Desarrollo de una guía de controles ciberseguridad para la protección integral de la pyme

Carlos José López Fernández

Máster Universitario en Seguridad de las Tecnologías de la Información y de las Comunicaciones
Seguridad Empresarial

Consultor: Jorge Chinea López
Profesor responsable de la asignatura: Víctor García Font

Fecha Entrega: 06/2019

FICHA DEL TRABAJO FINAL

Título del trabajo:	*Desarrollo de una guía de controles ciberseguridad para la protección integral de la pyme*
Nombre del autor:	*Carlos José López Fernández*
Nombre del consultor/a:	*Jorge Chinea López*
Nombre del PRA:	*Víctor García Font*
Fecha de entrega:	06/2019
Titulación:	*Máster Universitario en Seguridad de las Tecnologías de la Información y de las Comunicaciones*
Área del Trabajo Final:	*Seguridad Empresarial*
Idioma del trabajo:	*Español*
Palabras clave	*Ciberseguridad, ISO27002*

Resumen:

Que la tecnología ha cambiado el mundo es algo evidente, tanto en las relaciones personales como en las profesionales, centrándonos en estas últimas, en los últimos años se observa un continuo acercamiento de las pymes al ciberespacio como consecuencia de su continua adaptación y transformación digital, que les ayude a simplificar y agilizar sus procesos empresariales, para dar respuesta a los nuevos hábitos de consumo.

Como consecuencia de esta transformación vertiginosa, las pymes aumentan exponencialmente su índice de exposición tanto a internet como a nuevos y numerosos riesgos que no siempre son analizados ni contemplados.

El objetivo de este trabajo es dar a conocer algunas de las amenazas existentes en el ciberespacio, y crear una guía basada en la norma ISO/IEC 27002 que ayude a las pymes a identificar las tareas necesarias para implementar medidas de seguridad que permitan mitigar dichos riesgos.

Abstract:

That technology has changed the world is evident, both in personal and professional relationships, focusing on the latter, in recent years there is a continuous approach of SMEs to cyberspace as a result of its continuous adaptation and digital transformation, that helps them simplify and streamline their business processes, to respond to new consumption habits.

As a consequence of this vertiginous transformation, SMEs exponentially increase their exposure index both to the Internet and to new and numerous risks that are not always analysed or contemplated, as a result of the lack of resources or the lack of adequate training on information security.

The objective of this paper is to present some of the existing threats in cyberspace, and to create a guide based on the ISO / IEC 27002 standard that helps SMEs identify the tasks necessary to implement security measures to mitigate those risks.

Índice

1. Introducción 1
2. Estado del Arte 5
2.1. Ciberamenazas actuales 7
2.2. Riesgos 12
2.3. El estado de las pymes en materia de seguridad 13
2.4. Familia ISO 27000 15
2.5. Implementación ISO 27000 19
3. Guía de ciberseguridad 20
3.1. Análisis de riesgos 22
3.1.1. Activo: 22
3.1.2. Amenaza: 22
3.1.3. Vulnerabilidad: 23
3.1.4. Impacto: 23
3.1.5. Metodología 24
3.2. Controles de ciberseguridad 28
3.2.1. Políticas de seguridad de la información 33
3.2.2. Organización de la seguridad de la información 34
3.2.3. Seguridad relativa a los recursos humanos 35
3.2.4. Gestión de activos 36
3.2.5. Control de acceso 38
3.2.6. Criptografía 39
3.2.7. Seguridad física y del entorno 40
3.2.8. Seguridad de las operaciones 42
3.2.9. Seguridad de las comunicaciones 45
3.2.10. Adquisición, desarrollo y mantenimiento de los sistemas de información 47
3.2.11. Relación con proveedores 49
3.2.12. Gestión de incidentes de seguridad de la información 51
3.2.13. Aspectos de seguridad de la información para la gestión de la continuidad del negocio 53
3.2.14. Cumplimiento 54
4. Conclusiones 57
5. Glosario 60
6. Bibliografía 62
7. Anexos 64
7.1. Planificación 64
7.2. Lista de controles ISO/IEC 27002:2013 65
7.3. Correspondencia entre la normas ISO/IEC 27002:2013 y ISO/IEC 27032:2012 69

Lista de figuras

Ilustración 1: Foco objetivo de ciberdelincuentes (2) 1
Ilustración 2: Planificación proyecto 3
Ilustración 3: Volumen de empresas por tamaño 5
Ilustración 4: Cantidad de Malware 8
Ilustración 5: Distribución del malware 10
Ilustración 6: Amenazas futuras y tendencias en crímenes online (12) 11
Ilustración 8: Impactos de ciberataques en empresas (14) 13
Ilustración 9: Familia de normas ISO 27000 (15) 15
Ilustración 10: Proceso de gestión de incidentes (18) 51

Lista de tablas

Tabla 1: Planificación proyecto 4
Tabla 2: ISO 27000: Estándares vocabulario 15
Tabla 3: ISO 27000: Estándares de requisitos 16
Tabla 4: ISO 27000: Estándares directrices 16
Tabla 5: ISO 27000: Estándares directrices de sector 17
Tabla 6: ISO 27000: Estándares directrices de control 18
Tabla 7: Controles ISO/IEC 27002:2013 aplicables por PCI-DSS 32

1. Introducción

Cada día es más habitual encontrarnos en los medios de comunicación referencias a ciberataques y si bien pudiera parecer, en cierta medida gracias al a industria de Hollywood, que el objetivo de estos ataques son grandes empresas o grandes infraestructuras (que también), la realidad es que el objetivo más buscado es la pequeña y mediana empresa, según el informe anual realizado por Verizon, en torno al 60% de las víctimas de un ciberataque son pequeñas empresas (1), dado que las medidas de seguridad implementadas por estas son nulas o bien fácilmente sorteables. Según Stephen Cobb (Investigador principal de seguridad en ESET) las pequeñas empresas son el objetivo principal de los piratas informáticos, ya que se encuentran en el punto justo (sweet spot) entre el botín obtenido, ya que tienen más recursos informáticos que un individuo, y la dificultad necesaria para vulnerar su seguridad, ya que tienen menos seguridad que una empresa grande. (2)

Ilustración 1: Foco objetivo de ciberdelincuentes (2)

En España el Instituto Nacional de Ciberseguridad detecto en 2017 más de 123.000 ataques dirigidos a empresas (3), para entender por qué se producen tantos ataques deberíamos comprender dos conceptos: vulnerabilidad y amenaza.

Una vulnerabilidad es una debilidad o fallo en un sistema de información, y una amenaza es una acción capaz de aprovechar dicha vulnerabilidad y atentar contra la seguridad de la información.

Si tenemos en cuenta el elevado número de vulnerabilidades detectadas anualmente (en 2018 han sido 16.500) y si a este hecho le sumamos la aparición diaria de más y más ficheros de malware distinto (número que no para de crecer, en 2015 hablábamos de 230.000 al día y en el año 2017 se contabilizaban ya los 285.000 diarios), parece necesario establecer medidas que no nos dejen indefensos ante estos números.

Si bien las grandes compañías pueden permitirse altas partidas presupuestarias en materia de seguridad, la realidad española indica que las pymes en general no pueden permitirse un alto presupuesto en seguridad, a pesar de estar sometidas a las mismas ciberamenazas y vulnerabilidades que las grandes, y que como ya he indicado antes, los propios ciberdelicuentes son conscientes de que puede existir esa ausencia de seguridad en multitud de pymes y en consecuencia poder materializar un ataque con altas posibilidades de éxito con un mínimo esfuerzo.

Ante este panorama tan desalentador, y como consecuencia de esta amenaza constante, surge la necesidad de crear una guía que ayude a pequeñas y medianas empresas (PYMES) a obtener el conocimiento suficiente que les permita defenderse ante estas amenazas y proteger su información.

Este trabajo pretende cubrir dicha necesidad por parte de las pymes de contar con medidas de ciberseguridad que permitan gestionar de manera efectiva las ciberamenzas a las que se enfrentan garantizando la continuidad del negocio. Para ello se define como objetivo principal el poder presentar una guía a las pymes que les permita establecer controles de protección frente a ciberamenazas.

Para lograr este objetivo, se establecen una serie de objetivos secundarios, a saber:

- Generar conciencia general sobre la seguridad de la información
- Generar conciencia específica sobre las ciberamenazas.
- Promover el uso de la familia de normas en seguridad de la información ISO 27000, como base para el establecimiento de medidas de ciberseguridad.

El enfoque seguido para el desarrollo del trabajo comienza con un análisis inicial de las ciberamenazas/ciberdelitos actuales, presentando informes estadísticos al respecto, que permitan concienciar al lector de la importancia de la seguridad de la información y de la necesidad de aplicar medidas sobre las PYMES que las protejan frente a las ciberamenazas.

Una vez concienciado al lector, se realizará una explicación de la familia de normas ISO 27000 y de cómo esta puede ayudar a la empresa mediante la aplicación de una serie de medidas basadas en los controles de la norma ISO/IEC 27002:2013 y ISO/IEC 27032:2012 que le permita proteger su información.

