivada del organigrama y de las funciones Se detectan riesgos en asignación de permisos a nivel técnico	ISO 27001 En docu. de roles Análisis de riesgos
A.6.1.2 Segregation of duties	si	Existen diferentes roles/responsabilidades	ISO 27001 En docu. de roles
A.6.1.3 Contact with authorities	si	Hay servicios jurídicos contratados para gestiones legales (lopd...) Hay proveedores de servidores	ISO 27001
A.6.1.4 Contact with special interest groups	si	Hay necesidad de formarse e intercambiar conocimiento especializado.	ISO 27001 Análisis de riesgos
A.6.1.5 Information security in project management	si	Se desarrollan proyectos de información (desarrollo de aplicaciones..)	ISO 27001
A.6.2 Mobile devices and teleworking			
A.6.2.1 Mobile device policy	si	Los empleados tienen móviles y los usan en el trabajo, y además son de la empresa	ISO 27001 Política de Seg.
A.6.2.2 Teleworking	no	No se permite el teletrabajo	ISO 27001 Política de Seg.
A.7 Human resource security			
A.7.1 Prior to employment			
A.7.1.1 Screening	no	No se práctica screening o comprobación de antecedentes	ISO 27001 Recomendado por asesoría
A.7.1.2 Terms and conditions of employment	si	Hay contratos de trabajadores aunque todos son socios y deben cumplir con condiciones relativos a la seguridad de la información	ISO 27001 Recomendado por asesoría
A.7.2 During employment			
A.7.2.1 Management responsibilities	no	No se exige, se entiende que todos los socios cumplirán con los procedimientos establecidos	ISO 27001
A.7.2.2 Information security awareness, education and training	si	Se establecen criterios en la política de seguridad dedicadas a concienciar, formar...	ISO 27001 Política de Seg.
A.7.2.3 Disciplinary process	no	Siendo todos socios no es realista ni va con la filosofía de la empresa	ISO 27001
A.7.3 Termination and change of employment			

A.7.3.1 Termination or change of employment responsibilities	si	Hay que cambiar claves y de más	ISO 27001 política y procedimiento
A.8 Asset management			
A.8.1 Responsibility for asset			
A.8.1.1 Inventory of assets	si	Existe y inventario realizado en el análisis de riesgos (en el apartado análisis de impacto)	ISO 27001 Análisis de riesgo
A.8.1.2 Ownership of assets	si	Existen activos. El propietario es la empresa misma.	ISO 27001
A.8.1.3 Acceptable use of assets	si	Existen reglas que regulan uso de ciertos activos. Por ejemplo el correo...	ISO 27001 Política de Seg.
A.8.1.4 Return of assets	si	Está recogido en la política la obligación de devolver	ISO 27001 Política de Seg.
A.8.2 Information classification			
A.8.2.1 Classification of information	si	Se han detectado amenazas con riesgo moderado relacionado con falta de clasificación	ISO 27001 Análisis de riesgos
A.8.2.2 Labelling of information	si	Se han detectado amenazas con riesgo moderado relacionadas con la falta de etiquetado	ISO 27001 Análisis riesgos
A.8.2.3 Handling of assets	si	Se han detectado amenazas con riesgo moderado relacionado con el tratamiento de la información	ISO 27001 Análisis de riesgos
A.8.3 Media handling			
A.8.3.1 Management of removable media	si	Se usan pendrives y discos externos.	ISO 27001
A.8.3.2 Disposal of media	si	Cuando se cambian discos o ordenadores por deterioro	ISO 27001
A.8.3.3 Physical media transfer	no	En el departamento de desarrollo no se sacan de la organización soportes con información.	ISO 27001
A.9 Access control			
A.9.1 Business requirements of access control			
A.9.1.1 Access control policy	si	Se han detectado amenazas con riesgo moderado relativas a asignación de permisos	ISO 27001 política contraseña
A.9.1.2 Access to networks and network services	si	Solo se conectan tienen servicios usuarios y/o con vpn...	ISO 27001 Pol. servicios red
A.9.2 User access management			
A.9.2.1 User registration and de-registration	si	Ahora hay 10 empleados con usuarios. Pero se incorporan nuevos o se van algunos.	ISO 27001

A.9.2.2 User access provisioning			
A.9.2.3 Management of privileged access rights	si	Se han detectado amenazas con riesgo moderado relacionado con mala asignación	ISO 27001 análisis de riesgos
A.9.2.4 Management of secret authentication information of users	si	Existe política de contraseñas	ISO 27001 política seguridad
A.9.2.5 Review of user access rights	si	Hay activos controlados (así como el correo...) y políticas que requieren la revisión de estos.	ISO 27001
A.9.2.6 Removal or adjustment of access rights	si	Se contempla la amenaza de empleados despedidos/contrato finalizado en el análisis de riesgos	ISO 27001 Análisis de riesgos
A.9.3 User responsibilities			
A.9.3.1 Use of secret authentication information	si	Hay una polítca de contraseñas	ISO 27001 Política de Seg.
A.9.4 System and application access control			
A.9.4.1 Information access restriction	si	Se han detectado amenazas con riesgo moderado relacionado con falta de definición de acceso	ISO 27001 Análisis de riesgo
A.9.4.2 Secure log-on procedures	si	Está definido en la política de seguridad	ISO 27001 Política de Seg.
A.9.4.3 Password managment system	no	No se establecerán sistemas tan completo (sin forzar cambios, con restricciones). La empresa delega responsabilidad en empleados para que apliquen la política y para el cambio el responsable de seguridad lo notificará cada 6 meses.	ISO 27001 Política de Seg.
A.9.4.4 Use of privileged utility programs	no	No se restringirá. Se confía en los empleados que en principio no usarán usuarios con privilegios especiales más que en caso de ser muy necesario.	ISO 27001
A.9.4.5 Access control to program source code	si	Restringido a usuarios de desarrollo	ISO 27001 Política de desarrollo
A.10 Cryptography			
A.10.1 Cryptographic controls			
A.10.1.1 Policy on the use of cryptographic controls	si	Se establece que las contraseñas deben de ir cifradas.	ISO 27001 Política de correo. Política de recursos comunicación
A.10.1.2 Key management	si	Se hace uso de cifrado para copias, para correos con información confidencial...luego existen claves y requieren una política o ciertas normas de gestión	ISO 27001
A.11 Physical and environmental security			

A.11.1 Secure areas			
A.11.1.1 Physical security perimeter	si	La empresa está en una oficina protegida con puerta, paredes, ventanas...Hay video vigilancia en el edificio...	ISO 27001
A.11.1.2 Physical entry controls	si	Hay acceso de gente tanto de la empresa como de visitas ajenas (clientes, comerciales...) a las oficinas de la empresa.	ISO 27001 Análisis de riesgos
A.11.1.3 Securing offices, rooms and facilities	si	Se evita el acceso por el público en general	ISO 27001
A.11.1.4 Protecting against external and environmental threats	si	Existen medidas (SAI, extintores...) También se han valorado los riesgos	ISO 27001 Análisis de riesgos
A.11.1.5 Working in secure areas	no	La empresa no dispone de ninguna área segura	ISO 27001
A.11.1.6 Delivery and loading areas	no	La empresa no dispone de espacio para ello	ISO 27001
A.11.2 Equipment			
A.11.2.1 Equipment siting and protection	si	Hay equipos mínimo 1 por empleado. Se usan a diario y deberían de protegerse. Existen RACs...	ISO 27001
A.11.2.2 Supporting utilities	si	Hay SAI-s instalados	ISO 27001
A.11.2.3 Cabling security	si	La oficina está preparada para tener puntos donde conectar equipos...El cableado está protegido	ISO 27001
A.11.2.4 Equipment maintenance	si	Los técnicos del departamento de soporte hacen mantenimientos de los equipos de la empresa	ISO 27001
A.11.2.5 Removal of assets	si	Hay reuniones con clientes y a veces necesidad de llevarse código para presentar y de más...y dispositivos móviles. Hay una política que establece reglas para ello.	ISO 27001 Política de seguridad
A.11.2.6 Security of equipment and assets off-premises	no	Nadie del departamento de desarrollo trabaja con equipamientos y activos fuera de la empresa	ISO 27001
A.11.2.7 Secure disposal or reuse of equipment	si	Se cambian equipos cada cierto tiempo.	ISO 27001
A.11.2.8 Unattended user equipment	si	Hay bloqueos de pantallas con contraseñas	ISO 27001
A.11.2.9 Clear desk and clear screen policy	si	Existe información que no debe estar en la mesa o pantallas. Existe política que hace referenci a ello (contraseñas...).	ISO 27001 Política de seg.
A.12 Operations security			
A.12.1 Operational procedures and responsibilities			
A.12.1.1 Documented operating procedures	si	Existen configuraciones y de más que deben documentarse... La empresa lo hace en una wiki	ISO 27001

		propia.	
A.12.1.2 Change management	si	La empresa suele experimentar cambios en los procesos de negocio y en sistemas que deberían de ser controlados.	ISO 27001
A.12.1.3 Capacity management	si	Se han detectado amenazas que afectan el tema de almacenamiento, transmisión de datos y consumo de red...	ISO 27001 Análisis de riesgos
A.12.1.4 Separation of development, testing and operational environments	si	Existen diferentes entornos. Y la política de desarrollo establece criterios para que se desarrollen ciertas operaciones en su debida forma y entorno..	ISO 27001 Análisis de riesgos
A.12.2 Protection from malware			
A.12.2.1 Controls against malware	si	Existen IDS-s, firewalls, y también se han detectado amenazas relacionadas con el malware que suponen un riesgo alto y moderado	ISO 27001 Análisis de riesgos
A.12.3 Backup			
A.12.3.1 Information backup	si	Se hacen copias de información y sistemas...	ISO 27001 Política de Seg.
A.12.4 Logging and monitoring			
A.12.4.1 Event logging	si	Se han detectado amenazas que suponen un riesgo moderado de la falta de un seguimiento.	ISO 27001 Análisis de riesgos
A.12.4.2 Protection of log information	no	No hay espacio para guardar logs	ISO 27001
A.12.4.3 Administrator and operator logs	si	Existen logs de actividades del administrador en servidores, de equipos	ISO 27001
A.12.4.4 Clock synchronisation	no	No hay servicios que requieran tal precisión	ISO 27001
A.12.5 Control of operational software			
A.12.5.1 Installation of software on operational systems	si	Hay una política de software	ISO 27001 Política de Seg.
A.12.6 Technical vulnerability management			
A.12.6.1 Management of technical vulnerabilities	si	Se hace en el análisis de riesgos	ISO 27001 Análsis de riesgos
A.12.6.2 Restrictions on software installation	si	Hay una política de software	ISO 27001
A.12.7 Information systems audit considerations			
A.12.7.1 Information systems audit controls	si	Existe plan de auditorías	ISO 27001
A.13 Communications security			
A.13.1 Network security management			
A.13.1.1 Network controls	si	Hay política de servicios de red, protocolos	ISO 27001

		seguros, uso de vpn...	
A.13.1.2 Security of network services	si	Hay contratados servicios de red de diferentes proveedores	ISO 27001
A.13.1.3 Segregation in networks	si	Se implementan VLAN-s...	ISO 27001
A.13.2 Information transfer			
A.13.2.1 Information transfer policies and procedures	si	La empresa intercambia información a través de correo mayormente, información con clientes... Existe política de uso de los recursos de comunicación y de correo.	ISO 27001 Política de Seg.
A.13.2.2 Agreements on information transfer	no	La empresa no intercambia información con terceros	ISO 27001
A.13.2.3 Electronic messaging	si	Existe política de correo electrónico Se han detectado amenazas que suponen un riesgo con el envío de información por correo	ISO 27001 Política de Seg. Análisis de riesgos
A.13.2.4 Confidentiality or nondisclosure agreements	si	Existen acuerdos de confidencialidad a nivel interno en contratos y también se recogen requisitos sobre confidencialidad en en la política de seguridad	ISO 27001 Política de Seg.
A.14 System acquisition, development and maintenance			
A.14.1 Security requirements of information systems			
A.14.1.1 Information security requirements analysis and specification	si	Se identifican ciertos requisitos durante el análisis, a través de la política de desarrollo de software...	ISO 27001 Análisis de riesgos
A.14.1.2 Securing application services on public networks	si	Se establece en la política de desarrollo el uso de protocolos seguros en aplicaciones públicas. Se evalúa temas de certificados en el análisis de riesgos.	ISO 27001 Politica de seg. desarrollos Análisis de riesgos
A.14.1.3 Protecting application services transactions	si	Se establece en la política de desarrollo el uso de protocolos seguros en aplicaciones públicas. Se evalúa temas de certificados en el análisis de riesgos.	ISO 27001 Politica de seg. desarrollos Análisis de riesgos
A.14.2 Security in development and support processes			
A.14.2.1 Secure development policy	si	Existe la política de desarrollo	ISO 27001 Política de desarrollo
A.14.2.2 System change control procedures	si	Se hace control de versiones, documentación y de más en la política de desarrollo	ISO 27001 Política de desarrollo
A.14.2.3 Technical review of applications after operating platform	si	Se hacen cambios en sistemas operativos. Estos cambios se deben de hacer en base a la política de software que existe.	ISO 27001

A.14.2.4 Restrictions on changes to software packages	no	No se tocan las librerías	ISO 27001
A.14.2.5 Secure system engineering principles	si	Existe una wiki y también más documentación técnica en un alfresco. Hay políticas en la empresa que establecen normas para documentar ciertos proyectos y sistemas desarrollados.	ISO 27001 Análisis de riesgos
A.14.2.6 Secure development environment	si	El entorno de desarrollo el el "localhost" de cada desarrollador. Accesbile únicamente desde el propio puesto.	ISO 27001
A.14.2.7 Outsourced development	si	Está supervisado, documentado, y se controlan los cambios con el control de versiones (un servicio bitbucket exclusivo para colaboradores)	ISO 27001
A.14.2.8 System security testing	no	La empresa no tiene recursos destinados a ello, y no tiene procedimientos, conocimientos.	ISO 27001
A.14.2.9 System acceptance testing	no	La empresa no tiene procedimientos, conocimientos y recursos dedicados para ello.	ISO 27001
A.14.3 Test data			
A.14.3.1 Protection of test data	no	En Secure Team no se trabaja con datos reales para los tests, son ficticios, luego no requieren protección.	ISO 27001
A.15 Supplier relationships			
A.15.1 Information security in supplier relationships			
A.15.1.1 Information security policy for supplier relationships	si	Secure Team trabaja con proveedores que pueden tener acceso a sus datos o de sus clientes que hacen uso de esos servicios. Se acuerdan los términos y condiciones de uso y políticas al contratar el servicio.	ISO 27001
A.15.1.2 Addressing security within supplier agreements	si	Secure Team trabaja con proveedores que pueden tener acceso a sus datos o de sus clientes que hacen uso de esos servicios. Se acuerdan los términos y condiciones de uso y políticas al contratar el servicio.	ISO 27001
A.15.1.3 Information and communication technology supply chain	si	Secure Team trabaja con proveedores que a su vez usan otros servicos y pueden tener acceso a sus datos o de sus clientes que hacen uso de esos servicios. Se acuerdan los términos y condiciones de uso y políticas al contratar el servicio.	ISO 27001
A.15.2 Supplier service delivery management			
A.15.2.1 Monitoring and review of supplier services	si	Los proveedores con los que Secure Team disponen de paneles de monitorización y mecanismos de control de los servicios.	ISO 27001
A.15.2.2 Managing changes to supplier services	si	Los servicios de los proveedores con los que trabaja Secure Team suelen tener cambios.	ISO 27001