Para el desarrollo del trabajo, se han definido los siguientes elementos:

- Análisis del estado actual.
- Redacción del capítulo de Estado del Arte.
- Planificación inicial.
- Establecimiento de Objetivos.
- Redacción de la introducción al trabajo, indicando la relevancia del tema a tratar y las necesidades a cubrir.
- Redacción del estado del arte, reflejando la situación actual en materia de ciberseguridad.
- Establecimiento del marco normativo que aplicaremos.
- Entrega de un primer borrador de la memoria donde se haya iniciado el contenido de la guía y que permita evaluar su eficacia y lo acertado de la metodología seguida.
- Entrega Memoria Final, que incluirá adicionalmente las conclusiones obtenidas durante la realización del trabajo y posibles líneas de trabajo futuro que puedan complementar el trabajo actual.
- Entrega de un vídeo explicativo que incluye la síntesis del trabajo.

Dichos elementos han sido planificados según Ilustración 2 que representa el diagrama de GANTT y que podemos ver en detalle en la Tabla 1:

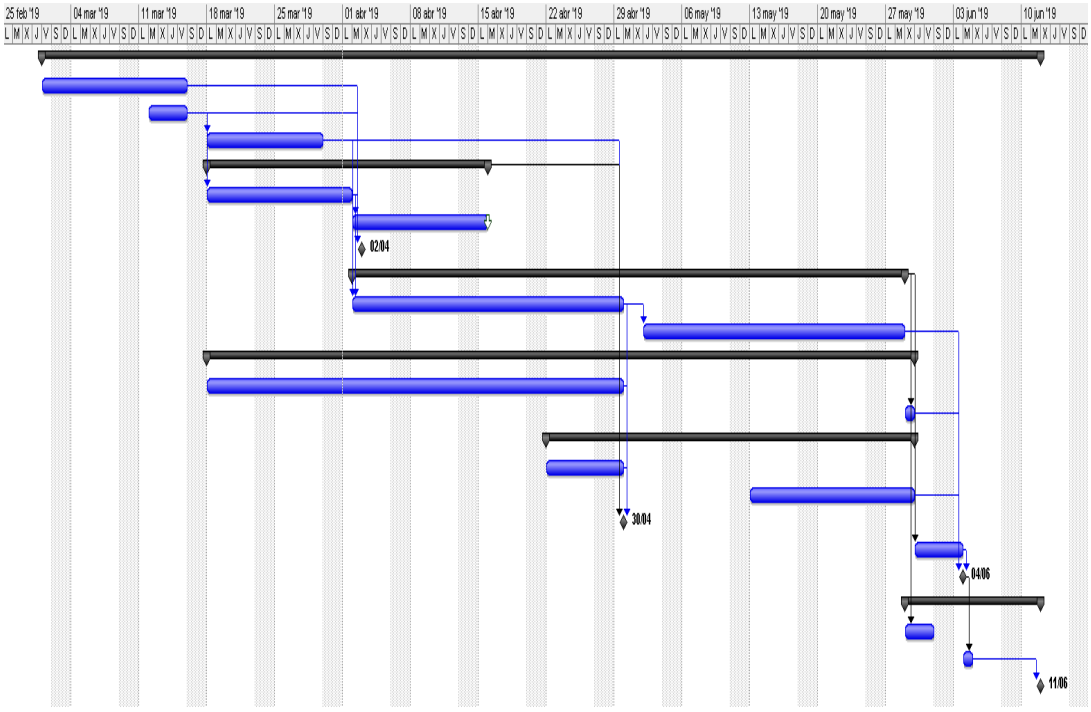


Ilustración 2: Planificación proyecto

Tarea	Duración	Comienzo	Fin	Predecesoras
Guía de controles de Seguridad	73 días	01/03/2019	11/06/2019	
Planificación inicial	11 días	01/03/2019	15/03/2019	
Definición de objetivos	4 días	12/03/2019	15/03/2019	
Introducción	10 días	18/03/2019	29/03/2019	3
Estado del arte	21 días	18/03/2019	15/04/2019	
Borrador	11 días	18/03/2019	01/04/2019	3
Versión Definitiva	10 días	02/04/2019	15/04/2019	6
Entrega inicial	0 días	02/04/2019	02/04/2019	2;3;4;6
Guía	41 días	02/04/2019	28/05/2019	
Borrador	20 días	02/04/2019	29/04/2019	4;6
Versión Definitiva	19 días	02/05/2019	28/05/2019	10
Glosario	53 días	18/03/2019	29/05/2019	
Borrador	31 días	18/03/2019	29/04/2019	
Versión Definitiva	1 día	29/05/2019	29/05/2019	9
Anexos	28 días	22/04/2019	29/05/2019	
Borrador	6 días	22/04/2019	29/04/2019	
Versión Definitiva	13 días	13/05/2019	29/05/2019	
Entrega Borrador	0 días	30/04/2019	30/04/2019	4;5;10;13;16
Conclusiones	3 días	30/05/2019	03/06/2019	9
Entrega final	0 días	04/06/2019	04/06/2019	11;14;17;19
Video explicativo	10 días	29/05/2019	11/06/2019	
Índice	3 días	29/05/2019	31/05/2019	9
Realización	1 día	04/06/2019	04/06/2019	20
Entrega	1 día	11/06/2019	11/06/2019	23

Tabla 1: Planificación proyecto

El entregable principal de este trabajo, y que vendrá desarrollado en el capítulo 3, es una guía que pretende orientar y ayudar a las pymes a establecer controles de seguridad que puedan disuadir a un atacante novel de iniciar un ataque y poner buenas barreras frente a ataques profesionales.

Adicionalmente el trabajo cuenta con un análisis preliminar del estado del arte recogido en el capítulo 2, donde se repasan las amenazas actuales, el estado en materia de seguridad de las pymes y una introducción a la familia de normas ISO 27000 y que servirán de fundamento para la elaboración de la guía, entendiéndolas no solo como un medio de defensa frente a amenazas sino también como ayuda frente al cumplimiento legal (LOPD. RGPD. LPI. LSSI, …), así como facilitar la continuidad del negocio ante un incidente, mejorando por ende la imagen de la empresa ante clientes y proveedores.

En el capítulo 4 se expondrán las conclusiones obtenidas durante la elaboración de este trabajo la realización del trabajo y posibles líneas de trabajo futuro que puedan complementar el trabajo actual.

2. Estado del Arte

Dado que la gran mayoría de las empresas quedan dentro del ámbito de las Pymes, tal y como demuestran los datos de enero de 2018 del Ministerio de Empleo y Seguridad Social (MEySS) es una necesidad el que estas cuenten con medios y ayudas para implementar medidas de ciberseguridad.

Empresas por tamaño	Número de empresas
Autónomos[1] (PYME sin asalariados)	**1.535.472**
PYME (1-249 asalariados)	**1.307.776**
Microempresas (1-9 asalariados)	1.135.054
Pequeñas (10-49 asalariados)	149.320
Medianas (50-249 asalariados)	23.402
Grandes (250 o más asalariados)	4.487
Total empresas	**2.847.735**

Ilustración 3: Volumen de empresas por tamaño

La mayoría de las Pymes mantienen una política reactiva frente las ciberamenazas, es decir una vez sufren un ataque, deciden aplicar medidas para evitar que vuelva a suceder, y en muchas ocasiones limitando las medidas al ataque especifico sufrido y no haciendo un barrido por las distintas amenazas existentes en el ciberespacio y que puedan suponer un riesgo para la misma. El principal problema de este enfoque es que, hoy en día, hay una posibilidad notable de que con un solo ataque un ciberdelincuente pueda conseguir que una empresa tenga que cesar en sus actividades, bien por dejarla inoperativa, bien por impacto económico o bien y para mí el más relevante por pérdida de imagen.

El motivo de decidir seguir esa política suele venir derivado de una falsa sensación de seguridad, por ejemplo al pensar que:

- Mis datos no le interesan a nadie
- Todos mis empleados son de fiar.
- Nunca entro a sitios raros de Internet.
- …

Estas falsas suposiciones suelen ser consecuencia de:

- Desconocimiento de seguridad de la información
- Desconocimiento de la capacidad y el objetivo de los ciberdelincuentes
- Exceso de confianza en el ser humano en general.

Comenzaré por este último punto, la confianza excesiva en el ser humano, si bien no habría por qué dudar de las personas de mayor confianza dentro de la organización, estas no están exentas del “error humano”, que según el Informe de Hiscox (una de las principales aseguradoras especializadas

de Europa y EEUU) sobre siniestralidad en el entorno digital, es el origen de la mayoría de los ciberdelitos, según este informe, “Más de dos tercios (un 67%) de todos los siniestros entrañan un factor de negligencia por parte de un empleado.” (4), aunque parezca un número elevado, este dato también es presentado por IBM en su informe IBM X-Force Threat Intelligence Index, de 2018, donde indica que en las dos terceras partes de los incidentes registrados en 2017 tenían como origen a empleados, ya fuera por fallos de configuración, o víctimas de ataques(por ejemplo phising). Con estos datos queda probada la importancia del factor humano y la necesidad de concienciar a los empleados y establecer políticas de mínimo acceso.

Si analizamos la capacidad de los ciberdelincuentes, no solo debemos pensar en un ser solitario trabajando en un sótano, realmente debemos entender que son grandes organizaciones con hackers altamente cualificados que cuentan con medios económicos cuantiosos, y en base a esta idea replantear la necesidad de establecer medidas de seguridad, recordando, como ya he mencionado que las pymes son su claro objetivo, tal y como demuestran múltiples informes como por ejemplo el Cisco SMB security, que indica que, de algo más de 3600 pymes encuestadas de 26 países distintos, el 53% había sufrido al menos un ataque en 2017. (5)

Si bien estamos en la era del dato, en la que todo dato tiene un valor, cuando pensamos en ciberdelincuentes, su objetivo no es el dato sino el valor del dato, y ese valor lo marca o bien el mercado, o bien el que contrata los servicios a ciberdelincuentes, o bien el propietario de los mismos, ya sea para que no se hagan públicos o para poder garantizar la continuidad de su negocio.