A.16 Information security incident management			
A.16.1 Management of information security incidents and improvements			
A.16.1.1 Responsibilities and procedures	si	Las responsabilidades están definidas, y la gestión de incidentes se realiza a través de una aplicación.	ISO 27001 gestión de roles y responsabilidades
A.16.1.2 Reporting information security events	si	El personal y los clientes conocen la existencia del programa de gestión de incidentes y también hay soporte telefónico	ISO 27001 gestión de roles y responsabilidades
A.16.1.3 Reporting information security weaknesses	si	La empresa tiene una aplicación para notificar los eventos de seguridad entre otros. También ofrece dicha aplicación para que los clientes comuniquen eventos de seguridad.	ISO 27001
A.16.1.4 Assessment of and decision on information security events	no	No hay recursos humanos para establecer un punto de contacto para clasificación y la empresa no tiene una plantilla de clasificación de eventos	ISO 27001
A.16.1.5 Response to information security incidents	si	Suceden incidencias relacionadas con la seguridad la información y se tratan o se responder desde la misma empresa. (Los empleados evalúan cómo responder a los incidentes relativos a los clientes asignados)	ISO 27001
A.16.1.6 Learning from information security incidents	si	Existe la aplicación de gestión de incidentes que posibilita la cuantificación y el seguimiento.	ISO 27001
A.16.1.7 Collection of evidence	si	Existe la aplicación de gestión de incidentes que ya marca a través del formulario la información que hay que recoger o aportar.	ISO 27001
A.17 Information security aspects of business continuity management			
A.17.1 Information security continuity			
A.17.1.1 Planning information security continuity	si	Secure Team puede sufrir un desastre o situaciones seriamente adversas, y esto puede ser un ransomware o un incendio... Aunque en el análisis de riesgos tienen pequeña probabilidad de ocurrencia o de que algún desastre de dicho tipo ocurra. Debería de tener un mínimo de plan.	ISO 27001
A.17.1.2 Implementing information security continuity	si	Ante la posibilidad de un desastre, es necesario un plan de continuidad con un nivel de continuidad definido.	ISO 27001
A.17.1.3 Verify, review and evaluate information security continuity	si	Los planes de continuidad deberían de revisarse y evaluarlos. Secure Team necesita que ante un desastre tenga un plan de continuidad revisado, verificado.	ISO 27001
A.17.2 Redundancies			
A.17.2.1 Availability of information processing	si	Existen portátiles y algún ordenador de puestos preparados en caso de no disponer del propio.	ISO 27001

facilities			
A.18 Compliance			
A.18.1 Compliance with legal and contractual requirements			
A.18.1.1 Identification of applicable legislation and contractual requirements	si	Se trabaja con una asesoría jurídica para implantar medidas de cumplimiento legal y algunas se recogen en las políticas	ISO 27001 Política de seguridad
A.18.1.2 Illectual property rights	si	Hay una política sobre propiedad intelectual y se cuenta una asesoría jurídica para ello.	ISO 27001 Ley Propiedad intelectual LSSI
A.18.1.3 Protection of records	si	Se cuenta con una asesoría jurídica para implantar medidas de cumplimiento legal y algunas se recogen en las políticas	ISO 27001 LOPD
A.18.1.4 Privacy and protection of personally identifiable information	si	Se cuenta con una asesoría jurídica para implantar medidas de cumplimiento legal y algunas se recogen en las políticas	ISO 27001 LOPD
A.18.1.5 Regulation of cryptographic controls	si	Se cuenta con una asesoría jurídica para implantar medidas de cumplimiento legal y algunas se recogen en las políticas.	ISO 27001 LOPD LSSI
A.18.2 Information security reviews			
A.18.2.1 Independent review of information security	no	Secure Team solo hará auditorías internas. Además,aunque si tiene como base la ISO27001, de momento y por falta de recursos, no tiene intención de sacar el certificado.	ISO 27001
A.18.2.2 Compliance with security policies and standards	si	Existe el plan de auditoría donde se contemplan revisar y medir el cumplimiento de las políticas y estándares	ISO 27001 auditoría interna
A.18.2.3 Technical compliance review	si	Existe el procedimiento de auditoría donde se contemplan revisar y medir el cumplimiento de las políticas y estándares cada cierto periodo	ISO 27001 auditoría interna

Tabla 5: Plantilla de Declaración de Aplicabilidad

6. Análisis de riesgos

6.1 Introducción

Un análisis de riesgos corresponde al proceso de identificación de los mismos, junto con su relevancia o impacto e identificando los activos que requieren medidas de protección para tratar de reducir los riesgos sobre ellos.

6.2 Fuentes de amenaza

6.2.1 Fuentes de amenaza intencionadas (*adversarial*)

En la siguiente tabla se recogen las fuentes de amenaza intencionadas, es decir, amenazas que los causa o individuos o grupos de personas. Para definirlos se han tenido en cuenta la información facilitada por la empresa, en base a compañías de la competencia, la existencia de empleados despedidos, estado de relaciones de empleados, análisis de la realidad en base a amenazas de hackers... Siempre se tienen contemplar el máximo de posibilidades pero con una base de realismo, es decir, en el caso de Secure Team no tendría sentido contemplar o recoger grupos terroristas, o secuestradores o cosas por el estilo.

Identificador	Fuente de amenaza	Categoría	Capacidad	Intencionalidad	Elección de objetivo (*targeting*)
FAA-1	Colaboradores - freelances	Individual - semi-externo	Alto	Alto	Alto
FAA-2	Crecientes grupos de hackers	Grupo - General	Alto	Moderado	Muy bajo
FAA-3	Competencia	Grupo - Ad hoc	Moderado	Alto	Alto
FAA-4	Creciente script kiddies	Individual - Externo	Bajo	Bajo	Muy bajo
FAA-5	Empleado descontento/socio cesado, despedido...	Individual - Interno	Moderada	Muy Alto	Muy Alto
FAA-6	Mayor tasa de delincuencia (crisis, conflictos)	Grupo - Externo	Moderado	Muy bajo	Muy bajo
FAA-7	Cliente/Visitante (repartidores/técnicos telefonía...) a instalaciones	Individual - Externo	Bajo	Muy bajo	Muy bajo

Tabla 6: Fuentes de amenaza intencionadas

En cuanto a las columnas capacidad, intencionalidad y elección del objetivo (targeting) la mayoría también se basa en información aportada por la propia empresa (experiencias, conocimiento y sensaciones) y la contextualización y conocimiento de la organización y su actividad.

En la correspondiente a hackers se basa en la información que recogen webs e informes de una creciente industria de malware, en la que detrás se encuentran organizaciones criminales bien organizadas, estados (en este caso no sería muy realista) con el fin de espionaje industrial y ciber guerras [Symantec, 2016],[Symantec, 2016 (gov)].

Para Secure Team hay que tener en cuenta, que esa creciente industria sí supone una fuente de amenaza, con una alta capacidad, también considerable intencionalidad pero que no es un objetivo por motivos exclusivos, si no más bien generales. Los script kiddies no tienen demasiada capacidad, pero en internet no es difícil encontrar malware e instrucciones para poder usarlo, sin que realmente sepan lo que hacen o lo usen como si fuera un juguete o de un juego se tratara.

También hay que contemplar a los empleados y socios, que en caso de que quieran pueden ser la fuente de muchas amenazas, lo mismo los colaboradores.

No hay que dejar pasar por alto a los visitantes o personal ajeno a la empresa que accede a las oficinas. Repartidores, técnicos de telefonía, técnicos del aire acondicionado, clientes...

6.2.2 Fuentes de amenaza no intencionados

Identificador	Fuente de amenaza e base de información	Categoría	Rango de efectos
FAN-1	Agotamiento de espacio o deterioro de sistema almacenamiento	Estructural - Almacenamiento	Baja
FAN-2	Insuficiencia de capacidad transmisión de datos	Estructural - Procesamiento y comunicación	Muy baja
FAN-3	Temperatura	Estructural - Entorno	Baja
FAN-4	Suministro eléctrico	Estructural - Entorno	Alto
FAN-5	Problemas de comunicaciones/red/telefonía	Estructural - Entorno / software	Alto
FAN-6	Obsolescencia y/o caducidad sistema operativo	Estructural - Software	Baja
FAN-7	Obsolescencia de software general	Estructural - Software	Baja
FAN-8	Obsolescencia de software desarrollado	Estructural - Software	Baja
FAN-9	Caducidad de licencias	Estructural - Software	Moderado
FAN-10	Incendios	Ambiental/Entorno – Natural/Humano	Muy alto
FAN-11	Telecomunicaciones (telefonía, internet)	Ambiental/Entorno – Infraestructura	Alto
FAN-12	Suministro Eléctrico	Ambiental/Entorno – Infraestructura	Alto
FAN-13	Error o despiste o evento accidental de usuarios (programadores)	Accidental - Usuario	Moderado
FAN-14	Error o despiste o evento accidental de usuario con privilegios / administradores (gerente,responsables)	Accidental - Usuario Administrador	Alto

Tabla 7: Fuentes de amenaza no intencionadas

En esta bala se ha recogido al igual que en la anterior, las fuentes de amenazas no intencionadas, es decir, aquellas que pueden ser fuentes/factores que generan amenazas como incidentes, despistes, errores...

Esta información también ha sido valorada basándose en información aportada por la empresa, así como el diagrama, experiencias, infraestructuras y el diagrama de red tecnológica, y fuentes de amenazas bastante comunes (medioambientales, de entorno...). Como es lógico, en esta tabla no se valora la intencionalidad, capacidad... sino que se valora el rango de efectos... que mayormente determina en que medida afecta a los recursos de la empresa, si afecta a todas, a casi todas... En este caso, el incendio podría afectar a todas, algo relacionado con el suministro eléctrico, al dispone de eqipos portatiles y móviles sería casi a todas por lo que alto... En la de obsolescencia de software general, no podría darse de forma que afecte a todo, a menos que se exagerase, ya que no todo los equipos tienen mismo software ni sistema operativo... la temperatura sería algo que no afectaría a todas, ya que hay aire acondicionado en varios puntos, quedando algunos activos más expuestos que otros.

6.3 Amenazas

No se seguirán reverenciando las amenazas que tienen el valor N/A en la columna relevancia tal y como se ha definido en la metodología.

6.3.1 Amenazas intencionadas

Identificador	Amenaza	Fuente amenaza	Relevancia	Contramedidas / salvaguardas	Probabilidad ocurrencia /iniciación	Probabilidad Impactos adversos	Media probabilidad
A-1	Reconocimiento/escaneo red	FAA-2	Posible	A.13.1	Bajo	Moderado	Bajo
A-2	Sniffer de red interna	FAA-5	N/A				
A-3	Recopilado de información desde recursos abiertos (web,emails,medios...)	FAA-2	Posible	A.5	Moderado	Moderado	Moderado
A-4	Reconocimiento y vigilancia de objetivos	FAA-5	N/A				
A-5	Reconocimiento y vigilancia de objetivos	FAA-3	N/A				
A-6	Malware instalado dentro de la organización	FAA-5	N/A				
A-7	Ataques de phising	FAA-1	N/A				
A-8	Ataques de phising	FAA-2	Posible	A.12.2	Moderado	Muy alto	Alto
A-9	Suplantación de web	FAA-2	Confirmado	A.12.2	Moderado	Moderado	Moderado
A-10	Certificado comprometido	FAA-2	Posible	A.12.2	Bajo	Alto	Moderado
A-11	Envió de virus/malware conocido (email..)	FAA-4	Confirmado	A.12.2	Alto	Moderado	Moderado
A-12	Envío malware modificado	FAA-2	Confirmado	A.12.2	Alto	Moderado	Moderado
A-13	Envío de malware de control	FAA-2	Confirmado	A.12.2	Alto	Alto	Alto
A-14	Soporte extraíble con malware	FAA-5	N/A				
A-15	Soporte extraíble con malware	FAA-3	N/A				

A-16	Soporte extraíble con malware	FAA-1	N/A				
A-17	Malware en software descargable o comercial	FAA-2	Confirmado	A.12.2	Moderado	Alto	Moderado
A-18	Instalación de sniffers en red interna	FAA-5	N/A				
A-19	Explotación de vulnerabilidades conocidas en sistemas móviles	FAA-2	Posible	-	Moderado	Alto	Moderado
A-20	Explotación de vulnerabilidades descubiertas recientemente	FAA-2	Esperado	-	Alto	Muy alto	Muy alto
A-21	Explotación de vulnerabilidades de sistemas internos	FAA-2	Posible	-	Moderado	Muy Alto	Alto
A-22	Explotación de vulnerabilidades de sistemas internos	FAA-5	N/A				
A-23	Explotación de vulnerabilidades de tipo zero-day	FAA-2	Pronosticado		Moderado	Muy alto	Alto
A-24	Comprometer sistemas críticos a través de acceso físico	FAA-5	N/A				
A-25	Comprometer software crítico de la empresa	FAA-2	Posible	A.12.2	Moderado	Muy alto	Alto
A-26	Comprometer software crítico de la empresa	FAA-5	N/A				
A-27	Ataques de denegación de servicio dirigido (DoS)	FAA-3	N/A				
A-28	Ataques de denegación de servicio dirigido (DoS)	FAA-5	N/A				
A-29	Ataques de denegación de servicio (DoS)	FAA-4	Posible	A.12.2	Bajo	Alto	Moderado
A-30	Ataques de denegación de servicio (DDoS)	FAA-2	Esperado	A.12.2	Moderado	Alto	Moderado
A-31	Incendio provocado	FAA-6	N/A				

A-32	Atacar/dañar infraestructuras	FAA-6	Posible	-	Bajo	Muy Alto	Moderado
A-33	Ataques aplicaciones web de la organización (xss, sql injection, sesión hijacking)	FAA-2	Confirmado	A.16 A.14	Muy alto	Muy alto	Muy alto
A-34	Ataques aplicaciones web de la organización (xss, sql injection, sesión hijacking)	FAA-1	N/A				
A-35	Ataques MiTM	FAA-2	Posible	A.12.2	Bajo	Moderado	Bajo
A-36	Ingeniería social	FAA-3	N/A				
A-37	IngenIería social desde dentro	FAA-5	N/A				
A-38	Ingeniería social desde dentro	FAA-1	N/A				
A-39	Pérdida de integridad de información pública (p.e.:web)	FAA-2	Confirmado	A.16 A.14	Moderado	Moderado	Moderado
A-40	Pérdida de integridad de información pública (p.e.:web)	FAA-4	Confirmado	A.16 A.14	Bajo	Moderado	Bajo
A-41	Pérdida de integridad de información pública (p.e.:web)	FAA-3	N/A				
A-42	Pérdida de información crítica	FAA-5	N/A				
A-43	Acceso no autorizado a sistemas	FAA-2	Pronosticado	A.12.2	Moderado	Muy alto	Alto
A-44	Acceso no autorizado a sistemas	FAA-5	N/A				
A-45	Degradar/alterar servicios	FAA-2	Confirmado	A.12.2	Moderado	Alto	Moderado
A-46	Ataques coordinados y de origen cambiante	FAA-2	Confirmado	A.12.2 A.16	Alto	Moderado	Moderado
A-47	Robo de activos (robo físico)	FAA-6	Posible	Puerta/vide o vigilancia edifico	Bajo	Muy alto	Moderado
A-48	Robo de activos (robo físico)	FAA-7	Posible	-	Bajo	Muy alto	Moderado
A-49	Obtención de información de sistema/equipo desatendido	FAA-7	Posible	A.11.2.8	Bajo	Moderado	Bajo
A-50	Robo de información	FAA-2	Posible	A.10	Bajo	Muy alto	Moderado

	sensible y/o crítica (datos personales, información proyectos...)			A.18			
A-51	Robo de información sensible y/o crítica (datos personales, información proyectos...)	FAA-5	N/A				

Tabla 8: Amenazas intencionadas (ataques)

Las amenazas que tienen como fuente FAA 1, FAA3 y FAA 5 son N/A (No Aplicables) ya que su la fuente de amenaza a día de hoy es inexistente o no podría constituir una amenaza.