Por ultimo si pensamos en la seguridad de la información, y nos hacemos como pyme la pregunta: ¿Por qué van a querer atacar mí empresa?, si no soy una gran empresa, la respuesta muchas veces es: porque es muy fácil, al no contar con medidas de seguridad apropiadas.

Es bien sabido que la mayor parte de los hackers reconocidos inician sus conferencias con frases del estilo “la seguridad en Internet no existe nunca al 100%” (Deepack Daswani), o “La seguridad 100% no existe, …” (Chema Alonso en la primera Jornada de Ciberseguridad en Siero), y siguiendo con frases célebres en el sector, es curioso ver como algunas han ido alterándose en los últimos años reflejando la realidad en el mundo de la ciberseguridad, por ejemplo en 2012 el director del FBI, Robert Mueller durante un discurso en el RSA Cyber Security Conference, apuntaba: “there are only two types of companies: those that have been hacked and those that will be” (6), es decir “solo hay dos tipos de empresas, las que han sido atacadas y las que lo serán”, si buscamos frases similares en estos días, la más escuchada se le atribuye a John Chambers, CEO de Cisco en 2015, que en una publicación en el World Economic Forum, exponía: “There are two types of companies: those who have been hacked, and those who don’t yet know they have been hacked”

es decir " hay dos tipos de empresas, las que han sido hackeadas y las que no saben que han sido hackeadas" (7), reflejando el claro aumento del cibercrimen en el mundo.

Siguiendo con frases más actuales: "No existe una empresa 100% segura frente a la ciberdelincuencia y quien afirme eso, está engañando", afirmado por Chema Alonso en la conferencia "El arte y la ciencia en la seguridad informática de la empresa" durante el ESET Security Day de Octubre de 2018 (8).

Si bien al escuchar frases como estas, da la sensación que la batalla está perdida, la realidad es que no es así, es decir no se debe hablar en términos absolutos sino de niveles razonables de seguridad, es decir si no ponemos ninguna medida de seguridad en nuestros sistemas, un niño desde sus casa podría robarnos los datos del servidor, no obstante por cada control o medida adicional que implementemos en nuestros sistemas iremos elevando la dificultad para que un atacante pueda tener éxito, la clave es encontrar el equilibrio entre seguridad razonable y coste de la inversión, por ejemplo no tiene sentido para una empresa que tiene unos beneficios de miles de euros invertir millones en seguridad ya que esto consumiría la empresa. La mejor manera de conocer cuál es la inversión adecuada para un sistema concreto es la realización de un análisis de riesgos que nos permita detectar los activos críticos de la organización y los riesgos a los que se encuentran sometidos, de tal manera que todas las medidas a aplicar vayan enfocadas a mitigar dichos riesgos y proteger los activos en base a su criticidad para la empresa.

La idea de este trabajo no es conseguir la seguridad total, ya que como ha quedado claro, la seguridad al 100% no existe, no obstante, sí que he definido como objetivos, el concienciar al lector de la importancia de la misma y darle a conocer las tareas asociadas a controles que puedan ayudarle a conseguir un nivel aceptable de seguridad. Pero antes analicemos las capacidades de los ciberdelincuentes.

2.1. Ciberamenazas actuales

Dada la gran proliferación de las nuevas tecnologías y la hiperconectividad, hoy en día la sociedad en general y las empresas en particular están más expuestas al ciberespacio y en consecuencia se ven sometidas a continuos ciberataques, buscando diferentes objetivos, ya sean estos económicos, políticos o sociales.

Como ya he adelantado antes el principal objetivo de los ciberdelincuentes es económico y para ello se basan en localizar víctimas, bien buscando objetivos específicos o bien de manera indiscriminada, dependiendo del vector de ataque.

Según el informe de ciberamenazas de ENISA de 2018 (9), las principales ciberamenazas del año anterior fueron:

- **Malware**: aplicaciones específicamente desarrolladas para dañar de alguna manera un equipo, ya sea este un pc o un servidor. Entre sus consecuencias encontramos:
  - Perdida de rendimiento en el equipo
  - Bloqueo del equipo
  - Registrar las pulsaciones del teclado (keylogger), pudiendo llegar a enviarlas a un tercero.
  - Convertir al equipo en un bot, que formando parte de una botnet puede realizar acciones sobre otros equipos.
  - Modificar o borrar datos o incluso llegar a cifrarlos para solicitar a posteriori un rescate para recuperarlos (Ransomware).
  - Instala una puerta trasera al equipo (backdoor) para que un tercero pueda acceder, o instalar otras aplicaciones.

  Hoy en día todos conocemos casos de diferentes malware que han sido descubiertos y el impacto que han tenido sobre las empresas afectadas: discontinuidad del servicio, pérdida de imagen, perdida de contratos,…, pero es importante conocer el volumen de malware registrado y como este crece cada año, tal y como muestra la figura Ilustración 4 (10).

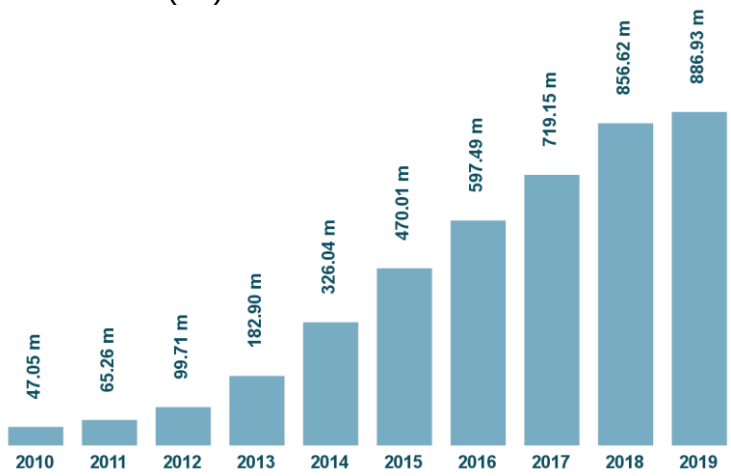


Ilustración 4: Cantidad de Malware

- **Ataques vía web**: Son ataques realizados sobre sistemas que permiten navegar por Internet, como por ejemplo navegadores o que alojan sitios web, como por ejemplo servidores web, y que aprovechan las vulnerabilidades de estos para realizar distintos tipos de ataques, como por ejemplo la suplantación de los mismos, o la inclusión de código malicioso.
- Ataques a aplicaciones web: son ataques dirigidos contra aplicaciones o servicios web, o contra aplicaciones móviles.

- Phishing: Este tipo de ataques se han ido incrementado tanto en volumen como en sofisticaciones y se basa en atraer a los usuarios a sitios maliciosos para una vez allí robar información confidencial (tradicionalmente datos bancarios o claves de acceso a otros sistemas).
- Ataques de Denegación de Servicio (DoS): Este tipo de ataque consumir todos los recursos de un sistema para hacerlos inaccesibles para sus usuarios legítimos. Entre estos ataques cabe destacar los ataques distribuidos (DDoS) ya que implican muchos más recursos para realizar el ataque y aumentan sus posibilidades de ser exitosos.
- **SPAM**: El uso de correo no deseado es un vector de ataque muy empleado para la distribución de malware (incluidos como adjuntos) o direcciones maliciosas.
- **Botnets**: Los ataques mediante botnets tienen principalmente como objetivo inutilizar servicios prestados por sistemas, como por ejemplo servicios DNS, servicios de correo, páginas web,…
- Violación de datos: Si bien no son un tipo de ataque especifico, engloba aquellos ataques que tienen como objetivo divulgar de forma ilegal datos de usuario.
- Amenazas internas: Se entienden por amenazas internas, aquellas en las que personal autorizado, ya sea consciente o inconscientemente, provoca daños sobre la información de la organización
- Ataques físicos: Si bien no usan internet en el inicio del ataque, suelen tener una segunda fase en la que sí es usado. Se incluyen dentro de esta categoría, el robo, pérdida o destrucción de activos, la manipulación de sistemas, …
- Fugas de información: Dichas fugas pueden producirse por vulnerar la falta de configuración de componentes, por errores de programación o por comportamiento indebido de un usuario.
- Robo o suplantación de identidad: Con este tipo de ataques, el atacante intenta obtener la información confidencial, que le permitirá identificarse como un usuario o como una máquina para realizar otras actividades ilícitas.
- Cryptojacking: También conocido como cripto minería (cryptominery), si bien es un ataque que no atenta contra la información, sí que atenta contra los recursos de los equipos infectados. El atacante consigue utilizar los recursos de los equipos infectados para minar criptomonedas sin el consentimiento de la víctima, y redirigiendo los posibles beneficios para sí.
- Ransomware: A pesar de ser un tipo de malware, se ha ganado una categoría propia debido al alto volumen de ataques registrados, en 2017 se estimaba que el 60% del malware era ransomware (11). El funcionamiento de un ransomware se basa en cifrar los datos del equipo infectado y solicitar un rescate por la recuperación de los mismos.

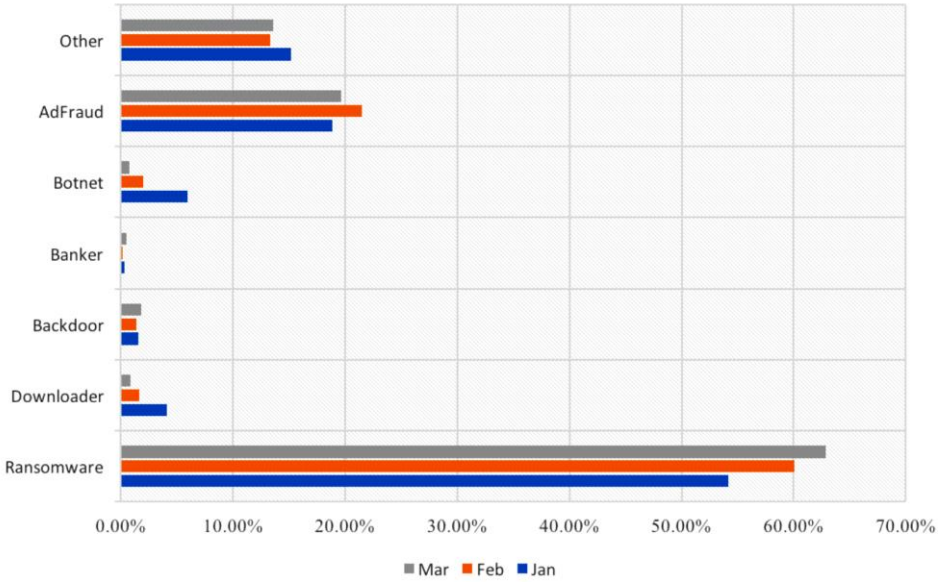


Ilustración 5: Distribución del malware

- Ciberespionaje: Si bien suele aparecer en los medios estos tipos de ataques a nivel de naciones (como por ejemplo las acciones realizadas sobre las últimas elecciones norteamericanas), también se producen entre empresas competidoras.

Si analizamos otros informes de empresas u organizaciones referente en el sector observamos que las conclusiones son muy similares, por ejemplo, si analizamos las predicciones para la ciberseguridad en 2018 realizadas por las distintas empresas referentes en el sector, por ejemplo, S21 sec, concuerdan bastante ya que entre las amenazas más destacadas se mencionan:

- distintas vías de ransomware: Mencionando nombres propios como Wannacry y Petya,
- bonets generadas vía IoT, como, por ejemplo: satori.
- Phising dirigido a personas de alto perfil (spear phising), esta modalidad de phising tiene un alto componente de ingeniería social.

De igual manera, si analizamos el IOCTA 2018 (Internet Organised Crime Threat Assessment), publicado por Europol, vemos como destaca al Ransomware frente al resto de amenazas, pero sin dejar de lado al resto de amenazas principales como los ataques DDoS, los ataques de Cryptojacking, y el empleo de ingeniería social como fase inicial en muchos ciberdelitos.

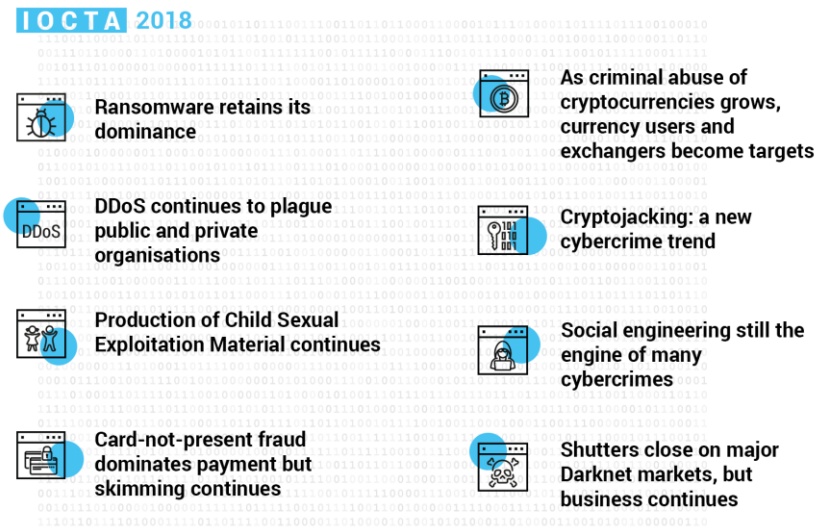


Ilustración 6: Amenazas futuras y tendencias en crímenes online (12)

Llegados a este punto hay que analizar dos hechos relevantes, el primero es que a pesar de que el listado es suficientemente largo la realidad es que no son las únicas y cada año aparecen nuevas o variantes de estas, y el segundo es que, si bien pudieran parecer amenazas independientes, la realidad es que normalmente estas amenazas van de la mano, por ejemplo, mediante un correo SPAM, nos podría entrar un malware en el equipo convirtiendo nuestro equipo en un bot que junto con el resto de la botnet se dedicara a enviar ataques de denegación de servicio a otros sistemas. Con esto quiero decir que la seguridad no se consigue aplicando un único control o medida, sino mediante una identificación de los activos críticos y una implementación de medidas tanto técnicas como organizativas que se complementen entre sí para abordar y mitigar los riesgos a los que se encuentra sometida una organización, mediante la realización de un análisis de riesgos en la organización. Pero antes es necesario conocer a que riesgos se enfrenta una organización.

2.2. Riesgos

Los principales riesgos a los que una pyme se enfrenta son:

- Robo de información
- Donde deberíamos hacer una especial atención al robo de datos personales.
- Fraude económico:
- Es evidente que la motivación económica es una de las más extendidas entre las redes de cibercriminales, entre las múltiples formas de intentar conseguir este objetivo se encuentran:
    - Fraude mediante el robo de datos de tarjetas de crédito, para ello existen diversas técnicas, como hackear sitios donde exista una pasarela de pago, o redirecciones a sitios web falsos que emulan el original, como por ejemplo mediante técnicas de pharming, o algo tan sencillo como solicitar los datos de la tarjeta mediante anuncios o correos falsos (phishing).
    - Fraudes mediante la venta de productos a un precio muy inferior al de mercado, o emulando organizaciones de caridad garantizando desgravaciones en impuesto (SCAM).
    - Muy ligado al robo de información, mediante el uso de spyware o malware, sustraen datos de tarjetas, accesos bancarios, …
    - Fraudes solicitando un Rescate de información que, si bien no ha sido robada, si ha sido inutilizada mediante el uso de criptografía (Ransomware).
- Indisponibilidad de los servicios: La interrupción de los servicios prestados online mediante por ejemplo ataques de denegación de servicio (DoS o DDoS) que impedirían a los clientes acceder a los servicios prestados.
- Perdida de reputación: Personalmente creo que es el riesgo más difícil de cuantificar ya que no conocemos de antemano exactamente el impacto y alcance del mismo.

2.3. El estado de las pymes en materia de seguridad

Si tenemos en cuenta que durante el año 2018 se han reportado más de 16.500 vulnerabilidades (13), y debido a la tendencia generalizada de transformación digital que han acometido multitud de empresas que aumenta sensiblemente su exposición, es fácilmente entendible que si nuestros sistemas de información no están debidamente actualizados o protegidos, que no muchas pymes no cuentan con medidas técnicas u organizativas en materia de seguridad de la información, y si a esto le sumamos la falta de concienciación en materia de seguridad de la información en las pymes, la posibilidad de que un ataque tenga éxito es extremadamente alto.

Ya ha quedado claro que el objetivo principal para los ciberdelincuentes son las pymes, dado que estas no suelen contar con los recursos y conocimientos necesarios para protegerse, pero analicemos el impacto de dichos ataques sobre las pymes, según datos de la Encuesta Mundial de Seguridad de la Información 2018, elaborada por PwC, en la que se encuesto a 9500 directivos y responsables de TI de 122 países (14) , tal y como muestra la Ilustración 7, personalmente me parecen muy relevantes los siguientes datos:

- El 40% de las empresas que sufrieron un ataque tuvieron que realizar una parada de sus sistemas de al menos 8 horas
- El 39% sufrió un ataque de tal magnitud que llego a afectar a la mitad de sus sistemas.
- Entre un 20 y un 30% puede llegar a dañar tanto propiedades como a personas.

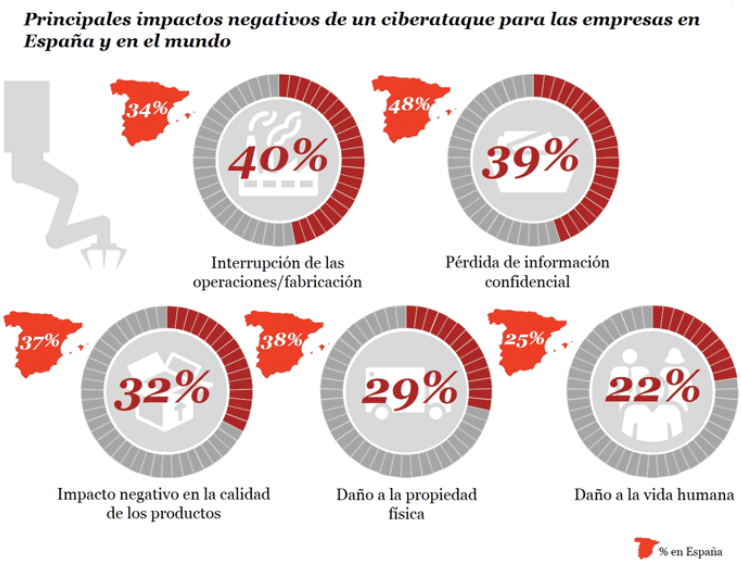


Ilustración 7: Impactos de ciberataques en empresas (14)

Visto el impacto en las Pymes, analicemos ahora como de preparadas están las pymes frente a las amenazas existentes, con los datos obtenidos del mismo informe:

- el 53% que no cuentan con programas de formación para los empleados
- el 55% que no disponen de procedimientos establecidos para responder a los incidentes de seguridad
- El 41% de las empresas no son capaces de identificar el autor del ataque.
- el 47% de los ciberataques que tienen su origen dentro de la compañía son realizados por empleados o ex empleados.
- Y una proporción algo menor del 40,7%, por proveedores

Si nos centramos en España, el 49% de los directivos españoles reconocen que sus empresas no cuentan con una estrategia integral de seguridad

Con estos datos parece evidente pensar que las pymes no están preparadas para combatir las ciberamenazas que les acechan, ya que no cuentan con:

- Programas de formación y concienciación en materia de seguridad de la información.
- No disponen de políticas y procedimientos tanto internos como para gestionar la relación con terceros (proveedores, clientes,…).
- Medidas técnicas enfocadas a proteger sus activos críticos.