No hay nada que indique que un empleado-socio esté descontento, y sería raro que algún socio fuese la fuente de amenaza de amenazas como ataques... Aunque se ha contemplado porque alguna vez ha habido empleados despedidos, eso fue hace tiempo y se cerraron los asuntos de manera correcta. En cuanto a la competencia, al nivel que trabaja actualmente Secure Team no se contempla que haya amenazas intencionadas que vengan de la competencia, en pricipio hay buena relación con las empresas que se consideran de la competencia. En cuanto a los freelance, se está trabajando con uno, y es de confianza y se le está pagando bien y dándole bastante trabajo, por lo que sería muy raro que hubiera amenazas por su parte, no se constata nada.

En cuanto los que tiene la fuente de grupos de hackers (FAA-2) y script kiddies (FAA-4), hay que tener en cuenta la creciente industria detrás del malware. Cada vez hay más ataques, grupos más cualificados y la probabilidad de que las amenazas que tienen como fuente a esos grupos se materialicen y causen daño es considerable. En concreto, el phising, el envió de malware y el ataque a aplicaciones web es bastante alto, aunque algunas técnicas hayan bajado [Symantec, 2016 (gov)],[Symantec, 2016].

La amenaza de envío de malware por email es creciente, en 2016 1 de cada 132 emails llevaba malware según Symantec. Ha habido un aumento de botnets. Además, las compañías de entre 1-250 empleados no son de las más atacadas pero si que sufren un número considerable de ataques. Phising bajó en 2016 respecto a años anteriores. 1 en 2596 correos. y lo mismo que el email con malware, ha bajado un poco, pero 1 de 2897 mensajes lleva malware. Pero el éxito de estos ataques muchas veces o mayormente recae en lo que haga el usuario, y como recoge la persona es el eslavón más debil de la seguridad [Mitnick, 2002],[Hadnagy, 2010].

Por otro lado, un 76% de las webs escaneadas por Symantec contienen alguna vulnerabilidad. Aunque las críticas han bajado mucho comparando con otros años. En 2015 era de un 20% y en 2017 un 9% . Se ve que la amenaza de ataques es muy grande y no es muy probable ser objeto de algún ataque independientemente del tamaño de la organización [Symantec, 2016],[Symantec, 2016 (gov)],[ENISA,2016].

En cuanto a la delincuencia (robos, ataques...) podría darse, pero las amenazas de ese tipo (FAA-6) no son muy probables. En los 10 años de existencia de Secure Team, solo han sufrido dos robos. Parecido en las empresas de alrededor, y la tasa de delincuencia es baja en la Comunidad Autónoma Vasca [Deia, 2016].

6.4 Amenazas no intencionadas

ID	Amenaza	Fuente amenaza	Relevancia	Contramedidas / salvaguardas	Probabilidad ocurrencia/iniciación	Probabilidad Impactos adversos	Media probabilidad
A-52	Divulgación de información sensible	FAN-13	Confirmado	A.5 A.13	Alto	Moderado	Moderado
A-53	Divulgación de información sensible	FAN-14	Confirmado	A.5 A.13	Moderado	Moderado	Moderado
A-54	Mal manejo de información crítica	FAN-14	Confirmado	A.5 A.13	Bajo	Alto	Moderado
A-55	Asignación errónea de permisos a usuarios	FAN-14	Confirmado	A.9.2	Muy alto	Moderado	Alto
A-56	Incendios afectando recursos/instalaciones principales	FAN-10	Posible	Extintores / detector de humos backups	Muy bajo	Muy alto	Bajo
A-57	Incendios en recursos de respaldo	FAN-10	Posible	Extintores / detector de humos	Muy bajo	Alto	Bajo
A-58	Error de fabricante en discos duros	FAN-1	Confirmado	-	Bajo	Moderado	Bajo
A-59	Error en disco duro	FAN-1	Confirmado	-	Bajo	Moderado	Bajo
A-60	Webs/aplicaciones con recursos pesados y picos de datos (videos,imágenes, muchas visitas, muchos datos)	FAN-2	Confirmado	-	Moderado	Bajo	Bajo
A-61	Corte de suministro eléctrico	FAN-3	Confirmado	A.11.2.2	Moderado	Moderado	Moderado
A-62	Corte de comunicación e interrupción de acceso a información interna	FAN-5	Confirmado	A.11.2.2	Moderado	Moderado	Moderado
A-63	Incompatibilidades de software y sistema	FAN-7	Confirmado	-	Bajo	Alto	Moderado
A-64	Errores y fallos de programación/configuración en proyectos	FAN-13	Confirmado	A.14	Moderado	Alto	Moderado
A-65	Incompatibilidad sistemas/servidores y software desarrollado	FAN-8	Confirmado	-	Bajo	Alto	Moderado

A-66	Errores en servicios de red (openvpn, dhcp, firewall)	FAN-5	Confirmado	-	Bajo	Muy alto	Moderado
A-67	Corte de linea telefónica	FAN-11	Confirmado	A.11.2.2	Bajo	Bajo	Bajo
A-68	Corte de internet	FAN-11	Confirmado	A.11.2.2	Moderado	Alto	Moderado

Tabla 9: amenazas no intencionadas

La valoración estás asociada a información que se ha aportado desde miembros de la organización y de algunas que se deducen por el entorno, descripción del organigrama, red tecnología, instalaciones... Junto a cada amenaza se recoge la relevancia que puede decirse que determina la constancia o información que se tiene y de donde viene, al ser una empresa dedicada a la informática muchas veces hay constancia directa de ello y si no de blog y paginas relacionadas con la informática a las que los empleados siguen. También si existe o no contramedidas o salvaguardas que pudieran parar o neutralizar la amenaza, la probabilidad de que esta amenaza se dé o se materialice, y una vez materializado si ésta podría derivar en un impacto adverso.

En este apartado simplemente se constatan despistes, errores, amenazas medioambientales, de entorno partiendo de las que han sucedido hasta la fecha, y algunas de ellas interpretando un poco el modo de trabajo, la red tecnológica, infraestructuras, ubicación de la empresa...

Las amenazas que tienen como origen despistes o errores humanos (A52,A53), al ser una empresa que no tiene políticas y tiene hábitos y formas de trabajo bastantes abiertos, se puede decir que la probabilidad de ocurrencia es más alta.

Por la experiencia y nivel de conocimiento del responsable de seguridad, es baja la probabilidad de ocurrencia de A66, además se podrían dar errores, pero una vez solventadas, no es una cosa que se cambie demasiado... En cambio, la asignación de permisos, puede darse con mayor probabilidad, ya que no hay un procedimiento o plantillas o nada, y es muy probable que ocurra A55.

La falta de metodología y testing y code reviews y de más, podrían darse errores de programación A64. Las relativas a cortes de internet, de teléfono no es algo que esté sucediendo muchas veces, pero si pasa. La ocurrencia de incendios sería poco probable, pero si se diese tendría impactos adversos altos.

No se está revisando ni haciendo seguimiento de las aplicaciones web y son de bastante flujo de datos y tráfico, por lo que es una amenaza los picos (A60).

La empresa está ubicada en una región donde es muy común las tormentas y eso afecta al suministro eléctrico. Y las amenazas relativas a incompatibilidades, y errores de hardware, no es demasiado común ya que no se están cambiando mucho, no es anual pero si más de una vez cada 10 años (A58, A59).

6.5 Vulnerabilidades y condiciones predispuestas

6.5.1 Vulnerabilidades

Identificador	Vulnerabilidad	Severidad o grado de vulnerabilidad
V-1	Falta de contrato con colaboradores	Moderado
V-2	Extintores/Sensores sin revisar	Moderado
V-3	Todos los discos del mismo fabricante	Alto
V-4	Aplicaciones sin actualizar	Alto
V-5	S.O. Fuera de versiones estables o no LTS (sin actualizar y sin soporte)	Alto
V-6	Aplicaciones y librerías “abandonadas” u “obsoletas” (deprecated...)	Alto
V-7	Desarrollos en producción sin testear (pentesting, metodología tdd, sin code reviews...)	Alto
V-8	Falta de documentación de desarrollos realizados	Bajo
V-9	Hay diferentes aplicaciones instaladas, descontroladas y de todas la versiones	Moderado
V-10	Información sin clasificar	Bajo
V-11	Falta de políticas de transmisión interna de información sensible y crítica	Moderada
V-12	Asignación de permisos sin planificar,actualizar...	Bajo
V-13	Las claves se guardan como le parece a cada emplead	Moderado
V-14	Los recambios de equipos, discos... se hacen según la necesidad del momento y sin seguir un criterio	Moderado
V-15	Ubicación del servidores (accesible todo personal y cualquiera en oficina, temperatura...)	Alto
V-16	Falta de backups de SVN	Alto
V-17	Backups en misma ubicación	Alto
V-18	No se procede a tomar medidas especificas sobre usuarios durante y después del contrato	Alto
V-19	Ausencia procedimiento tratamiento, revisión, seguimiento de logs e incidentes	Alto
V-20	Falta de mantenimiento periódico, planificado de equipos, software	Moderado

V-21	Puertas sin doble capa y acceso llave simple	Moderado
V-22	Ausencia backups de equipos de puestos	Moderado
V-23	Falta de tabla definición técnica de roles – permisos de sistema	Alto
V-24	Falta de formación y concienciación	Alto
V-25	Ausencia de alarmas y de video vigilancia en oficina	Alto
V-26	Falta de control o no existe registro de visitas o acceso de terceros	Moderado
V-27	Información sin clasificar	Moderado
V-28	Falta de hostings adaptables a necesidad	Baja
V-29	Falta de SAI en equipos programadores	Baja

Tabla 10: Vulnerabilidades

De la información aportada en actas, de la información interpretada de la red tecnología se pueden detectar ciertas vulnerabilidades que podrían ser explotadas por las amenazas. Una vulnerabilidad se considera como una debilidad en un sistema de información, o en un procedimiento o control que pueda ser explotado por una amenaza.

6.5.2 Condiciones predispuestas

Identificador	Condición	Presencia/envergadura de la condición
CP-1	Ubicación donde muchas tormentas	Muy alto
CP-2	Materiales fáciles de arder	Muy alto
CP-3	Equipos y hardware calidad media+baja	Alto
CP-4	Existencia de información personal	Moderado
CP-5	Aplicaciones de comercio electrónico	Bajo

Tabla 11: Condiciones predispuestas

Estas condiciones recogidas en la tabla hacen que una amenaza iniciada o que ya ha ocurrido, resulte en un mayor impacto adverso. Son condiciones que están asociadas a la actividad en sí, y otras, derivadas de decisiones, como la media /baja calidad de hardware, lo cual haría que ciertas amenazas que puedan afectar al hardware, tenga un mayor impacto, ya que no están preparadas para ello. O por ejemplo, la existencia de información personal, si hubiera un acceso no autorizado o robo de información, el impacto adverso sería mayor que si no existiera. La existencia de aplicaciones de comercio electrónico o actividades de comercio electrónico da lugar a que una amenaza a una aplicación tenga un impacto adverso mayor ya que puede afectar a toda la actividad de esa empresa...

6.6 Probabilidad de ocurrencia

Son las columnas añadidas en el lado derecho de las tablas del apartado de amenazas

6.7 Impacto

6.7.1 Inventario de activos

Ámbito / Categoría	ID	Activos	Descripción/Detalles
Hardware Interno (Servidores/Servicios)	HW-I.1	Serv1 “intranet”	Alberga WIKI
Hardware Interno (Servidores/Servicios)	HW-I.2	Serv2 “zerbitzaria”	Alberga SVN, nagios, cacti, webapp de RRHH,chiper de CMDB, fetchmail (imap)
Hardware Interno (Servidores/Servicios)	HW-I.3	Vmware (alfresco)	Documentación sobre clientes, proyectos...
Hardware Interno (Servidores/Servicios)	HW-I.4	NAS1	Backups de alfresco, NAS2 y DB aplicaciones clientes
Hardware Interno (Servidores/Servicios)	HW-I.5	NAS2	Documentación de la empresa
Hardware Interno (Servidores/Servicios)	HW-I.6	RACK	Alberga HW-I.1, HW-I.2, HW-I.4, HW-I.5, HW-I.7, HW-I.8, HW-I.9, HW-I.10, HW-I.11,
Hardware Interno (Servidores/Servicios)	HW-I.7	SAI	Para los activos que alberga HW-I.6
Hardware Interno (Servidores/Servicios)	HW-I.8	Equipo Firewall+dhcp+openvpn	
Hardware Interno (Servidores/Servicios)	HW-I.9	Switch	
Hardware Interno (Servidores/Servicios)	HW-I.10	Cable modem Euskaltel 1	
Hardware Interno (Servidores/Servicios)	HW-I.11	Cable modem Euskaltel 2	
Hardware Interno (Servidores/Servicios)	HW-1.12	Impresora brother 1	
Hardware Interno (Servidores/Servicios)	HW-1.13	Impresora brother 2	
Hardware Interno (Servidores/Servicios)	HW-1.14	Impresora HP	
Hardware Puestos	HW-P.1	PC+Pantalla... programador 1	
Hardware Puestos	HW-P.2	PC+Pantalla... programador 2	
Hardware Puestos	HW-P.3	PC+Pantalla... responsable dto.	
Hardware Móvil	HW-M.1	Smartphones	Samsung Galaxy para cada empleado-socio
Software Interno	SW-I.1	S.O. servidores	Debian 9, Ubuntu 14.04, FreeBSD 9.1, FreeBSD 11
Software Interno	SW-I.2	Aplicación monitorización	Nagios, cacti
Software Interno	SW-I.3	App RRHH, Cifrado CMDB info	Laravel 5.4

Software Interno	SW-I.4	Openvpn	2.3.18 stable
Software Interno	SW-I.5	Firewall	iptables
Software Interno	SW-I.6	Software copias	(rsync,mysqldump,duplicity ...)
Software Interno	SW-I.7	Control de versiones	SVN 1.8
Software Puestos	SW-P.1	IDE	PHPStorm 2017, Sublime Text
Software Puestos	SW-P.2	Docker	Por si se necesita trabajar con otras versiones de mysql, apache..
Software Puestos	SW-P.3	MySQL	5.7.73
Software Puestos	SW-P.4	Apache	2.4
Software Puestos	SW-P.5	Cliente control de versiones	SmartSVN 9
Software puestos	SW-P.6	S.O.	Ubuntu 16.04
Hardware Externo	HW-E.1	VPS servidor correo	OVH
Hardware Externo	HW-E.2	VPS Web y aplicación gestión Secure Team	OVH
Hardware Clientes	HW-C.1	VPS (5 vps)	OVH
Software Clientes	SW-C.2	S.O. De vps y hostings	Ubuntu 16.04 + Plesk 17 + (apache,mysql, nginx...)
Software Clientes	SW-C.3	Aplicaciones web instalaciones desarrolladas	Laravel 4.2 – 5.4 (php 5-7), mysql
Software Clientes	SW-C.4	Páginas web	Wordpress 3.5 – 4.8.3 Laravel 4.2 – 5.4 (php 5-7), mysql
Software Externo	SW-E.1	S.O.	Ubuntu 16.94 + Plesk 17 + (apache,mysql, nginx...)
Software Externo	SW-E.2	Software correo	Postfix, dovecot, roundcube...
Software Externo	SW-E.3	Bitbucket+Jira	Compartir proyecto con freelance
Software Externo	SW-E.4	Web propia	
Información	I-1	BBDD aplicaciones clientes	
Información	I-2	BBDD uso interno: Wiki, gestión RRHH, gestión proyectos...	
Información	I-3	Código aplicaciones clientes + internos	
Información	I-4	Claves (aplicaciones,servidores...)	
Información	I-5	Copias de BBDD	
Red	R-1	Linea telefónica	
Red	R-2	Internet	