En el informe “CISCO Cybersecurity special report" (5) donde se encuestan casi 2000 empresas de 26 países, se explica cómo las pymes tienen pensado invertir en diferentes soluciones de seguridad:

- el 19% en soluciones de antimalware
- el 18% opta por mejorar sus aplicaciones
- el 17% opta por implementar soluciones de prevención de intrusiones (IPS)
- entorno al 50% opta por subcontratar servicios de seguridad de distinta índole (asesoramiento. Consultoría, monitorización, respuesta ante incidentes, …)

Como podemos ver, las decisiones, aunque varían, demuestran un porcentaje muy bajo de inversión en seguridad, esto viene explicado en el propio informe, ya que el 77% de las pymes encuestadas, declara que les resulta muy complicado implementar en sus empresas medidas de seguridad, debido a la complejidad inherente a este tipo de sistemas, no obstante para ayudar en esta tarea existen diversos marcos de trabajo y normativas de seguridad como la familia de normas ISO 27000.

2.4. Familia ISO 27000

La mejor arma frente a la ciberdelincuencia es la prevención, y que mejor prevención que asumir e implementar buenas prácticas en materia de seguridad de la información, tal y como recoge uno de los estándares más implementados en materia de seguridad e la información: la familia de normas ISO 27000.

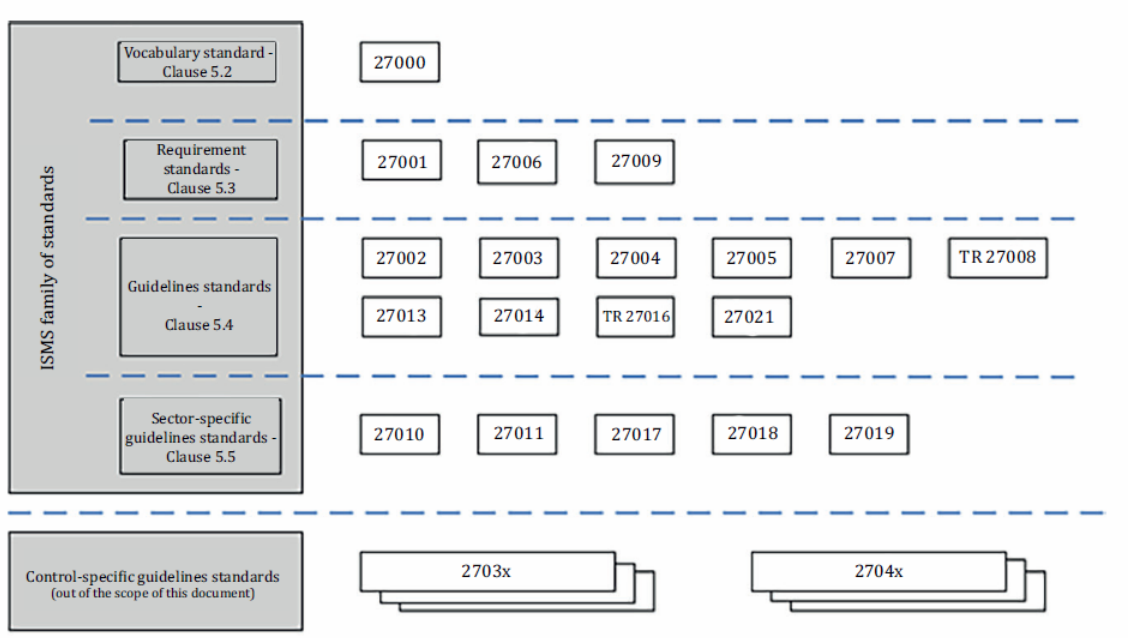


Ilustración 8: Familia de normas ISO 27000 (15)

Las relaciones existentes entre las distintas normas de la familia ISO/IEC 27000 queda reflejada por la Ilustración 8, y la descripción de cada una de las normas que la conforman, así como su posibilidad de ser certificable, queda reflejada en las siguientes tablas.

Estándares vocabulario

Norma	Descripción	Certificable
ISO/IEC 27000	Proporciona una introducción y visión de conjunto de todo el marco ISO 27000 y facilita un glosario común	No

Tabla 2: ISO 27000: Estándares vocabulario

Estándares requisitos

Norma	Descripción	Certificable
ISO/IEC 27001	Recoge los requerimientos para la implantación de un sistema de gestión de la seguridad de la información	SI
ISO/IEC 27006	Define los requerimientos específicos para entidades de certificación que quieran acreditarse en el marco de la ISO/IEC 27000 y deseen certificar SGSI contra la norma ISO/IEC 27001.	NO
ISO/IEC 27009	Guía sobre el uso y aplicación de los principios de ISO/IEC 27001 para el sector servicios específicos en emisión de certificaciones acreditadas de tercera parte.	NO

Tabla 3: ISO 27000: Estándares de requisitos

Estándares directrices

Norma	Descripción	Certificable
ISO/IEC 27002	Código de buenas prácticas para la gestión de la seguridad de la información. Recoge el conjunto de controles que la Norma ISO/IEC 270001 toma como referencia a la hora de seleccionar controles de seguridad.	NO
ISO/IEC 27003	Guía para implementar un SGSI según la norma ISO/IEC 270001.	NO
ISO/IEC 27004	Guía y sugiere mecanismos para medir la eficiencia de un SGSI.	NO
ISO/IEC 27005	Guía para la gestión de los riesgos de seguridad de la información, y proporciona un marco para realizar un análisis de riesgos	NO
ISO/IEC 27007	Guía para la auditoría de SGSI	NO
ISO/IEC TR 27008	Informe técnico que da las guías para la auditoría de los controles de seguridad.	NO
ISO/IEC 27013	Guía para la implementación integrada de ISO 27001 e ISO 20000-1.	NO
ISO/IEC 27014	Guía de gobierno corporativo de la seguridad de la información.	NO
ISO/IEC 27016	Guía de SGSI para aspectos económicos de las organizaciones.	NO
ISO/IEC 27023	Es una guía de correspondencias entre las versiones del 2013 de las normas ISO/IEC 27001 y ISO/IEC 27002 como apoyo a la transición de las versiones publicadas en 2005	NO
ISO/IEC 27050	Orientada a promover las buenas prácticas en métodos y procesos de captura forense y evidencia en la investigación digital.	NO

Tabla 4: ISO 27000: Estándares directrices

Estándares directrices de sector

Norma	Descripción	Certificable
ISO/IEC 27010	Guías para la gestión de la seguridad en las comunicaciones entre diferentes sectores, con especial hincapié en infraestructuras críticas y sistemas industriales	NO
ISO/IEC 27011	Directrices para la gestión de la seguridad y la información en el sector de las telecomunicaciones	NO
ISO/IEC 27012	Conjunto de requisitos y directrices de gestión de seguridad de la información en organizaciones que proporcionen servicios de e-Administración	NO
ISO/IEC 27015	Guía de SGSI para organizaciones del sector seguros y finanzas.	NO
ISO/IEC 27017	Código de prácticas para los controles de seguridad de la información en base a la norma ISO/IEC 27002 para los servicios en la nube.	NO/SI
ISO/IEC 27018	Código de buenas prácticas en controles de protección de datos para servicios de computación en la nube.	NO/SI
ISO/IEC TR 27019	Principios de guía y buenas prácticas basadas en la norma ISO/IEC 27002 para la gestión de seguridad de la información y aplicada a sistemas de control de procesos en entornos industriales de suministro de la energía	NO
ISO/IEC 27021	Presenta los requisitos de competencia profesional en SGSI. Si bien esta norma no es certificable, servirá como base para certificar a profesionales sobre SGSI.	NO
ISO/IEC 27799	Proporciona directrices para apoyar la interpretación y aplicación en el sector sanitario de ISO/IEC 27002	NO

Tabla 5: ISO 27000: Estándares directrices de sector

Estándares directrices de control

Norma	Descripción	Certificable
ISO/IEC 27031	Guía de continuidad de negocio referente a tecnologías de la información y comunicaciones	NO
ISO/IEC 27032	Guía sobre ciberseguridad	NO
ISO/IEC 27033	Guía para la gestión de redes.	NO
ISO/IEC 27034	Guía de seguridad en aplicaciones.	NO
ISO/IEC 27035	Guía de gestión de incidentes de seguridad de la información.	NO
ISO/IEC 27036	Guía de seguridad de servicios externalizados.	NO
ISO/IEC 27037	Guía para la identificación, recopilación y preservación de evidencias digitales.	NO
ISO/IEC 27038	Guía de especificación para la redacción digital.	NO
ISO/IEC 27039	Guía los sistemas de detección de intrusos.	NO
ISO/IEC 27040	Guía para la seguridad en medios de almacenamiento.	NO
ISO/IEC 27041	Directrices para garantizar la idoneidad y adecuación del método de investigación de incidentes.	NO
ISO/IEC 27042	Directrices para el análisis y la interpretación de las evidencias electrónicas.	NO
ISO/IEC 27043	Principios y procesos de investigación de incidentes.	NO
ISO/IEC 27044	Gestión de eventos y de la seguridad de la información.	NO

Tabla 6: ISO 27000: Estándares directrices de control

Si bien he incluido solo las normas publicadas hasta enero de 2018, la realidad es que en el proceso de mejora continua se siguen publicando normas, como por ejemplo la norma ISO/IEC 27103:2018, la cual proporciona una guía sobre cómo aprovechar los estándares existentes en un marco de ciberseguridad.

2.5. Implementación ISO 27000

Si aplicamos los controles especificados en la norma ISO/IEC 27002:2013, podríamos disponer de un sistema de gestión de seguridad de la información que será una primera gran barrera para los ciberdelincuentes que quieran atentar contra nuestra información

Se recomienda la implantación de los controles siguiendo una mentalidad de mejora continua y acorde al ciclo de Demming (PDCA), en el cual se definen 4 fases que se repiten en el tiempo:

Fase 1: Planificar (PLAN)
Los hitos principales de esta fase son:

- Formación y concienciación del personal clave de la organización en materia de seguridad de la información.
- Identificar los activos críticos de la organización.
- Definir un organigrama con los roles en referencia a la seguridad de la información.
- Definir la política que seguirá la organización en materia de seguridad de la información.
- Realizar un análisis de riesgos.
- Identificar los controles de la norma que son de aplicabilidad (SOA) para la organización.

Fase 2: Hacer (DO)
Los hitos principales de esta fase son:

- Gestionar los riesgos identificados en la fase anterior, implementando medidas que minimicen dicho riesgo.
- Adicionalmente a las medidas de seguridad técnicas se recomienda definir procedimientos para la gestión del cambio, para la gestión de incidentes.

Fase 3: Revisar (CHECK)
Los hitos principales de esta fase son:

- Realizar auditorías internas sobre los controles implementados que garanticen la correcta implantación de los mismos.
- Realizar revisiones por la dirección que garantizan que las medidas siguen alineadas con el negocio y que permitan valorar su eficacia.

Fase 4: Actuar (ACT)
Los hitos principales de esta fase son:

- Implementar mejoras tanto a nivel procedimental como a nivel técnico como consecuencia de la revisión anterior.

3. Guía de ciberseguridad

Dado que la empresa debe velar que la información tanto de sus clientes como la suya propia permanezca segura y protegida, y no solo desde un punto de vista ético, sino que existe un incentivo financiero, las empresas tienen la responsabilidad de mejorar las prácticas de ciberseguridad.

Siguiendo una mentalidad de mejora continua y acorde al Círculo de Demming (PDCA) podemos definir 4 como las etapas en las que enmarcar un proyecto de implantación de un sistema de ciberseguridad:

Etapa 1: Planificación (PLAN)

Durante esta fase se debería:

- Formar al personal clave de la organización en relación a la normativa, incluyendo formación específica en gestión de riesgos.
- Definir el alcance:
  - Definir cuáles son los procesos que deben quedar amparados por la norma.
  - Definir los activos involucrados en dichos procesos.
- Planificación del GAP en base a la norma ISO/IEC 27002:2013.
- Establecer un comité de seguridad y definir los roles y organigrama de la organización en relación a la seguridad.
- Definir la política de seguridad de la información
- Definir los objetivos de seguridad de la organización.
- Realización del análisis de riesgos, identificando los riesgos.
- Declaración de aplicabilidad (SOA)
  - Identificar que controles de la norma son de aplicación para la organización y justificar los de no aplicabilidad.

Etapa 2: Hacer (DO)

En esta fase hay dos hitos fundamentales:

- Gestión del riesgo
  - En base al análisis de riesgos anteriormente realizado definir las medidas a implementar para gestionar los riesgos detectados.
- Implementación de controles.
  - En base a la gestión de riesgos definida implementar los controles necesarios.
    Adicionalmente a las salvaguardas técnicas también se deberían implementar procedimientos de gestión de incidentes, de gestión del cambio, de gestión la capacidad,…
  - Definir indicadores que permitan medir la eficacia del sistema.

Etapa 3: Revisión del sistema (CHECK)

- Analizar Objetivos e indicadores definidos anteriormente y establecer las acciones pertinentes en base a los resultados
- Establecer un plan de auditorías internas que permitan medir de una manera objetiva el nivel de implantación de los controles y su eficacia.
- Establecer revisiones por la dirección (la norma determina el establecimiento de una periodicidad mínima anual) del sistema, que permitan validar su eficiencia y alineación con los objetivos del negocio.

Etapa 4: Actuar (ACT)

En esta fase hay dos hitos fundamentales:

- Implementar mejoras: principalmente consecuencia de las acciones definidas durante la etapa anterior.
- Gestión documental, establecer procedimientos y técnicas que permitan identificar, almacenar, proteger, recuperar y eliminar registros que dan soporte al sistema o que puedan ser presentados como evidencia ante una auditoria.

Si bien el alcance de este trabajo queda limitado a las tareas más críticas de las dos primeras fases, es importante abordar las cuatro fases mencionadas para acometer con garantías un proyecto de implantación de un sistema de ciberseguridad.

3.1. Análisis de riesgos

Una de las tareas más críticas es la realización de un análisis de riesgo en materia de seguridad de la información sobre los activos de nuestra organización. Los elementos más importantes y que por ende hay que identificar, son, por un lado los elementos que se deben proteger (**activos**), por otro las causas potenciales de incidentes no deseados y de las cuales hay que protegerse (**amenazas**), las debilidades que facilitan que una amenaza afecte a un activo (**Vulnerabilidades**), y por último también hay que analizar los costes derivados de la materialización de la amenaza (**impacto**). Para asegurar que el análisis de riesgos es objetivo y que pueda conseguir resultados repetibles y comparables, es necesario utilizar la **metodología** apropiada.

Pero antes de iniciar un análisis de riesgos, es importante entender los conceptos mencionados.

3.1.1. Activo:

Entendiendo por activo todo recurso (tangible o intangible) necesario para que la empresa pueda realizar sus actividades y conseguir sus objetivos marcados.
O dicho de una manera más sencilla, cualquier cosa que tenga un valor para la organización y que deba ser por ende protegido.

Esto incluye:

- Datos: La información
- Aplicaciones: que procesan o almacenan la información
- Equipos: Almacenan o por los que fluye la información.
- Soportes: Almacenan información.
- Servicios: Servicios proporcionados por departamentos internos o por terceros para soportar el tratamiento de la información.
- Personas: Personal interno o externo con acceso o que maneja información.
- Ubicaciones: Lugares donde están ubicados los Equipos y las personas.
- Otros: Por ejemplo activos intangibles como la reputación, confianza de los clientes,…

3.1.2. Amenaza:

Entendiendo por amenaza aquellas causas que provocan daños o perdidas en los activos de información.
Existen diferentes sistemas de clasificación de las amenazas, por su naturaleza (humana o no humana), por su carácter (voluntario e involuntario), por su origen (internas o externas),…, no obstante todas las amenazas las podemos agrupar en 4 grandes grupos:

- Desastres: Este grupo incluye: Inundación, fenómenos meteorológicos, fuego, actos de terrorismo,…
- Errores: Este grupo incluye: errores de configuración o mantenimiento en hardware o software, de usuarios,…

- Fallos: Este grupo incluye: cortes de energía o en sistemas de climatización, averías mecánicas en hardware, deterioro de soportes, falta de personal, incumplimientos de contratos,…
- Intencionadas: Este grupo incluye: Ataques DoS, vandalismo, intrusiones (físicas o lógicas), robos, software malicioso, uso inadecuado ilícito de recursos,…

3.1.3. Vulnerabilidad:

Entendiendo por vulnerabilidad la debilidad de un activo que puede ser aprovechada. Si antes he mencionado que la amenaza es una causa, el concepto de vulnerabilidad es el hecho de que esa causa genere consecuencias. Ejemplos de vulnerabilidades serían:

- Puertas abiertas: tanto lógicas como físicas.
- Necesidad de Mantenimientos: La necesidad de los equipos y software a recibir un mantenimiento.
- Necesidad de Energía: La necesidad de los equipos de energía eléctrica.
- Elemento eléctricos no protegidos: cables pelados, interruptores y diferenciales de fácil acceso,…
- Personal clave: La existencia de personal con conocimiento único.
- Falta de formación: Personal no formado para manejar o tratar los activos.
- Ubicación no apta: Ubicar los activos en ubicaciones protegidas,…
- …

3.1.4. Impacto:

La manera más fácil de definirlo sería identificar el impacto con las consecuencias de las que hablaba al definir vulnerabilidad.