Red	R-3	Wifi	
Red	R-4	Cableado y puntos de red datos y eléctrico	
Capital Humano	CH-1	Programadores	2
Capital Humano	CH-2	Responsable dpto.	1
Capital Humano	CH-3	Responsable seguridad	1
Capital Humano	CH-4	Gerente	1
Capital Humano	CH-5	Freelance	1
Instalación e infraestructura	II-1	Detector de humos	3
Instalación e infraestructura	II-2	Extintores	3
Instalación e infraestructura	II-3	Aire acondicionado	
Instalación e infraestructura	II-4	Suministro eléctrico	General (no hay generadores...)
Instalación e infraestructura	II-5	Sistema video vigilancia	Instalado en edificio
Instalación e infraestructura	II-6	Oficina	

Tabla 12: Inventario de activos

6.7.2 Análisis del impacto

Amenaza	Tipo de impacto	Impacto activo afectado	Impacto máximo
A-1	Daño en activos tecnológicos e información	Revelación de características técnicas HW-E.1, HW-E.2, HW-C.1, S2-E.1, SW-E2, SW-C.2	Muy bajo
A-3	Daños personales	Suplantación/robo de identidad CH-1, CH-2, CH-3, CH-4	Muy bajo
A-8	Daño en empresa-actividad / Daño a otras empresas / Daños personales	Impedimento de desarrollo de la actividad Deterioro de imagen y reputación Robo/suplantación de identidad SW-I*, SW-E*, I-1, I-4 CH-1, CH-2, CH-3, CH-4	Moderado
A-9	Daño en empresa-actividad	Deterioro de imagen y reputación SW-E4	Muy bajo
A-10	Daño en empresa-actividad / Daños personales	Deterioro de imagen y reputación Robo/suplantación de identidad CH-1, CH-2, CH-3, CH-4, SW-E4	Moderado
A-11	Daño en empresa-actividad / Daño en activos tecnológicos e información	Pérdida económica directa Incapacidad de continuar/recuperar cierta actividad o llevarla a cabo de manera correcta (desarrollo código/proyecto) Pérdida o deterioro de sistemas, soportes de almacenamiento, informació n Otra empresa no puede cumplir objetivos, HW-I*,HW-E*,SW-I*,HW-P*, SW-P*, SW-E*, SW-C*,I-1, I-2,I.3,I-4	Moderado
A-12	Daño en empresa-actividad / Daño en activos tecnológicos e información	Pérdida económica directa Incapacidad de continuar/recuperar cierta actividad o llevarla a cabo de manera correcta (desarrollo código/proyecto) Pérdida o deterioro de sistemas, soportes de almacenamiento, informació n Otra empresa no puede cumplir objetivos, HW-I*,HW-E*,SW-I*,HW-P*, SW-P*, SW-E*, SW-C*,I-1, I-2,I.3,I-4	Alto
A-13	Daño en empresa-actividad / Daño en activos tecnológicos e información / Daño a otra empresa	Pérdida económica directa Incapacidad de continuar/recuperar cierta actividad o llevarla a cabo de manera correcta (desarrollo código/proyecto) Pérdida o deterioro de sistemas, soportes de almacenamiento, informació n Otra empresa no puede cumplir objetivos HW-I*,HW-E*,SW-I*,HW-P*, SW-P*, SW-E*, SW-C*,I-1, I-2,I.3,I-4	Alto
A-17	Daño en activos tecnológicos e información	Pérdida o deterioro de sistemas, soportes de almacenamiento, informació n	Bajo
A-19	Daño en activos tecnológicos e información / Daños personales	Deterioro del sistema Robo de datos personales HW-M.1, CH-1, CH-2, CH-3, CH-4	Bajo
A-20	Daño en empresa-actividad / Daño en activos tecnológicos e información	Deterioro de imagen y reputación Pérdida o deterioro de sistemas, soportes de almacenamiento, informació n SW-E*,HW-E*	Bajo

A-21	Daño en empresa-actividad / Daño en activos tecnológicos e información	Deterioro de imagen y reputación Pérdida o deterioro de sistemas, soportes de almacenamiento, informació n SW-I*,HW-I*,HW-P*, SW-P*,I-1, I-2,I.3,I-4	Moderado
A-23	Daño en empresa-actividad / Daño en activos tecnológicos e información	Deterioro de imagen y reputación Pérdida o deterioro de sistemas, soportes de almacenamiento, informació n SW-I*,HW-I*,SW-E*,HW-P*, SW-P*,HW-E*,I-1, I-2,I.3,I-4	Moderado
A-25	Daño en empresa-actividad / Daño en activos tecnológicos e información / Daño a otras empresas	Deterioro de imagen y reputación Incapacidad de continuar/recuperar cierta actividad o llevarla a cabo de manera correcta (desarrollo código/proyecto) Pérdida o deterioro de sistemas, soportes de almacenamiento, informació n Daño a otras empresas para cumplimiento de compromisos SW-I*,HW-I*,HW-P*, SW-E*,HW-E*,I-1, I-2,I.3,I-4, SW-C*,HW-C*	Alto
A-29	Daño en activos tecnológicos e información	Pérdida o deterioro de sistemas, soportes de almacenamiento, informació n	Bajo
A-30	Daño en activos tecnológicos e información	Pérdida o deterioro de sistemas, soportes de almacenamiento, informació n	Bajo
A-32	Daño en empresa-actividad	Pérdida o deterioro de sistemas,, instalaciones soportes de almacenamiento, informació n HW-I*,I-1, I-2,I.3,I-4, HW-P*, II-*	Moderado
A-33	Daño en empresa-actividad / Daño en activos tecnológicos e información	Incapacidad de continuar/recuperar cierta actividad o llevarla a cabo de manera correcta (desarrollo código/proyecto) Pérdida o deterioro de sistemas, soportes de almacenamiento, informació n SW-E*,I-2	Moderado
A-35	Daño en activos tecnológicos e información	Pérdida o deterioro de sistemas, soportes de almacenamiento, informació n I-*	Moderado
A-39	Daño en empresa-actividad	Deterioro de imagen y reputación	Bajo
A-40	Daño en empresa-actividad	Deterioro de imagen y reputación	Muy bajo
A-43	Daño en empresa-actividad / Daño en activos tecnológicos e información / Daño a otras empresas / Daño a otras empresas	Deterioro de imagen y reputación Incapacidad de continuar/recuperar cierta actividad o llevarla a cabo de manera correcta (desarrollo código/proyecto) Pérdida o deterioro de sistemas, soportes de almacenamiento, informació n Daño a otras empresas para cumplimiento de compromisos-contratos SW-I*,HW-I*,HW-P*, SW-E*,HW-E*,I-1, I-2,I.3,I-4, SW-C*,HW-C*	Alto
A-45	Daño en activos tecnológicos e información	Pérdida o deterioro de sistemas, soportes de almacenamiento, informació n SW-I*	Bajo
A-46	Daño en activos tecnológicos e información	Pérdida o deterioro de sistemas, soportes de almacenamiento, informació n SW-E*,HW-E*	Bajo
A-47	Daño en activos tecnológicos e información	Pérdida o deterioro de sistemas, soportes de almacenamiento, informació n SW-I*,HW-I*,HW-P*, I-1, I-2,I.3,I-4,	Moderado

A-48	Daño en activos tecnológicos e información	Pérdida o deterioro de sistemas, soportes de almacenamiento, informació n SW-I*,HW-I*,HW-P*,SW-PI, I-1, I-2,I.3,I-4,	Moderado
A-49	Daño en activos tecnológicos e información	I-1, I-2,I.3,I-4,	Bajo
A-50	Daño en empresa-actividad / Daños personales / Daño a otras empresas	Deterioro de imagen y reputación Incapacidad de continuar/recuperar cierta actividad o llevarla a cabo de manera correcta (desarrollo código/proyecto) Pérdida de datos personales Deterioro de imagen de otra empresa I-1, I-2,I.3,I-4 CH-1, CH-2, CH-3, CH-4	Alto
A-52	Daño en empresa-actividad / Daños personales / daño a otras empresas	Deterioro de imagen y reputación Incapacidad de continuar/recuperar cierta actividad o llevarla a cabo de manera correcta (desarrollo código/proyecto) Pérdida de datos personales Deterioro de imagen de otra empresa I-1, I-2,I.3,I-4 CH-1, CH-2, CH-3, CH-4	Alto
A-53	Daño en empresa-actividad / Daños personales / daño a otras empresas	Deterioro de imagen y reputación Incapacidad de continuar/recuperar cierta actividad o llevarla a cabo de manera correcta (desarrollo código/proyecto) Pérdida de datos personales Deterioro de imagen de otra empresa I-1, I-2,I.3,I-4 CH-1, CH-2, CH-3, CH-4	Alto
A-54	Daño en empresa-actividad / Daños personales / daño a otras empresas	Deterioro de imagen y reputación Incapacidad de continuar/recuperar cierta actividad o llevarla a cabo de manera correcta (desarrollo código/proyecto) Pérdida de datos personales Deterioro de imagen de otra empresa I-1, I-2,I.3,I-4 CH-1, CH-2, CH-3, CH-4	Alto
A-55	Daño en activos tecnológicos e información	Pérdida o deterioro de sistemas, soportes de almacenamiento, informació n SW-I*,SW-C*,SW-E*,I-1, I-2,I.3,I-4	Moderado
A-56	Daño en empresa-actividad / Daño en activos tecnológicos e información / Daños personales	Incapacidad de continuar/recuperar cierta actividad o llevarla a cabo de manera correcta HW-I*,HW-P*, II-6, CH-1, CH-2, CH-3, CH-4	Muy alto
A-57	Daño en empresa-actividad / Daño en activos tecnológicos e información	Pérdida o deterioro de sistemas, soportes de almacenamiento, informació n Incumplimiento ley y compromisos-contractuales HW-I.5 , I-5,	Bajo
A-58	Daño en activos tecnológicos e información	Pérdida o deterioro de sistemas, soportes de almacenamiento, informació n HW-P*, HW-I*,I*	Bajo
A-59	Daño en activos tecnológicos e información	Pérdida o deterioro de sistemas, soportes de almacenamiento, informació n HW-P*, HW-I*,I*	Bajo
A-60	Daño en empresa-actividad / Daño en activos tecnológicos e información / Daño a otras empresas	Deterioro de imagen y reputación Pérdida o deterioro de sistemas, soportes de almacenamiento, informació n Deterioro de imagen de otra empresa	Bajo

		Daño a otras empresas para cumplimiento de compromisos-contratos SW-C.*, HW-C.*	
A-61	Daño en activos tecnológicos e información	Pérdida o deterioro de sistemas, soportes de almacenamiento, informació n HW-P*	Bajo
A-62	Daño en empresa-actividad	Incapacidad de continuar/recuperar cierta actividad o llevarla a cabo de manera correcta HW-I.*, SW-I.*	Bajo
A-63	Daño en empresa-actividad / Daño a otras empresas	Incapacidad de continuar/recuperar cierta actividad o llevarla a cabo de manera correcta Daño a operaciones/compromisos de otra empresa SW-E.*, SW-I.*,SW-C*	Bajo
A-64	Daño en empresa-actividad / Daño en activos tecnológicos e información / Daño a otras empresas	Pérdida o deterioro de sistemas, soportes de almacenamiento, informació n Incumplimiento de ley Daño a operaciones/compromisos de otra empresa SW-E.*, SW-I.*, SW-C*, I-1	Bajo
A-65	Daño en empresa-actividad / Daño a otras empresas	Incapacidad de continuar/recuperar cierta actividad o llevarla a cabo de manera correcta Daño a operaciones/compromisos de otra empresa SW-E.*, SW-I.*,SW-C*	Bajo
A-66	Daño en activos tecnológicos e información	Pérdida o deterioro de sistemas, soportes de almacenamiento, informació n SW-I*,I-*	Bajo
A-67	Daño en activos tecnológicos e información	Pérdida o deterioro de sistemas, red, soportes de almacenamiento, informació n	Muy bajo
A-68	Daño en activos tecnológicos e información	Pérdida o deterioro de sistemas, red, soportes de almacenamiento, informació n	Bajo

Tabla 13: Análisis del impacto

Por cada amenaza, y después de determinar su probabilidad media, en esta tabla se recoge el máximo del impacto que sufriría la organización. Para más detalle, se han recogido los activos que sufrirían el impacto o que se verían afectados.

6.8 Valoración del Riesgo

6.8.1 Riesgo de amenazas intencionadas

1	2	3	4	5	6	7	8	9	10	11	12	13
Amenaza	Fuente amenaza	Características de fuente amenaza			Relevancia	Prob. Iniciación ataque	Vulnerabilidad y condiciones predispuestas	Severidad y envergadura	Probabilidad de éxito de ataque	Media de probabilidad	Nivel de impacto	Riesgo
		Capacidad	Intención	Selección (targeting)								
A-1	FAA-2	Alto	Moderado	Muy bajo	Posible	Bajo	-	-	Moderado	Bajo	Muy bajo	Muy bajo
A-3	FAA-2	Alto	Moderado	Muy bajo	Posible	Moderado		-	Moderado	Moderado	Muy bajo	Muy bajo
A-8	FAA-2	Alto	Moderado	Muy bajo	Posible	Moderado	Alto (V-24)	-		Alto	Moderado	Moderado
A-9	FAA-2	Alto	Moderado	Muy bajo	Confirmado	Moderado	Alto (V-7)	-	Moderado	Moderado	Muy bajo	Muy bajo
A-10	FAA-2	Alto	Moderado	Muy bajo	Posible	Bajo	Alto (V-7) Alto (V-4) Alto (V-5)	Moderado (CP-4) Bajo (CP-5)	Alto	Moderado	Moderado	Moderado
A-11	FAA-4	Bajo	Bajo	Muy bajo	Confirmado	Alto	Alto (V-24) Alto (v-5) Alto (V-4)	-	Moderado	Moderado	Moderado	Moderado
A-12	FAA-2	Alto	Moderado	Muy bajo	Confirmado	Alto	Alto (V-24) Alto (v-5) Alto (V-4)	-	Moderado	Moderado	Alto	Moderado
A-13	FAA-2	Alto	Moderado	Muy bajo	Confirmado	Alto	Alto (V-24) Alto (V-5) Alto (V-4)	-	Alto	Alto	Alto	Alto