3.1.5. Metodología

Si bien existen multitud de metodologías para la realización de dicho análisis, la norma ISO 27001, no específica que norma se debe seguir (ISO 27001 4.2.1c), por lo que en principio cualquier metodología existente es apta para realizar el análisis de riesgos, no obstante por norma general siguen las siguientes fases:

- Definición del **alcance**: En este punto hay que definir qué áreas, departamentos, procesos o sistemas estarna incluidos dentro del análisis.
- Identificación de los **activos**: Es necesario identificar los activos más importantes, dentro del alcance definido previamente, y realizar un inventariado de los mismos.
- Identificación de las **amenazas**: Es necesario identificar aquellas amenazas a las que realmente se encuentran expuestos los activos previamente identificados.
- Identificación de las **vulnerabilidades** y salvaguardas: Es necesario identificar todas aquellas debilidades de nuestros activos y las medidas de protección con las que ya contamos.
- **Evaluación** del riesgo: En esta fase lo que hacemos es relacionar los elementos identificados en fases anteriores. Se establecen pares de activos/amenazas que le aplican, y se estimará una probabilidad de ocurrencia, y el impacto que tendría si esto sucediese, pudiéndose medir dicho impacto de forma cualitativa o cuantitativa y teniendo en cuenta también las salvaguardas ya aplicadas cuyo cometido es precisamente reducir el impacto.

  El riesgo es calculado según la ecuación:

  $$\text{Riesgo} = \text{Probabilidad} \times \text{Impacto}$$

- Tratamiento del riesgo: Por último, una vez identificados los riesgos asociados a los activos debemos decidir cuáles deben ser tratados en base a un umbral previamente definido, y todos aquellos riesgos que superen el umbral deberán ser priorizados y tratados siguiendo una de estas estrategias:

  - **Mitigar**: Estableciendo medidas que permitan reducir el riesgo.
  - **Eliminar**: Eliminando los sistemas o procesos afectados por el riesgo, este desaparece.
  - **Transferir**: Transfiriendo el riesgo a un tercero (por ejemplo a una entidad aseguradora).
  - **Asumir**: Asumiendo el riesgo por justificación de negocio (como por ejemplo que el coste de mitigar o eliminar el riesgo es superior al impacto que este tendría en la organización).

Una vez conocidas las fases básicas, enumeraré distintas metodologías empleadas y que pueden ser tomadas como referencia para la realización del análisis de riesgos, y posteriormente incluiré detalles adicionales de 3 de las más principales, a saber:

- MAGERIT
- OCTAVE
- CRAMM

Pero como ya he adelantado la lista de metodologías existentes es abundante, como por ejemplo:

- Mehari: Principes et mécanismes, definido por CLUSIF (Club de la Sécurité Informatique Français) en Francia.
- Marion: Méthodologie d'Analyse des Risques Informatiques et d'Optimisation par Niveau, también desarrollado por CLUSIF.
- Coras: Construct a platform for Risk Analysis of Security critical system, desarrollado por SINTEF financiado por la unión europea.
- Ebios: Expression des Besoins et Identification des Objectifs de Sécurité, definido por el DCSSI (Direction Centrale de la Sécurité des Systémes d'Information) en Francia.
- MIGRA: Metodologia Integrata Gestione Rischio Aziendale, desarrollado por Elsag Datamat en Italia.
- ISAMM: Information Security Assessment and Monitoring Method, desarrollado por Telindus Group en Bélgica.
- FIRM: Fundamental Information Risk Management, desarrollado por el ISF (Information Security forum)
- …

Adicionalmente diferentes normas nacionales e internacionales proponen métodos de análisis de riesgos como por ejemplo:

- SP 800-30: Risk Management Guide for IT Systems, definida por el NIST (National Institute of Standards and Technology) en Estados Unidos.
- ISO/IEC 13335-2: Management of information and communications technology security - Part2 (reemplazada por la ISO 27005)
- ISO 27005: Information security risk management, definida por ISO/IEC.
- ISO 17776 Petroleum and natural gas industries
- UNE71504: Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información, definida por AENOR.
- …

Y por supuesto siempre podemos definir una metodología propia, siempre que cumpla con lo establecido en la norma, es decir, que permita generar resultados comparables y reproducibles: *"…. (16)."*

Voy analizar levemente tres de estas metodologías: MAGERIT, OCTAVE y CRAMM:

Ambas metodologías se fundamentan en tres procesos principales:

MAGERIT	OCTAVE	CRAMM
Planificación	Evaluación de la organización	Recogida de información
Análisis de riesgos	Identificación de vulnerabilidades	Análisis de riesgos
Gestión de riesgos	Estrategia y desarrollo del plan	Gestión de riesgos

En relación al tipo de valoración, mientras que MAGERIT realiza valoraciones cuantitativas, realizando valoraciones económicas, tanto CRAMM como OCTAVE realizan valoraciones cualitativas, si bien esto a priori facilita la aplicación de la metodología, los resultados son estimativos y muchas veces es necesario realizar un segundo estudio con valores económicos que muestren el verdadero valor del riesgo.

Los pasos (que como podemos observar son muy similares a los identificados al inicio de este punto) para ambas metodologías se pueden resumir en:

1. Establecer criterios de medición de riesgo
2. Identificar los activos de información, especificando su criticidad.
3. Identificación de amenazas
4. Identificar riesgos
5. Analizar riesgos
6. Gestión del riesgo

Adicionalmente en OCTAVE se establece un paso adicional ya que es un proceso iterativo en el que se tratan los riesgos de uno en uno en base a su criticidad.

Criterios de medición del riesgo		
MAGERIT	CRAMM	OCTAVE
Establecimiento de parámetros como: - Valor de los activos - Vulnerabilidad - Impacto - Efectividad del control de seguridad	Define los parámetros numéricos para: - Valoración de activos - Valoración de probabilidades - Estimación de impactos	Define los criterios cualitativos para los parámetros en base a áreas de impacto que defina la organización.

Identificar activos		
MAGERIT	CRAMM	OCTAVE
Incluye valoración económica de los activos y el propietario.	Identificación y evaluación de los activos.	Se define un responsable de cada activo.

Identificación de amenazas		
MAGERIT	CRAMM	OCTAVE
Se identifican las amenazas		

Identificar riesgos		
MAGERIT	CRAMM	OCTAVE
Riesgo = Valor del activo × Vulnerabilidad × Impacto Se realiza un primer análisis intrínseco	Riesgo =Valor + Probabilidad + Impacto	Riesgo = Amenaza (condición) + Impacto (consecuencia)

Analizar riesgos		
MAGERIT	CRAMM	OCTAVE
Se analiza como disminuiría el riesgo aplicando nuevas medidas.	Se calculan los riesgos de materialización de las amenazas.	Se mide de forma cualitativa el grado en que una amenaza afecta a la organización.

Gestión del riesgo		
MAGERIT	CRAMM	OCTAVE
Se analizan las medidas de seguridad a aplicar y se realiza un nuevo análisis de riesgos, teniendo en cuenta las medidas a aplicar. Por último se toman decisiones sobre las medidas de seguridad a implementar.	Se identifican y se seleccionan las medidas de seguridad.	Se tratan los riesgos con mayor puntuación obtenida.

Si bien un análisis de riesgos es un proceso complejo, la existencia de múltiples herramientas en el mercado, tanto de pago como gratuitas, facilitan esta tarea, como por ejemplo la herramienta desarrollada por INCIBE (Instituto Nacional de Ciberseguridad de España) para el análisis de riesgos, basada en un documento Excel: https://www.incibe.es/sites/default/files/contenidos/dosieres/plan-director-seguridad/plan_director_de_seguridad_hoja_para_el_analisis_de_riesgos.xlsm.

Una vez que hemos identificado los riesgos a los que se ve sometido una organización, es el momento de aplicar medidas que mitiguen o eliminen dichos riesgos. Esta mitigación se realizará mediante la implantación de normas y políticas, procedimientos, programas de formación y concienciación y por supuesto la implementación de controles de seguridad, para poder implementar estas medidas es conveniente basarse en guías de buenas prácticas existentes en el mercado como puede ser la norma ISO/IEC 27002:2013 que será utilizada como referencia en el siguiente apartado.

3.2. Controles de ciberseguridad

A partir del análisis de riesgos inicial, se identifican los principales riesgos a los que se puede ver sometido la organización, y que suelen estar asociados a sus activos más críticos y de los que depende la continuidad de sus procesos de negocio, por lo que el siguiente paso es establecer una serie de medidas que o bien mitiguen o reduzcan el riesgo, o bien reduzcan su probabilidad de ocurrencia.

Puesto que vamos a tomar como referencia la norma ISO/IEC 27002:2013, el primer paso que debemos realizar es analizar cuáles de los 114 controles definidos por esta son de aplicabilidad para la organización. Esta aplicabilidad la realizaremos en base a la actividad de la empresa, la propia gestión y de su entorno, donde se incluyen los marcos legales y normativos a los que se encuentre sometida la organización.