1	2	3	4	5	6	7	8	9	10	11	12	13
A-17	FAA-2	Alto	Moderado	Muy bajo	Confirmado	Moderado	Alto (V-24) Alto (V-5) Alto (V-4) Moderado (V-9)	-	Alto	Moderado	Bajo	Bajo
A-19	FAA-2	Alto	Moderado	Muy bajo	Posible	Moderado	Alto (V-24) Alto (V-4) Alto (V-6)		Alto	Moderado	Bajo	Bajo
A-20	FAA-2	Alto	Moderado	Muy bajo	Esperado	Alto	Alto (V-4) Alto (V-5) Alto (V-6)		Muy alto	Muy alto	Bajo	Bajo
A-21	FAA-2	Alto	Moderado	Muy bajo	Posible	Moderado	Alto (V-4) Alto (V-5) Alto (V-6)		Muy alto	Alto	Moderado	Moderado
A-23	FAA-2	Alto	Moderado	Muy bajo	Predicho	Moderado	Alto (V-4) Alto (V-5) Alto (V-6)		Muy alto	Alto	Moderado	Moderado
A-25	FAA-2	Alto	Moderado	Muy bajo	Posible	Moderado	Moderado (V-21)		Muy alto	Alto	Alto	Alto
A-29	FAA-4	Bajo	Bajo	Muy bajo	Posible	Bajo	-	-	Alto	Alto	Bajo	Bajo
A-30	FAA-2	Alto	Moderado	Muy bajo	Esperado	Moderado	-	-	Alto	Moderado	Bajo	Bajo
A-32	FAA-6	Moderado	Bajo	Muy bajo	Posible	Bajo	Moderado (V-21) Moderado (V-2)	Muy alto (CP-2)	Muy alto	Moderado	Moderado	Moderado
A-33	FAA-2	Alto	Moderado	Muy bajo	Confirmado	Muy alto	Alto (V-7) Alto (V-24)	Moderado (CP-4) Bajo (CP-5)	Muy alto	Muy alto	Moderado	Moderado
A-35	FAA-2	Alto	Moderado	Muy bajo	Posible	Bajo	-	Moderado (CP-4) Bajo (CP-5)	Moderado	Bajo	Moderado	Bajo
A-39	FAA-2	Alto	Moderado	Muy bajo	Confirmado	Moderado	Alto (V-7) Alto (V-6)	-	Moderado	Moderado	Bajo	Bajo
A-40	FAA-4	Bajo	Bajo	Muy bajo	Confirmado	Bajo	Alto (V-7) Alto (V-6)	-	Moderado	Bajo	Muy bajo	Muy bajo
A-43	FAA-2	Alto	Moderado	Muy bajo	Predicho	Moderado	Alto (V-4) Alto (V-5) Alto (V-6)	Moderado (CP-4) Bajo (CP-5)	Muy alto	Alto	Alto	Alto

1	2	3	4	5	6	7	8	9	10	11	12	13
A-45	FAA-2	Alto	Moderado	Muy bajo	Confirmado	Moderado	Moderado (V-20)	-	Alto	Moderado	Bajo	Bajo
A-46	FAA-2	Alto	Moderado	Muy bajo	Confirmado	Alto	Alto (V-19)	-	Moderado	Moderado	Bajo	Bajo
A-47	FAA-6	Moderado	Bajo	Muy bajo	Posible	Bajo	Alto (V-25) Moderado (V-21)	-	Muy alto	Moderado	Moderado	Moderado
A-48	FAA-7	Bajo	Baja	Muy bajo	Posible	Bajo	Moderado (V-26)		Muy alto	Moderado	Moderado	Moderado
A-49	FAA-7	Bajo	Baja	Muy bajo	Posible	Bajo	-	Moderado (CP-4) Bajo (CP-5)	Moderado	Bajo	Bajo	Bajo
A-50	FAA-2	Alto	Moderado	Muy bajo	Posible	Bajo	-	Moderado (CP-4) Bajo (CP-5)	Muy alto	Moderado	Alto	Moderado

Tabla 14: Riesgos de amenazas intencionadas

6.8.2 Riesgo de amenazas no intencionadas

1	2	3	4	5	6	7	8	9	10	11
Amenaza	Fuente de amenaza	Rango de efectos	Relevancia	Probabilidad de ocurrencia	Vulnerabilidad y condiciones predispuestas	Severidad y envergadura	Probabilidad de impacto adverso	Media de probabilidad	Nivel de impacto	Riesgo
A-52	FAN-13	Moderado	Confirmado	Alto	Moderado (V-27) Moderado (V-11)	Moderado (CP-4)	Moderado	Moderado	Alto	Moderado
A-53	FAN-14	Alto	Confirmado	Moderado	Moderado (V-27) Moderado (V-11)	Moderado (CP-4)	Moderado	Moderado	Alto	Moderado
A-54	FAN-14	Alto	Confirmado	Bajo	Moderado (V-27) Moderado (V-11)	Moderado (CP-4)	Alto	Moderado	Alto	Moderado
A-55	FAN-14	Alto	Confirmado	Muy alto	Alto (V-23)	-	Moderado	Alto	Moderado	Moderado
A-56	FAN-10	Muy alto	Posible	Muy bajo	Moderado (V-2)	Muy alto (CP2)	Muy alto	Bajo	Muy alto	Muy bajo
A-57	FAN-10	Muy alto	Posible	Muy bajo	Moderado (V-2)	Muy alto (CP2)	Alto	Bajo	Bajo	Bajo
A-58	FAN-1	Baja	Confirmado	Bajo	Alto (V-3)		Moderado	Bajo	Bajo	Bajo
A-59	FAN-1	Baja	Confirmado	Bajo	Alto (V-3) Alto (V-16) Moderado (V-22)		Moderado	Bajo	Bajo	Bajo
A-60	FAN-2	Muy baja	Confirmado	Moderado	Bajo (V-28)	Bajo (CP-5)	Bajo	Bajo	Bajo	Bajo
A-61	FAN-3	Baja	Confirmado	Moderado	Bajo (V-29)	Muy alto (CP-1)	Moderado	Moderado	Bajo	Bajo

1	2	3	4	5	6	7	8	9	10	11
A-62	FAN-5	Alto	Confirmado	Moderado	Moderado (V-20)		Moderado	Moderado	Bajo	Bajo
A-63	FAN-7	Baja	Confirmado	Bajo	Alto (V-4) Alto (V-5) Alto (V-6) Moderado (V-20)		Alto	Moderado	Bajo	Bajo
A-64	FAN-13	Moderado	Confirmado	Moderado	Alto (V-7) Alto (V-19) Alto (V-24)		Alto	Moderado	Bajo	Bajo
A-65	FAN-8	Baja	Confirmado	Bajo	Alto (V-4) Alto (V-5) Alto (V-6) Moderado (V-20)		Alto	Moderado	Bajo	Bajo
A-66	FAN-5	Alto	Confirmado	Bajo	Moderado (V-20) Moderado (V-19)	Alto (CP-3)	Muy alto	Moderado	Bajo	Bajo
A-67	FAN-11	Alto	Confirmado	Bajo		Muy alto (CP-1)	Bajo	Bajo	Muy bajo	Muy bajo
A-68	FAN-11	Alto	Confirmado	Moderado		Muy alto (CP-1)	Alto	Moderado	Bajo	Bajo

Tabla 15: Riesgos de amenazas no intencionadas

6.8.3 Resumen de resultados

Valor	Descripción	Nº de aparaciones
Muy alto	Significa que una amenaza puede causar **múltiples daños graves o catastróficos**, llegando a dañar a la propia empresa, sus activos, actividades, personal y otras organizaciones	0
Alto	Significa que una amenaza puede causar **algún daño grave o catastrófico**, llegando a dañar a la propia empresa, sus activos, actividades, personal y otras organizaciones	3 A-25,A-13, A-43
Moderado	Significa que una amenaza puede causar **algún daño serio** a la propia empresa, sus activos, actividades, personal y otras organizaciones	14 A8,A10,A11,A12,A21,A23,A32,A33, A47,A48,A50,A52,A53,A54,A55
Bajo	Significa que la amenaza puede causar **algún daño limitado** a la propia empresa, sus activos, actividades, personal y otras organizaciones	21
Muy bajo	Significa que la amenaza puede causar a**lgún daño insignificante** a la propia empresa, sus activos, actividades, personal y otras organizaciones	6

Tabla 16: Resumen de valores de riesgos

6.9 Nivel de Riesgo Aceptable

Es necesario definir un límite a partir del cual podamos decidir si asumir un riesgo o por el contrario no asumirlo y por tanto aplicar controles. En el caso de Secure Team el nivel de riesgo aceptable es "bajo", todo lo que esté a la par o por debajo de este nivel de riesgo, no supondrá una amenaza importante para la empresa, y por tanto no se plantearán medidas para reducir o mitigar esos riesgos. Todo lo contrario ocurrirá si el nivel de riesgo supera el aceptable que como se ha dicho, será "bajo", en cuyo caso tendremos que establecer controles para reducirlo.

6.10 Recomendaciones para el tratamiento

De forma muy breve y de cara al apartado de propuestas de proyecto, teniendo en cuenta que el nivel de riesgo aceptable establecido es el "bajo", se hacen las siguientes recomendaciones agrupando diferentes amenazas de parecido origen o fuente de amenaza que suponen un riesgo alto y/o moderado.

Recomendación	Amenazas
Mejorar o implantar más controles de cara a ataques (hackers, script kiddies...) (firewalls, sistemas operativos, pentestings)	A13, A25, A43, A8, A10, A11, A12, A21, A23, A33,
Mejorar o implantar controles perimetrales (registro, alarmas, cámaras...)	A32, A47, A48
Mejorar o implantar o establecer medidas para el control y de buenas prácticas de los miembros sobre información	A52, A53, A54, A55
Formalizar control de acceso/asignación de permisos	A55, A43

Tabla 17: Recomendaciones generales para mitigar o reducir riesgos

7. Propuestas de Proyectos

Si tomamos en cuenta que el riesgo aceptable por Secure Team se ha establecido en "moderado", quedarían 3 riesgos altos y 14 moderados. En un principio, la prioridades de los proyectos se plantearán para intentar mitigar o disminuir en primer lugar los riesgos valorados como altos y luego, como se recomienda en el apartado 6.10, sobre las que actúan en mayor cantidad de amenazas.

Los proyectos se cualifican económicamente y planifican en el tiempo, estableciendo plazos de consecución de sus objetivos (en general, corto, medio y largo plazo). Adicionalmente, la planificación recoge puntos de control que permitan considerar realmente el Plan de Implementación del SGSI como un proceso de mejora continua. Los proyectos no sólo responden a la mejora en relación con la gestión de la seguridad, sino también en posibles beneficios colaterales como puede ser la optimización de recursos, mejora en la gestión de procesos y tecnologías presentes en la organización.

7.1 Proyecto 1

Título	Concienciación y formación frente a malware	
Responsable	Responsable de Seguridad	
Prioridad	Alta	
Control Anexo A 27001	A 7.2.2 Concienciación, educación y capacitación en seguridad de la información A 12.2.1 Controles contra el código malicioso	
Objetivo	• Concienciar a los miembros de la creciente amenaza de malware por correo entre otros medios • Interiorizar los criterios mínimos de buenas prácticas para prevenir malware por correo • Formar como mínimo al responsable en seguridad en implantar y configurar el servidor de correo para evitar malware, spam...	
Descripción	Como se constata en las amenazas A13, A12, A8 el envío de malware y otras técnicas como el phising suponen un riesgo alto y/o moderado para la empresa. En el caso del malware, en principio, es verdad que en el departamento de desarrollo se está usando Linux y que la amenaza es menor en dichos sistemas, pero sigue siendo una amenaza importante para la empresa, ya que también existen sistemas Windows y siempre hay correos cruzados entre empleados de diferentes departamentos. Por otro lado, en el caso del phising, independientemente del sistema, es una amenaza en la que su éxito recae en el factor humano. Este proyecto tiene que aportar un mayor conocimiento de dichas amenazas, de buenas prácticas para evitarlo y algún conocimiento técnico para poder desplegar medidas que reduzcan el riesgo o lo mitiguen. Por lo tanto, se hará lo siguiente: • Se formará al responsable de seguridad para que mejore las medidas técnicas del servidor y clientes de correo. • El responsable, con posterioridad preparará o recopilará cierta información interesante y hará una presentación/sesión para que los empleados puedan concienciarse y puedan tener en cuenta ciertas prácticas.	
Motivo	Reducir y/o mitigar riesgos relativas a las amenazas A13, A12, A8, A43	
Coste o impacto económico	Curso del responsable	450€
	Total	450€
Mejora o beneficio colateral		

Tabla 18: Proyecto 1: concienciación y formación frente a malware

7.2 Proyecto 2

Título	Estudiar, testear y mejorar firewall	
Responsable	Responsable de seguridad	
Prioridad	Medio	
Control Anexo A 27001	A.13.1.1 Controles de red	
Objetivo	• Definir las necesidades de entrada y salida • Conocer estado del firewall (configuración, versión..) y documentarlo • Detectar deficiencias, reglas a mejorar o reglas incorrectas • Actualizar y corregir la configuración	
Descripción	Se recomienda usar políticas drop, es decir, denegar todo y luego solo habilitar aquello que se necesita. Para testear y tener una correcta configuración de firewall, habría que hacer un estudio de qué servicios hay, para quién o desde donde y cosas similares... Una vez definido todo eso, habría que ver si la configuración actual del firewall es correcta, y si hay firewalls y cómo están, en aquellas máquinas-servidores que ofrecen servicios y también en máquinas de puestos, y si así se requiere configurar esos firewalls de cada máquina también. Otra opción sería pasar a firewall en hardware, pero requiere una mayor inversión ya que solo el firewall costaría unos 700€ , y se puede decir que con los conocimientos del responsable de seguridad, y siguiendo las pautas mencionados y el testeo, y considerando que no tiene demasiada complejidad el control de red/servicios de Secure Team y por lo tanto menor probabilidad de meter la pata, se descarta la opción de firewall hardware.	
Motivo	Reducir riesgos relativas a la amenaza A43	
Coste o impacto económico	Estudiar necesidades	400€
	Formación configuración y testeo (iptables, nmap...)	500€
	Testear / reconfigurar / actualizar firewall	400€
	Total	1300€
Mejora o beneficio colateral	Adquirir conocimientos para testear firewalls de clientes y configurarlos mejor Al documentar, no depender únicamente del conociemiento del Responsable de Seguridad del firewall	

Tabla 19: Proyecto 2: Estudiar, testear y mejorar firewall

7.3 Proyecto 3

Título	Clasificación, etiquetado y tratamiento de información	
Responsable	Gerente	
Prioridad	Alto	
Control Anexo A 27001	A.8.2.1 Clasificación de la información A.8.2.2 Etiquetado de la información A.8.2.3 Manipulado de la información	
Objetivo	• Asegurar que la información reciba un nivel adecuado de protección de acuerdo con su importancia para la organización • Clasificar la información en términos de la importancia de su revelación frente a requisitos legales, valor, sensibilidad y criticidad ante revelación o modificación no autorizadas. • Etiquetar la información en base a la clasificación • Establecer unos procedimientos de uso en base a la clasificación • Concienciar sobre los procedimientos de etiquetado tanto a empleados como a externos	
Descripción	Se conoce que el envío de información crítica por correo, o por otros medios se hace sin control. Ello supone un riesgo moderado. Pero en el fondo de dicha amenaza está la falta de conocimiento de la criticad, o grado de confidencialidad requerida para la información que se maneja, la falta de procedimientos más concretos en base a una clasificación de la información. Por lo tanto se propone hacer dicha tarea, en la que el responsable será el gerente, y le ayudará el responsable de seguridad. Para el desarrollo de dicha tarea, se usará como guía de implementación el control 8 Clasificación de la información de la ISO 27002.	
Motivo	Reducir riesgos relativas a A52, A53, A54	
Coste o impacto económico	Clasificar, etiquetar y establecer procedimiento	400€
	Total	400€
Mejora o beneficio colateral	• Mayor confianza y mejora de imagen frente a clientes • Ante otros incidentes o amenazas, poder conocer mejor el riesgo en base a información concreta	

Tabla 20: Proyecto 3 Clasificación, etiquetado y tratamiento de información

7.4 Proyecto 4

Título	Implantación de cámaras y alarma	
Responsable	Responsable de seguridad	
Prioridad	Baja	
Control Anexo A 27001	A.11.1.1 Perímetro de seguridad física	
Objetivo	• Evitar robos • Detectar robos • Trazar robos	
Descripción	Aunque podrían instalarse varias cámaras, solo se instalará una en el interior de la oficia enfocando a la puerta de acceso, ya que no sería necesario tener videovigilado todo la oficina, y estando este en un 3. piso, la única entrada realista es por la puerta. En el exterior del edificio, aunque no es un despliegue demasiado importante, existen cámaras. Junto a la instalación de alarmas y videocámaras, se instalarán señales o indicadores para comunicar su existencia y así evadir o evitar robos y también que cualquiera esté informado que se le está grabando. Se recurrirá a una empresa especializada en la materia, y que cumpla ya con estándares y los requisitos legales de dicho control.	
Motivo	Reducir riesgos relativas a A47, A48, A32	
Coste o impacto económico	Cuota mensual	60€
	Total	12 x 60 = 720 €
Mejora o beneficio colateral	Puede que reduzcan costes en el seguro.	

Tabla 21: Proyecto 4: Implantación de cámaras y alarma

7.5 Proyecto 5

Título	Implantación de registro de visitas/personal ajeno	
Responsable	Responsable de Departamento Desarrollo	
Prioridad	Media	
Control Anexo A 27001	A.11.1.2 Controles físicos de entrada	
Objetivo	• Conocer entrada personal ajeno a la empresa para que ante cualquier incidente, robo o impacto, pudiera analizar su implicación.	
Descripción	En las oficinas de la empresa entran y salen clientes, técnicos (telefonía, aire, extintores...), repartidores... Pero no hay ningún control de ello. Habría que llevar un registro de esas visitas o esas entradas de personas. Se podría simplemente llevar en una hoja, pero teniendo un programadores en la misma empresa, sería bastante simple desarrollar una aplicación o un módulo para alguna aplicación existente, en la que se podría llevar ese control, además, de esta forma también se llevaría quién registro la visita. Sería conveniente junto al desarrollo de la aplicación, establecer un procedimiento para dicho control y uso del registro. Se plantea que el desarrollo lo haga algún programador de la empresa y la definición la haga el responsable de este proyecto.	
Motivo	Reducir riesgos relativas a A48	
Coste o impacto económico	Definición aplicación y desarrollo	500€
	Definición y redacción del procedimiento	180€
	Total	680€
Mejora o beneficio colateral		

Tabla 22: Proyecto 5: Implantación de registro de visitas/personal ajeno

7.6 Proyecto 6

Título	Pentesting de software crítico	
Responsable	Responsable del Departamento de Desarrollo	
Prioridad	Alto	
Control Anexo A 27001	A.12.6.1 Gestión de las vulnerabilidades técnicas	
Objetivo	• Conocer vulnerabilidades en software crítico • Obtener recomendaciones para mejorar medidas en software desarrollado	
Descripción	Secure Team dispone de varias aplicaciones desarrolladas por ella misma para la gestión de licencias de trabajo (vacaciones,horarios,bajas, etc.) , gestión de incidencias, tareas, presupuestos y propuestas, CMDB... También la propia web de la empresa, que a día de hoy es importante pero no entraría en el alcance de este proyecto de pentesting al no considerarlo crítico. Sería conveniente, ante el riesgo que suponen ciertas amenazas relacionadas con la explotación de vulnerabilidades, conocer las vulnerabilidades que tienen estas aplicaciones y conocer cómo se pueden solventar. Al considerar que la fuente de las amenazas son grupos de hackers cualificados, para que el pentesting sea en cierto modo lo más parecido, es contratar una empresa externa especializada en pentesting para encargarle un pentesting en modo black box (sin información previa (sin conocimiento de código, lenguage..) o con el mínimo...) y un informe con resultados y recomendaciones. El pentesting de aplicaciones se hará en un entorno cerrado, es decir, con una copia reciente de datos, idéntico código deplegado, etc. pero sin hacerlo en producción para que no tenga un impacto adverso.	
Motivo	Reducir riesgos relativas a amenazas A50, A43, A21, A10	
Coste o impacto económico	Pentesting	3500€
	Total	3500€
Mejora o beneficio colateral	Mayor confianza a los clientes de que la información está en sistemas testeados Ciertas recomendaciones servirán para implantarlos en otros desarrollos realizados.	

Tabla 23: Proyecto 6: Pentesting de software crítico

7.7 Proyecto 7

Título	Pentesting de sistemas-servidores	
Responsable	Responsable de Seguridad	
Prioridad	Alto	
Control Anexo A 27001	A.12.6.1 Gestión de las vulnerabilidades técnicas	
Objetivo	• Conocer estado de penetrabilidad en los sistemas (Testear servidores donde está wiki, alfresco, svn, web, aplicaciones de gestión) • Obtener recomendaciones	
Descripción	Del mismo modo que puede haber vulnerabilidades por errores o malas prácticas de programación, un sistema no actualizado, o mal configurado puede dar lugar a accesos no autorizados, a explotación de diferentes vulnerabilidades que afecten al correcto funcionamiento o que revelen información. Al considerar que la fuente de las amenazas son grupos de hackers cualificados, para que el pentesting sea en cierto modo lo más parecido, es contratar una empresa externa especializada en pentesting para encargarle un pentesting en modo black box (sin información previa (sin conocimiento de código, lenguage..) o con el mínimo...) y un informe con resultados y recomendaciones. La idea es testear aquellas máquinas servidores o que tengan algún servicio, software o información crítica. Teniendo en cuenta que ciertas máquinas están dentro de la red que solamente es accesible con vpn, lo suyo sería testear la máquina que hace tiene openvpn, firewall y dhcp. Ya que las explotación de alguna vulnerabilidad en dicha máquina podría derivar en una alteración en dichos servicios... Y por otro lado, habría que testear la VPS que alberga el programa de gestión de licencias y de gestión,	
Motivo	Reducir riesgos relativas a las amenazas A43, A21, A50, A33 (una vez obtenido acceso..)	
Coste o impacto económico	Pentesting	5000€
	Total	5000€
Mejora o beneficio colateral	Mayor confianza a los clientes de que la información está en sistemas testeados Poder aplicar ciertas recomendaciones en otros sistemas.	

Tabla 24: Proyecto 7: Pentesting de sistemas-servidores

7.8 Proyecto 8

Título	Definir política y modo de gestión de roles-permisos	
Responsable	Gerente	
Prioridad	Medio	
Control Anexo A 27001	Todos los controles de A.9.1 Requisitos de negocio para el control de acceso y A.9.2 Gestión de acceso de usuario	
Objetivo	• Otorgar permisos solo para aquello necesario • Controlar mejor el acceso a servicios/recursos	
Descripción	Hasta la fecha, como ya se ha comentado anteriormente, en Secure Team la gestión de roles/permisos las ha llevado a cabo el Responsable de Seguridad, y el modo de hacerlo a sido improvisado, según la necesidad. Pero no se ha basado en una política, y además se ha confiado en la gestión. Partiendo de esa realidad, se ha visto que la amenaza de una mala asignación de permisos supone un riesgo considerable (moderado), y la amenaza que suponen lo accesos no autorizados de hackers o de otros también podría agravarse en a raíz de una asignación demasiado permisivo para cualquier usuario. Además, habiendo un organigrama definido, y unas funciones bastante marcadas, lo suyo sería trasladar esa realidad a roles/permisos en el sistema. Hacer esa tarea exige la definición una política de roles, y los permisos de estos a servicios/recursos. En principio sería aplicar el modo RBAC y que todo lo relativo a esta gestión se defina y se implemente por parte del Responsable de Seguridad.	
Motivo	Reducir riesgos relativas a A55, A43 (una vez obtenido acceso..)	
Coste o impacto económico	Definición de roles-permisos	800€
	Implementación técnica	400€
	Total	1200€
Mejora o beneficio colateral	Tenerlo documentado para cualquier inprevisto con el Responsable de Seguridad (bajas, deja la empresa...)	

Tabla 25: Proyecto 8: Definir método de asignación de roles-permisos

7.9 Proyecto 9

Título	Actualizaciones de sistema operativo	
Responsable	Responsable de Seguridad	
Prioridad	Bajo	
Control Anexo A 27001	Aunque no lo especifica como explicitamente, se podría asociar con 12.2.1 Controles contra el código malicioso (la reducción de vulnerabilidades que podrían ser explotadas por el código malicioso...)	
Objetivo	• Evitar explotacion de vulnerabilidades • Tener sistemas estables y LTS • Posibilitar compatibilidades con las nuevas aplicaciones y tecnología.	
Descripción	Por un lado estarían los sistemas Linux, y por otra parte los Windows. En cuanto a los Linux, en los puestos se está usando Ubuntu en versión 16.04 LTS . En cuanto a los Windows, también están actualizados a nivel de versión. Pero convendría tener instalados parches y actualizaciones que cubran las vulnerabilidades, y elaborar un procedimiento para que esto se haga de forma ordenada y normalizada, y siempre siguiendo un criterio (ejemplo: la penúltima version estable...). Conviene también revisar los sistemas operativos de los servidores y actualizarlos a versiones LTS. Se propone hacer este trabajo fuera del horario de actividad. Y que lo haga un técnico de la propia empresa.	
Motivo	Mitigar/reducir riesgo de amenazas A23, A21, A50	
Coste o impacto económico	Instalación de actualizaciones	300€
	Elaboración de norma y procedimiento	200€
	Total	500€
Mejora o beneficio colateral	Tener la opción de usar software más nuevo y con más funciones	

Tabla 26: Proyecto 9: Actualizaciones de sistema operativo

7.10 Planificación de proyectos

Teniendo en cuenta a que plazo se plantean los proyectos, sus prioridades, y el coste de cada uno (a veces ese coste está estimado de forma que los empleados dedican un tiempo a dichos proyectos), hay que planificar su desarrollo de forma que Secure Team pueda hacer frente a los costes y pueda distribuir la dedicación de los empleados a dichos proyectos de manera que afecten lo menos posible a otras tareas.

Si se suman los costes de todo los proyectos el coste de la inversión o el desembolso es de 13.850 €. Parte del coste es lo que supone que el personal propio dedique tiempo a los proyectos.

El desarrollo de todos los proyectos quedaría planificado para 2 años, y repartiendo el coste de forma similar para cada año. Por otra parte teniendo en cuenta que habría que intentar desarrollar primero los proyectos de mayor prioridad. También se ha tenido en cuenta el aspecto de tener que interferir lo menos posible en la actividad a la hora de llevar a cabo los proyectos, y para ello también se ha planteado una planificación que dura prácticamente 2 años ya que Secure Team no puede dedicar recursos para afrontar el desarrollo de los proyectos paralelamente. Por ejemplo, el pentesting de sistemas-servidores se plantea de julio a septiembre siendo estos unos meses en los que la actividad de Secure Team es menor.

Proyecto	Prio.	Coste	Ene	Feb	Mar	Abr	May	Jun	Jul	Ago	Sep	Oct	Nov	Dic
Pro. 1	alta	450												
Pro. 3	alta	400												
Pro. 7	alta	5000												
Pro 5	media	680												
		6630												

Tabla 27: Planificación de proyectos para 1. año

Proyecto	Prio.	Coste	Ene	Feb	Mar	Abr	May	Jun	Jul	Ago	Sep	Oct	Nov	Dic
Pro. 6	alta	3500												
Pro. 2	media	1300												
Pro. 8	media	1200												
Pro. 9	baja	500												
Pro. 4	baja	720												
		7220												

Tabla 28: Planificación de proyectos 2. año

Se ha cambiado un proyecto de prioridad alta por uno medio para así igualar los costes anuales. Por otra parte, aunque hay proyectos que durarán bastante más que otros, se les ha otorgado el mismo tiempo máximo, ya que se ha decidido que no se desarrollarán en paralelo, por lo tanto hay margen y así el esfuerzo y dedicación puede distribuirse de manera menos intensa.

8. Auditoría de cumplimiento

El objetivo de la auditoría interna es comprobar el cumplimiento de la organización con respecto a los requerimientos de la ISO 27001. Esta auditoría pretende conocer el estado de la empresa tras la implementación del sistema y tras haber desarrollado o llevado a cabo los proyectos propuestos para tratar los riesgos. Esta auditoría se realizará en base al procedimiento definido en el apartado 5.2 . Siendo la primera auditoría se comprobarán los apartados 4 al 10 de la ISO 27001, y al ser la primera auditoría que se va a realizar, se ha decidido comprobar todos los controles que se aplican.

La auditoría pretende:

- Confirmar que la organización cumple con sus políticas y procedimientos.
- Comprobar que el SGSI desarrollado es conforme con las especificaciones de la Norma ISO/IEC 27001.
- Verificar que el SGSI está logrando los objetivos que la organización se ha marcado.

Para conseguir estos objetivos, el equipo auditor se basa en cómo la organización auditada:

- Apoya la política de seguridad desde la dirección. Es decir, su grado de implicación.
- Analiza los riesgos a los que está sometida su información.
- Selecciona los controles basándose en el análisis de riesgos.
- Relaciona el análisis de riesgos, la Declaración de Aplicabilidad, el plan de tratamiento de los riesgos y la política de seguridad.
- Implementa los controles teniendo en cuenta los mecanismos de medida de la efectividad de los mismos, y la consecución de los objetivos de control.
- Revisa la efectividad de su SGSI y de los controles. Cómo se monitoriza, mide, informa y mejora.
- Realiza las auditorías internas y la revisión interna por parte de la dirección.

Como resultado de la auditoría se redactará un informe para emitirlo a la dirección de la empresa para su revisión.

8.1 Especificaciones de la auditoría

En la siguiente tabla se especifican detalles sobre la auditoría interna. El auditor es un empleado de la empresa externa Auditores S.L. Secure Team, siguiendo los principios de las auditorías, es decir, para poder realizar una auditoría que sea objetiva, parcial e independiente, viendo que no podía satisfacer dichos requisitos con personal propio cualificado, ya que estos tienen responsabilidades en decisiones y acciones sobre el SGSI, decidió contratar un servicio profesional de auditores para poder realizar la auditoría interna o de primera parte.

Auditor	Javi M. (Auditores S.L.)
Fecha auditoría	04/12/2017 – 08/12/2017
Lugar	Andoain – Oficinas de Secure Team Coop.
Alcance	Auditar Secure Team Coop para comprobar cumplimiento del SGSI: Controles anexo A de ISO/IEC 27001:2013 Apartados 4-10 de ISO/IEC 27001:2013 Área auditada: Dpto. De Desarrollo y actividades+personal de Secure Team relacionado con actividad de dicho departamento.
Personal auditado	• Responsable de Seguridad • Gerente • Desarrollador • Responsable Dpto. de Desarrollo

Tabla 29: Ficha de auditoría

8.2 Ejecución de la auditoría

Tras designar lo auditores y planificar la auditoría según el procedimiento, y con la aprobación de la dirección, se procedió a la ejecución de la auditoría, la cual se dividió en las siguientes fase:

8.2.1 Recolección de información previa

En este apartado se solicita toda la siguiente información para poder revisarla. En la siguiente fase, en la ejecución de pruebas de auditoría, en el apartado de revisión de documentación, suele ser normal que se solicite más información que pueda ser referenciada o estar asociada a la información solicitada en esta fase:

- Descripción de la empresa
- SOA o Declaración de Aplicabilidad
- Diagrama de red tecnológica
- Organigrama
- Políticas de seguridad
- Procedimientos
- Apartado de términos de contratos de empleados
- Contratos con proveedores
- Inventarios de activos
- Plan de tratamiento de riesgos o proyectos propuestos
- Memorias, documentación, información y facturas relacionadas con propuestas de proyectos
- Actas de reuniones de dirección relacionadas con SGSI
- Comunicaciones relativas a políticas y SGSI
- Informes de incidencias
- Registro de LOPD
- Documentación relativa a permisos y responsables de activos

8.2.2 Ejecución de la auditoría:

Esta fase se ha dividido en tres tareas.

Revisión de documentación

- Al revisar las políticas y procedimientos, se ha solicitado alguna información relacionada con estas si no se ha entregado en la primera fase, por ejemplo, se ha solicitado el registro de copias de seguridad y comprobaciones, o facturas o certificados de licencias adquiridas habiendo una política de actualizar software.

- Informes de incidencias

- Se han revisado memoria de proyectos, facturas... Derivado de estas,, se ha solicitado que se muestre cambio a nivel de código (svn) recomendados en proyectos de pentesting.

Realización de entrevistas y cuestionarios

- La entrevistas: Después de estudiar las responsabilidades/roles y sus funciones, y por intentar interferir lo menos posible en el funcionamiento de Secure Team y a su vez optimizar recursos-tiempo, se ha realizado un muestreo y han realizado 4 entrevistas (responsable, 1 programador, gerente y responsable de seguridad) para conocer si los empleados conocen y cumplen con las políticas, procedimientos y si hay un apoyo por parte de la dirección, si se cumplen las funciones, si se hace seguimiento o no del SGSI y si el comité de seguridad funciona... Éstas han servido para complementar con alguna prueba técnica y las entrevistas se han elaborado adaptando al contexto y en base a toda la información entregada. El objetivo de estas entrevistas ha sido extraer todas las evidencias necesarias para verificar que la organización actúa tal y como refleja la documentación entregada.

  En la siguiente tabla se puede ver un extracto de una entrevista realizada al Responsable de Seguridad:

Procedimiento de comunicaciones relativos al SGSI	
¿Existe algún procedimiento de comunicaciones relativos al SGSI?	Sí
¿Quién es el responsable de emitir dichas comunicaciones?	Mikel C.
¿Desde qué dirección se deben realizar?	sgsi@secureteam.com
Procedimiento de Copias de Seguridad	
¿Quién es el responsable?	Mikel C.
¿Qué responsabilidades tiene?	Automatizar copias semanales Comprobar 1 vez cada 6 meses
Revisión cuestiones organizativas, técnicas o metodológicas. Basandose en tabla indicadores	
¿Cada cuanto hay que revisar?	Hay diferentes indicadores, y no me las conozco de memoria, pero hay un documento que lo define y tengo tareas programadas en base a eso.
Formación	
¿Qué vías y fuentes de formación usas?	Webs... cursos libros
¿A cuántos cursos, talleres y sesiones de formación...vas al año?	Dependiendo de la carga de trabajo, pero siempre intentamos estar al día de cursos que hay en la web, y suelo acudir casi cada dos meses algún curso, charla o evento relacionado con temas de seguridad informática, redes...
¿Costea la empresa todos esos cursos?	Sí. Siempre que tenga algo que ver con lo dicho, seguridad, redes, servidores... sí.
Política de Contraseña	
¿Cada cuánto hay que cambiar de contraseña?	Cada 6 meses
¿Como se acuerdan los empleados de ello?	La política establece que soy yo quien debe de recordarles cada 6 meses que cambien de contraseña, les mando un email a todos.
Coordinación, colaboración, ejemplo	
¿Envías correos con información interesante en torno a la seguridad de la información?(buenas prácticas...)	Intento no agobiar a los empleados, por lo que después de un tiempo, estamos pensando en plantear un tiempo de 30 minutos semanales para dichas cosas. Es decir, mejoras, avisos, notas. Pero hasta ahora, si que envío algunas cosas que salen, como por ejemplo, alguna guía sobre contraseñas seguras, ataques a webs que podrían afectarnos...
¿Planificas, estimas, sigues y valoras las tareas, incidencias...?	Tenemos una aplicación para ello, y siempre intento usarla, pero también intento recoger

	alguna mejora para dicha aplicación, ya que la aplicación de gestión juega un papel fundamental y tiene que responder a las necesidades que van surgiendo y adaptando en lo que se pueda a estas.
¿Convocas, preparas, realizas reuniones con los compañeros?	Si, preparo las reuniones con un orden del día y lo comunico a todos con tiempo, designo siempre alguien para que tome acta y luego me aseguro de que se pasa a limpio. Intento que todos participen pero que no sean debates infinitos. Tenemos apalabrada metodología para las reuniones, pero no está documentada.

Tabla 30: Extracto de la entrevista al Responsable de Seguridad con preguntas más abiertas y adaptadas al contexto, al rol, y basadas en cierta información solicitada (políticas, procedimientos...)

También se han realizado cuestionarios generales a los 4 empleados seleccionados. Así como cada cuanto cambian la contraseña, si existe algún sistema automatizado o cómo recuerdan dicho cambio, si usan el correo al realizar compras en internet u otro uso personal... Algunas de las preguntas, sirven para contrastarlas con las respuestas a las preguntas específicamente preparadas para cada rol.

Ejecución de pruebas técnicas

Conociendo el organigrama, la red tecnológica, y las propuestas de tratamiento de riesgos. Se ha procedido a ciertas pruebas tanto a nivel de redes, aplicaciones...Tampoco se ha procedido a realizar un pentest, ya que no se trata de profundizar tanto y de buscar nuevas vulnerabilidades, teniendo unas políticas y procedimientos, teniendo constancia de haber aplicado proyectos (pentest...) y teniendo un análisis de riesgos, se trata de ver si se cumplen requisitos definidos en esos documentos, si los controles se han implantado y si tienen lógica sobre el análisis de riesgos realizado. Se han usado las siguientes herramientas:

- nessus para aplicaciones
- nmap para la red
- maltego, whois, dns lookup... para información abierta

8.2.3 Análisis de la información

Partiendo de los resultados obtenidos de la revisión de la documentación, entrevistas y cuestionarios y en las pruebas técnicas, se han completado las siguientes tablas. Que indican mayormente los resultados que derivarán en la detección o conclusiones de no conformidades.

ISO 270001 (cumplimiento) apartado del 4 al 10

4. Contexto de la organización	Se cumple	Toda la documentación entregada demuestra que se ha establecido (4.2.1) e implementado el SGSI (4.2.2), se hace un seguimiento (monitoriza y revisa 4.2.3), se mejora 4.2.4 y se cumple con 4.3 requrimientos documentales): políticas, procedimientos, análisis de riesgos, indicadores, propuestas de proyectos para tratamiento de riesgos, auditorías. Se están implantando mejoras (facturas, proyectos). Hay un seguimiento que se constata en actas de reuniones, en informes, en registros de incidencias, una inversión considreable en proyectos, una estructura organización en alineada con necesidades del SGSI y está a su vez con actividad...
5. Liderazgo	Se cumple	La dirección se asegura de de forma periódica y siguiendo unos criterios de que los roles y funciones se estén cumpliendo, y que la asignación de ellas se comunica demuestra un compromiso(5.1).,Eso se recoge, se puede comprobar en convocatorias+actas de reuniones y comunicaciones de estas. También existe gestión de recursos, ya que hay políticas que establecen las normas para ello (uso de correo, activos, equipos, red...) y se están cumpliendo. Además la dirección se ha implicado y ha realizado el esfuerzo requerido elaborando y preparando documentación para el análisis de riesgos, así como el inventario de activos. La adaptación de la estructura de la organización y la inversión en diferentes proyectos demuestra que hay un compromiso para con el SGSI. Estas además están debidamente asignadas, documentadas... Hay una concienciación. Pero no solo eso, la formación de miembros de la dirección son muestra de la disposición, capacitación y concienciación en torno a la seguridad de la información.
6. Planificación	Se cumple	Hay unos objetivos marcados, hay unoas propuestas de proyectos debidamente planificadas, presupuestadas y priorizadas de cara al tratamiento de los riesgos basado en un análisis de riesgos.
7. Soporte	Se cumple	Hay bastante concienciación entre los empleados. Las entrevistas así lo demuestran. Se ha formado al personal (hay proyectos que lo demuestran, facturas de libros, cursos-certificados) y la labor del Responsable de Seguridad en trasmitir y trasladar información interesante lo demuestran... Las cosas relativas al SGSI se comunican de según el procedimiento establecido (hay un procedimiento). Y la información está documentada, bastante completa y organizada
8. Operación	Se cumple	Existe la evaluación o análisis de riesgos y el tratamiento de estos.
9. Evaluación del desempeño	Se cumple	Hay establecida un procedimientos formalizado para la realización de auditorías, en ella se define cómo acometer esta tarea... Esta misma es la primera auditoría.
10. Mejora	Sin realizar todavía – No se cumple	Esta es la primera auditoría, y todavía no se han comunicado las no conformidades, por lo que no se puede determinar si cumple o no, habrá que verlo en la siguiente auditoría.

Controles de ISO 27001 del anexo A

El estado sería el siguiente, que se deriva del documento anexo-A-27001-auditoría.xls , que es la misma plantilla utilizada para el análisis diferencial del inicio.. En este documento se detalla con más información sobre cada control, basándose de las pruebas realizadas en la auditoría. Teniendo en cuenta la Declaración de Aplicabilidad, habiendo algunos controles que no se aplican, se han marcado en gris, y se han excluido sus efectos de los cálculos. Se han tomado como no conformidades aquellos controles que a los que se les ha asignado el valor "'0 – Inexistente".

Se pueden observar los valores y observaciones control a control en el anexo **auditoría-interna.xls**

A.5 Information security policies	3,5
A.6 Organization of information security	2,7
A.7 Human resource security	2,3333
A.8 Asset management	2,3333
A.9 Access control	2,9375
A.10 Cryptography	2
A.11 Physical and environmental security	2,4375
A.12 Operations security	2,2381
A.13 Communications security	2
A.14 System acquisition, development and maintenance	2,1111
A.15 Supplier relationships	1,1667
A.16 Information security incident management	2,3333
A.17 Information security aspects of business continuity management	1,5
A.18 Compliance	2,2

Imagen 5: Auditoría: Valor de controles sobre 5

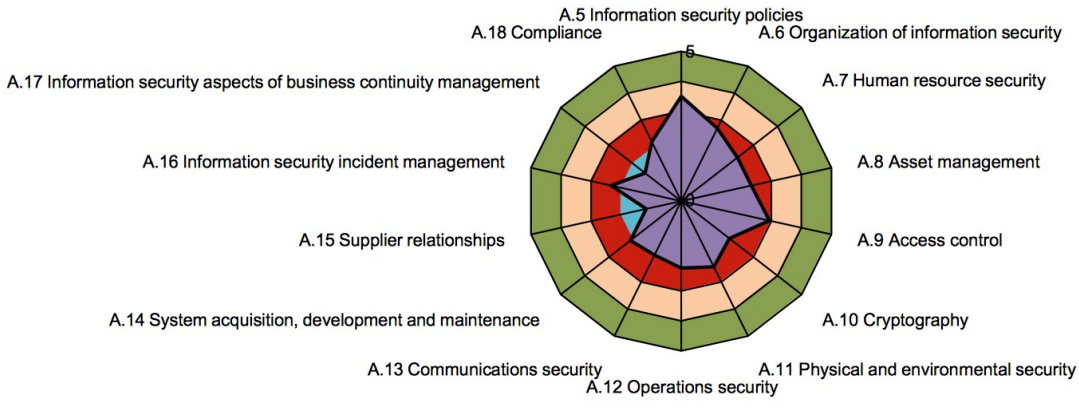

Imagen 6: Radar del estado de los controles sobre 5

8.2.4 Informe de auditoría

El informe que se elabora es un informe claro y lo más directo posible y siempre facilitando la información relevante. Al mismo tiempo, facilita de manera sencilla la forma de resolver las deficiencias halladas o por lo menos recomendar ciertas acciones o medidas correctivas.

- **Resumen ejecutivo**: Este informe contiene información sobre la auditoría interna realizada en Secure Team. El objetivo de la auditoría ha sido confirmar que la organización cumple con sus políticas y procedimientos y comprobar que el SGSI está conforme con las especificaciones de la Norma ISO/IEC 27001.

  La metodología que se ha seguido es la establecida en el procedimiento de auditorías de Secure Team. Se ha recabado información, y posteriormente se ha revisado y se ha complementado esa información tanto con los resultados de pruebas técnicas como de las entrevistas realizadas a diferentes empleados de la empresa. De forma resumida, las no conformidades que se han encontrado están relacionadas con la falta de un **plan de continuidad**, y la no existencia de algunas políticas para la definición de **contratos con proveedores**, la falta de **política sobre propiedad intelectual**, o la falta de gestión y documentación de **cambios en los servicios de red**.

- **Metodología empleada**: La metodología empleada ha sido la establecida en el procedimiento de auditorías de Secure Team. Se ha recabado información previa.Esa información a posibilitado por un lado tener información sobre políticas, procedimientos, actividad, etc. pero tambíen ha servido para poder preparar mejor las pruebas y las entrevistas. Las entrevistas se han realizado ha una parte de los empleados de la empresa. Siendo 10 en la empresa, se ha hecho un muestreo y se han elegido 4 de diferentes cargos y con eso, se ha cubierto casi un 50% de los empleados pero además con el plus aportan información complementaria o contrastable entre ellas. Por otro lado, también se han realizado pruebas técnicas que han consistido en la comprobación del estado de las redes y de las aplicaciones. Partiendo de ahí, se han completado unas tablas con los comentarios y observaciones para cada control. Una vez completadas las tablas se han detectado las no conformidades. Finalmente se ha redactado este informe que traslada las partes más relevantes de toda esa información.

- **Listado detallado de los hallazgos**: Se han completado dos tablas con información o resultados obtenidos de las entrevistas y de las pruebas. Partiendo del análisis y estudio de toda esa información, por un lado se recogen las no conformidades:

	No conformidad
A.6.1.4 Contact with special interest groups	No se está participando en foros o charlas ni hay relación con otras entidades del ámbito de la seguridad.
A.8.3.1 Management of removable media	No consta ni política ni procedimientos relacionados con la gestión de soportes extraíbles
A.13.1.2 Security of network services	No existe ningún acuerdo de servicios de red a nivel interno ni externo.
A.15.1.1 Information security policy for supplier relationships	No existe ninguna política
A.15.2.2 Managing changes to supplier services	No se están gestionando los cambios en los servicios. Tampoco existe una política como ya se ha podido saber, por lo que tampoco se puede actualizar. No hay un control documentado de los cambios.
A.17.1.1 Planning information security continuity	No existe un plan de continuidad
A.17.1.2 Implementing information security continuity	Al no tener plan no ha implementado nada.
A.17.1.3 Verify, review and evaluate information security continuity	Al no tener plan implementado no se revisa nada.
A.18.1.2 Illectual property rights	Hay una política sobre propiedad intelectual y se cuenta una asesoría jurídica para ello. Pero no hay un procedimiento establecido tal como se indica que debería de haberlo.
27001:2013 apartado 10: Mejora	No se han realizado auditorías hasta la fecha, por lo que a día de hoy no se cumple con este apartado.

Tabla 31: No conformidades de auditoría interna

9. Anexos

9.1 Imágenes y hojas de cálculo

Ciertos anexos son imágenes y hojas de cálculos que están en la capeta anexos y se han usado para la elaboración de esta memoria:

- organigrama.jpg
- diagrama_tec.jpg
- radar-analisis-diferencial.png
- GAP 27002_2013_secure_team.xls
- auditoria-interna.xls

9.2 Tablas de valores para análisis de riesgos

En este anexo se traducen las tablas de NIST que indican la escala de valores para la evaluación de riesgos, y el objetivo es poder aportar una explicación para poder interpretarlos. Solo se recogen los valores del modo cualitativo, ya que es la que se empleará. Las tablas de taxonomía y listado de amenazas y fuentes de amenazas, no se recogen aquí, ya que la propia tabla de amenazas, fuentes de amenazas, vulnerabilidades ya muestran cuáles se han usado y el texto en sí ya indica lo que son.

Valor	Descripción
Muy alto	El adversario tiene una gran capacidad técnica, dispone de altas prestaciones o recursos y pude generar oportunidades para llevar a cabo de forma continua y con éxito múltiples ataques coordinados.
Alto	El adversario tiene un gran capacidad técnica, dispone de ciertos recursos importantes y puede llevar a cabo múltiples ataques con éxito.
Moderado	El adversario dispone de una moderada capacidad técnica y recursos para poder llevar a cabo múltiples ataques con éxito.
Bajo	El adversario cuenta con oportunidades, recursos y capacidad técnica limitada para poder llevar a cabo algún ataque con éxito.
Muy bajo	El adversario apenas cuenta con recursos, capacidad técnica y oportunidades para llevar a cabo algún ataque con éxito.

Tabla 32: Capacidad de adversario (traducción de tabla D3 de NIST SP 800-30)

Valor	Descripción
Muy alto	El adversario busca socavar, impedir severamente o destruir una misión central o una función comercial, programa o empresa mediante la explotación de una presencia en los sistemas o infraestructura de información de la organización. Al adversario le preocupa la revelación de su actividad solo en la medida en que impida su capacidad para cumplir los objetivos establecidos.
Alto	El adversario busca socavar / impedir aspectos críticos de una misión central o función comercial, programa o empresa, o colocarse en una posición para hacerlo en el futuro, manteniendo una presencia en los sistemas de información o infraestructura de la organización. El adversario está muy preocupado por minimizar la detección / revelación de ataques o su actividad, particularmente mientras se prepara para ataques futuros.
Moderado	El adversario busca obtener o modificar información específica crítica o sensible o usurpar / interrumpir los recursos cibernéticos de la organización estableciendo un punto de apoyo en los sistemas de información o infraestructura de la organización. Al adversario le preocupa minimizar la detección / revelación de sus ataques o de su actividad, particularmente cuando se llevan a cabo ataques durante largos periodos de tiempo. El adversario está dispuesto a impedir que ciertos aspectos de las misiones / funciones comerciales de la organización logren sus fines.
Bajo	El adversario busca activamente obtener información crítica o sensible o usurpar / interrumpir los recursos cibernéticos de la organización, y lo hace sin preocuparse por la detección / divulgación de sus ataques o actividad.
Muy bajo	El adversario busca usurpar, alterar o desfigurar los recursos cibernéticos de la organización, y lo hace sin preocuparse por la detección / divulgación de sus ataques o actividad.

Tabla 33: Intención de adversario (traducción de tabla D4 de NIST SP 800-30)

Valor	Descripción
Muy alto	El adversario analiza la información obtenida a través de reconocimientos y ataques para apuntar persistentemente a una organización, empresa, programa, misión o función comercial específica, centrándose en información, recursos, flujos de suministro o funciones específicos de alto valor o de misión crítica; empleados o puestos específicos; proveedores / proveedores de infraestructura de apoyo; o organizaciones asociadas.
Alto	El adversario analiza la información obtenida a través del reconocimiento para apuntar persistentemente a una organización, empresa, programa, misión o función empresarial específica, centrándose en información, recursos, flujos de suministro o funciones específicos de alto valor o misión crítica, empleados específicos que respaldan esas funciones o posiciones clave.
Moderado	El adversario analiza la información disponible públicamente para dirigirse a organizaciones persistentemente específicas de alto valor (y puestos clave, como el Director de Información), programas o información.
Bajo	El adversario usa información pública para dirigirse a una clase de organizaciones o información de alto valor, y busca objetivos de oportunidad dentro de esa clase.
Muy bajo	El adversario puede o no apuntar a organizaciones o clases de organizaciones específicas.

Tabla 34: Motivación de selección de objetivo (traducción de tabla D5 de NIST SP 800-30)

Valor	Descripción
Muy alto	Los efectos del error, accidente o acto de la naturaleza son radicales, involucrando casi todos los recursos de la empresa
Alto	Los efectos del error, accidente o acto de la naturaleza son extensos, involucrando la mayoría de los recursos, e incluyen muchos recursos críticos.
Moderado	Los efectos del error, accidente o acto de la naturaleza son muy variados y abarcan una parte importante de los recursos, e incluyen algunos recursos críticos.
Bajo	Los efectos del error, accidente o acto de la naturaleza son limitados, involucrando algunos de los recursos, pero sin incluir recursos críticos.
Muy bajo	Los efectos del error, accidente o acto de la naturaleza son mínimos, implican pocos o ninguno de los recursos y no implican recursos críticos.

Tabla 35: Rango de efectos de amenazas no intencionadas (traducción de tabla D6 de NIST SP 800-30)

Valor	Descripción
Confirmado	La amenaza o TTP (tácticas, técnicas, procedimientos) ha sido visto por la organización.
Esperado	La amenaza o TTP (tácticas, técnicas, procedimientos) ha sido visto por los compañeros o colaboradores de la organización.
Anticipado	La amenaza o TTP (tácticas, técnicas, procedimientos) ha sido informado por una fuente fiable.
Pronosticado	La amenaza o TTP (tácticas, técnicas, procedimientos) ha sido pronosticado por una fuente fiable.
Posible	La amenaza o TTP (tácticas, técnicas, procedimientos) ha sido descrito por una fuente algo creíble.
N/A (No Aplicable)	La amenaza o TTP (tácticas, técnicas, procedimientos) no es actualmente aplicable. Ya que dicha amenaza implica tecnología que no existe o ya que la información de la que se dispone en base a esa amenaza y la fuente de amenaza indica que no se dan las condiciones en la organización para que ésta pueda aplicarse.

Tabla 36: Relevancia de la amenaza (traducción de tabla E4 de NIST SP 800-30)

Valor	Descripción
Muy alto	La vulnerabilidad está expuesta y explotable, y su explotación podría tener graves consecuencias. El control de seguridad relevante u otro remedio no se implementa y no se planifica; o no se puede identificar ninguna medida de seguridad para remediar la vulnerabilidad.
Alto	La vulnerabilidad es motivo de gran preocupación, en función de la exposición de la vulnerabilidad y la facilidad de explotación y / o de la gravedad de los impactos que podrían derivarse de su explotación. El control de seguridad relevante u otro remedio está planificado pero no implementado; los controles de compensación están en su lugar y al menos son mínimamente efectivos.
Moderado	La vulnerabilidad es de moderada preocupación, en función de la exposición de la vulnerabilidad y la facilidad de explotación y / o de la gravedad de los impactos que podrían derivarse de su explotación. El control de seguridad es relevante u otra remedio está implementado parcialmente y es algo efectivo.
Bajo	La vulnerabilidad es de menor importancia, pero la efectividad de la remedio podría mejorarse. El control de seguridad es relevante u otro remedio está completamente implementado y es algo efectivo.
Muy bajo	La vulnerabilidad no es motivo de preocupación. El control de seguridad relevante u otra solución se implementa, evalúa y aplica completamente.

Tabla 37: Gravedad de la vulneravilidad (traducción de tabla F2 de NIST SP 800-30)

Valor	Descripción
Muy alto	Se aplica a todas las misiones de la organización / funciones comerciales, procesos de misión / negocio o a sistemas de información
Alto	Se aplica a la mayoría de las misiones de la organización / funciones comerciales, procesos de misión / negocio o a sistemas de información
Moderado	Se aplica a la muchas o varias de las misiones de la organización / funciones comerciales, procesos de misión / negocio o a sistemas de información
Bajo	Se aplica a la algunas de las misiones de la organización / funciones comerciales, procesos de misión / negocio o a sistemas de información
Muy bajo	Se aplica a la alguna de las misiones de la organización / funciones comerciales, procesos de misión / negocio o a sistemas de información

Tabla 38: Envergadura / dimensión de la condición predispuesta (traducción de tabla F5 de NIST SP 800-30)

Valor	Descripción
Muy alto	Es casi seguro que un adversario inicie la amenaza.
Alto	Es muy probable que el adversario inicie la amenaza.
Moderado	Es probable que el adversario inicie la amenaza.
Bajo	Es poco probable que el adversario inicie la amenaza.
Muy bajo	Es muy poco probable que el adversario inicie la amenaza.

Tabla 39: Probabilidad de iniciación del ataque o amenaza intencionada (traducción de tabla G2 de NIST SP 800-30)

Valor	Descripción
Muy alto	Es casi seguro que ocurra un error, accidente o acto de la naturaleza; o ocurre más de 100 veces al año.
Alto	Es muy probable que ocurra un error, accidente o acto de la naturaleza; o se produce entre 10-100 veces al año.
Moderado	Es probable que ocurra un error, accidente o acto de la naturaleza; o se produce entre 1 y 10 veces al año.
Bajo	Es poco probable que ocurra un error, accidente o acto de la naturaleza; o ocurre menos de una vez al año, pero más de una vez cada 10 años.
Muy bajo	Es muy poco probable que ocurra un error, accidente o acto de la naturaleza; o ocurre menos de una vez cada 10 años.

Tabla 40: Tabla 12: Probabilidad de ocurrencia de amenaza no intencionada (traducción de tabla G3 de NIST SP 800-30)

Valor	Descripción
Muy alto	Si la amenaza se inicia o se produce, es casi seguro que tenga impactos adversos.
Alto	Si la amenaza se inicia o se produce, es muy probable que tenga impactos adversos.
Moderado	Si la amenaza se inicia o se produce, es probable que tenga impactos adversos.
Bajo	Si la amenaza se inicia o se produce, es poco probable que tenga impactos adversos.
Muy bajo	Si la amenaza se inicia o se produce, es muy poco probable que tenga impactos adversos.

Tabla 41: Probabilidad de que se generen impactos adversos (traducción de tabla G-4 de NIST SP 800-30)

Probabilidad de iniciación u ocurrencia de amenaza	Probabilidad de que la amenaza genere impactos adversos				
	Muy bajo	Bajo	Moderado	Alto	Muy alto
Muy alto	Bajo	Moderado	Alto	Muy alto	Muy alto
Alto	Bajo	Moderado	Moderado	Alto	Muy alto
Moderado	Bajo	Bajo	Moderado	Moderado	Alto
Bajo	Muy bajo	Bajo	Bajo	Moderado	Moderado
Muy bajo	Muy bajo	Muy bajo	Bajo	Bajo	Bajo

Tabla 42: Tabla para sacar la probabilidad media cruzando las tablas de ocurrencia/iniciación y de impactos adversos. Es decir G2/G3 y G4

Valor	Descripción
Muy alto	Se puede esperar que la amenaza tenga **múltiples efectos adversos graves o catastróficos** en las operaciones de la organización, los activos de la organización, los individuos, otras organizaciones o la Nación.
Alto	Se podría esperar que la amenaza tenga **algún efecto adverso grave o catastrófico** en las operaciones de la organización, los activos de la organización, los individuos, otras organizaciones o la Nación. Un efecto adverso severo o catastrófico significa que, por ejemplo, el evento de amenaza podría: (i) causar una degradación severa o pérdida de la capacidad de la misión en un grado y duración tal que la organización no pueda realizar una o más de sus funciones principales ; (ii) provocar daños importantes a los activos de la organización; (iii) resultar en una gran pérdida financiera; o (iv) ocasione daños graves o catastróficos a las personas que involucren la pérdida de la vida o lesiones graves que pongan en peligro la vida.
Moderado	Se puede esperar que la amenaza tenga **algún efecto adverso grave** en las operaciones de la organización, los activos de la organización, las personas, otras organizaciones o la Nación. Un efecto adverso grave significa que, por ejemplo, el evento de amenaza podría: (i) causar una degradación significativa en la capacidad de la misión en un grado y duración tal que la organización pueda realizar sus funciones principales, pero la efectividad de las funciones se reduzca significativamente ; (ii) resultar en un daño significativo a los activos de la organización; (iii) resultar en una pérdida financiera significativa; o (iv) ocasionar daños significativos a las personas que no impliquen pérdida de vidas o lesiones graves que pongan en peligro la vida.
Bajo	Se puede esperar que la amenaza tenga **algún efecto adverso limitado** en las operaciones de la organización, los activos de la organización, las personas, otras organizaciones o la Nación. Un efecto adverso limitado significa que, por ejemplo, el evento de amenaza podría: (i) causar una degradación en la capacidad de la misión en un grado y duración tal que la organización pueda realizar sus funciones primarias, pero la efectividad de las funciones se reduce notablemente; (ii) resultar en daños menores a los activos de la organización; (iii) resultar en una pérdida financiera menor; o (iv) causar daños menores a las personas.
Muy bajo	Se puede esperar que la amenaza tenga **algún efecto adverso insignificante** en las operaciones de la organización, los activos de la organización, las personas, otras organizaciones o la Nación.

Tabla 43: Impacto de la amenaza (traducción de tabla H-3 de NIST SP 800-30)

Probabilidad media de la amenaza	Nivel de impacto				
	Muy bajo	Bajo	Moderado	Alto	Muy alto
Muy alto	Muy bajo	Bajo	Moderado	Alto	Muy alto
Alto	Muy bajo	Bajo	Moderado	Alto	Muy alto
Moderado	Muy bajo	Bajo	Moderado	Moderado	Alto
Bajo	Muy bajo	Bajo	Bajo	Bajo	Moderado
Muy bajo	Muy bajo	Muy bajo	Muy bajo	Bajo	Bajo

Tabla 44: Valoración del riesgo

9.3 Actas

También hay **actas** de reuniones que se han mantenido con la dirección de Secure Team:

Documento	Descripción
R-2017-09-27.pdf	Exponer y acordar el calendario y metodología para la elaboración del Plan
R-2017-09-29.pdf	Información de organigrama, visión, misión, definir alcance
R-2017-10-04.pdf	Información sobre el estado de los controles para obtener análisis diferencial
R-2017-10-18.pdf	Lineas generales de política de seguridad, periodicidad de auditorías y composición de Comité de Seguridad

Tabla 45: Actas

Bibliografía

[ISO/IEC 27001:2013]: estándar, ISO 27001, 2013

[ISO/IEC 27002:2013]: estándar, ISO 27002, 2013

[Incibe, Plan Director de Seguridad]: artículo web, Plan Director de Seguridad ,2016, https://www.incibe.es/protege-tu-empresa/que-te-interesa/plan-director-seguridad

[Incibe, Plan Director de Seguridad - Un caso práctico]: artículo web, Plan Director de Seguridad: ¿Dónde estamos? ¿A dónde queremos llegar? Un caso práctico ,2016, https://www.incibe.es/protege-tu-empresa/blog/plan-director-deguridad-donde-estamos-donde-queremos-llegar-un-caso-practico

[Estevan de Quesada,2017]: Libro, Rafael Estevan de Quesada, Auditoría técnica y de certificación, 2017

[NIST, 2012]: documento técnico en web, Guide for Conducting Risk Assessments ,2012, http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf

[Cruz, 2007]: Libro, Daniel Cruz Allende, Análisis de riesgos, 2007

[Symantec, 2016]: informe, Internet Security Threat Report ,2016, https://www.symantec.com/content/dam/symantec/docs/reports/istr-21-2016-en.pdf

[Symantec, 2016 (gov)]: informe, Internet Security Threat Report - Goverment ,2016, https://www.symantec.com/content/dam/symantec/docs/reports/gistr22-government-report.pdf

[Mitnick, 2002]: Libro, K. Mitnick, The Art of Deception, 2002

[Hadnagy, 2010]: Libro, C. Hadnagy, Social engineering: The Art of Human Hacking, 2010

[ENISA,2016]: informe, Threat Lanscape Report ,2017, https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2016

[Deia, 2016]:artículo web, Deia, La delincuencia descendió en Euskadi un 3,17% durante el año 2016, 2017