Si bien este es un análisis particular para cada organización, en España podemos encontrar entre la posible legislación aplicable y su relación con algunos de los controles asociados:

- LSSI: Ley 34/2002 de Servicios de la Sociedad de la Información y de Comercio Electrónico.
    - 14.1.2 - Securizar los servicios de aplicaciones en redes públicas
    - 14.1.3 - Protección de las transacciones de servicios de aplicaciones
    - 14.1.2 - Securizar los servicios de aplicaciones en redes públicas

    - 10.1.1 - Política de uso de los controles criptográficos
    - 18.1.5 - Regulación de los controles criptográficos
- LPI: Ley 23/2006 de Propiedad Industrial
- LOPD/RGPD: Ley Orgánica 3/2018 de Protección de Datos y de Garantía de los Derechos Digitales que sustituye a la Ley Orgánica 15/99 de Protección de Datos de Carácter Personal, adaptándola al Reglamento (UE) 2016/679, General de Protección de Datos (RGPD)
    - 5.1.1 - Las políticas de seguridad de la información
    - 6.1.1 - Roles y responsabilidades en seguridad de la información
    - 18.1.1 - Identificación de la legislación aplicable
    - 18.1.4 - Protección de datos y privacidad de la información de carácter personal
    - 9.2.1 - Registro y baja de usuario
    - 12.3.1 - Copias de seguridad de la información
    - 16.1.2 - Notificación de los eventos de seguridad de la información
    - 10.1.1 - Política de uso de los controles criptográficos
    - 10.1.2 - Gestión de claves
    - 14.3.1 - Protección de los datos de prueba
    - 18.2.3 - Comprobación del cumplimiento técnico
- ENS: Real Decreto Legislativo 3/2010 de enero por el que se establece el Esquema Nacional de Seguridad.
- Si bien el Esquema Nacional de Seguridad tiene un carácter más imperativo que la norma ISO/IEC 27002:2013, ya que esta última es más descriptiva, existe múltiple documentación que facilita el cumplimiento del ENS a partir de la implantación de los controles de la norma ISO/IEC 27002:2013, por ejemplo la guía de seguridad (CCN-STIC 825) (17)
- Leyes locales como por ejemplo: Real Decreto 66/2012 - Política de seguridad de la información de la Generalitat, Real Decreto 130/2012 - Organización de la seguridad de la información de la Generalitat
- Reglamento (UE) n o 910/2014 del Parlamento Europeo y del Consejo de 23 de julio de 2014 relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por la que se deroga la Directiva 1999/93/CE
    - 10.1.1 - Política de uso de los controles criptográficos
    - 14.1.3 - Protección de las transacciones
    - 18.1.5 - Regulación de los controles criptográficos
- Ley 59/2003, de 19 de diciembre, de firma electrónica
    - 10.1.1 - Política de uso de los controles criptográficos
    - 14.1.3 - Protección de las transacciones
    - 18.1.5 - Regulación de los controles criptográficos

El concepto de aplicabilidad no se limita a legislación sino que incluye cualquier otro criterio que la empresa considere, como por ejemplo otras normativas de distinta índole como pueden ser ISO9001, normativas medioambientales como ISO14001 o regulaciones específicas como PCI-DSS (Regulación de la industria de tarjetas de pago), en esta última dado que el número de controles a implementar por esta norma son superiores a los definidos en la norma ISO/IEC 27002:2013, prácticamente son de aplicabilidad el 75 % de los controles definidos en esta, tal y como podemos ver en la Tabla 7.

Norma	Descripción	Certificable
ISO/IEC 27000	Proporciona una introducción y visión de conjunto de todo el marco ISO 27000 y facilita un glosario común.	No

Controles aplicables por PCI-DSS
5.1.1 Las políticas de seguridad de la información
6.1.1 Roles y responsabilidades en seguridad de la información
6.1.2 Segregación de tareas
6.1.3 Contacto con las autoridades
6.1.4 Contacto con grupos de interés especial
6.1.5 Seguridad de la información en la gestión de proyectos
6.2.1 Política de dispositivos móviles
6.2.2 Teletrabajo
7.1.1 Investigación de antecedentes
7.1.2 Términos y condiciones de contratación
7.2.1 Responsabilidades de la dirección
7.2.2 Concienciación, educación y capacitación en seguridad de la información
8.1.1 Inventario de activos
8.1.3 Uso aceptable de los activos
8.2.1 Clasificación de la información
8.2.3 Manipulado de la información
8.3.1 Gestión de soportes extraíbles
8.3.2 Eliminación de soportes
8.3.3 Soportes físicos en tránsito
9.1.1 Política de control de acceso
9.1.2 Política de uso de los servicios de red
9.2.1 Registro y baja de usuario
9.2.2 Provisión de acceso de los usuarios
9.2.3 Gestión de privilegios
9.2.4 Gestión de la información secreta de autentificación de los usuarios
9.2.5 Revisión de los derechos de acceso de usuario
9.2.6 Retirada de los derechos de acceso
9.3.1 Uso de la información secreta de autenticación

Controles aplicables por PCI-DSS
9.4.1 Restricción del acceso a la información
9.4.2 Procedimientos seguros de inicio de sesión
9.4.3 Sistema de gestión de contraseñas
10.1.1 Política de uso de los controles criptográficos
10.1.2 Gestión de claves
11.1.1 Perímetro de seguridad física
11.1.2 Controles físicos de entrada
11.1.3 Seguridad de oficinas, despachos y recursos
11.2.3 Seguridad del cableado
11.2.5 Retirada de materiales propiedad de la empresa
11.2.6 Seguridad de los equipos fuera de las instalaciones
11.2.7 Reutilización o eliminación de equipos
11.2.8 Equipo de usuario desatendido
12.1.1 Documentación de procedimientos de operación
12.1.2 Gestión de cambios
12.1.4 Separación de los recursos de desarrollo, prueba y operación
12.2.1 Controles contra el código malicioso
12.3.1 Copias de seguridad de la información
12.4.1 Registro de eventos
12.4.2 Protección de la información de registro
12.4.3 Registros de administración y operación
12.4.4 Sincronización del reloj
12.5.1 Instalación del software en explotación
12.6.1 Control de las vulnerabilidades técnicas
13.1.1 Controles de red
13.1.2 Seguridad de los servicios de red
13.1.3 Segregación en redes
13.2.1 Políticas y procedimientos de intercambio de información
13.2.3 Mensajería electrónica
13.2.4 Acuerdos de confidencialidad
14.1.2 Securizar los servicios de aplicaciones en redes públicas
14.1.3 Protección de las transacciones de servicios de aplicaciones
14.2.1 Política de desarrollo seguro
14.2.2 Procedimiento de control de cambios en sistemas
14.2.3 Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo
14.2.5 Principios de ingeniería de sistemas seguros
14.2.8 Pruebas funcionales de seguridad
14.2.9 Pruebas de aceptación de sistemas
14.3.1 Protección de los datos de prueba
15.1.1 Política de seguridad de la información en relaciones con los proveedores
15.1.2 Requisitos de seguridad en contratos con terceros
15.2.1 Supervisión y revisión de los servicios prestados por terceros
15.2.2 Gestión de cambios en los servicios prestados por terceros

Controles aplicables por PCI-DSS
16.1.1 Responsabilidades y procedimientos
16.1.2 Notificación de los eventos de seguridad de la información
16.1.4 Evaluación y decisión sobre los eventos de seguridad de información
16.1.5 Respuesta a incidentes de seguridad de la información
16.1.6 Aprendizaje de los incidentes de seguridad de la información
16.1.7 Recopilación de evidencias
17.1.1 Planificación de la continuidad de seguridad de la información
17.1.3 Pruebas, mantenimiento y reevaluación de los planes de continuidad del negocio
18.1.1 Identificación de la legislación aplicable
18.1.2 Derechos de propiedad intelectual (DPI)
18.1.3 Protección de los registros de la organización
18.2.3 Comprobación del cumplimiento técnico

Tabla 7: Controles ISO/IEC 27002:2013 aplicables por PCI-DSS

Llegados a este punto es el momento de analizar los 114 controles y analizar cuáles son las tareas asociadas a los mismos y que nos ayudaran a mitigar el impacto de o reducir la posibilidad de ocurrencia de los riesgos detectados. Estos controles están recogidos en la norma ISO/IEC 27002:2013 y aparecen agrupados en los siguientes dominios de control:

3.2.1. Políticas de seguridad de la información

Este dominio de control proporciona las directrices necesarias para la gestión de la seguridad de la información, en base a los requerimientos del negocio y su entorno, e implica la creación de una política de seguridad y su revisión periódica.

Tareas:

- Creación de una política de seguridad, que sea aprobada por la dirección y publicada a las partes interesadas (empleados, clientes, proveedores, …). Dicha política debería recoger entre otros:
  - El compromiso por parte de la dirección
  - El alcance
  - Los objetivos definidos
  - La disponibilidad de la infraestructura, tanto física como material necesaria para el cumplimiento de dichos objetivos.
  - Principios y normas
  - Responsabilidades
  - Legislación y/o normativas de aplicación.
  - …
- Mantener actualizada dicha política:
  - Estableciendo revisiones periódicas de la misma
  - Actualizándola en relación a los cambios y necesidades de la organización.

Controles asociados:

- 5.1.1 - Las políticas de seguridad de la información
- 5.1.2 - Revisión de las políticas de seguridad de la información

3.2.2. Organización de la seguridad de la información

Este dominio de control tiene como objeto describir y documentar la estructura organizativa en materia de seguridad definida en la organización y las responsabilidades y funciones asociadas.

Tareas:

- Creación de una relación de roles y responsabilidades (pudiendo estar recogidas en fichas de puesto de trabajo, por ejemplo, aunque también pueden ser terceras partes a la organización como proveedores o usuarios externos) en relación a la seguridad de la información, y asociar estos roles a personas concretas, intentando segregar tareas en la medida de lo posible por ejemplo separando las responsabilidades entre distintos entornos (producción, desarrollo,…) o que permitan un sistema de aprobación para tareas críticas. Estos roles y responsabilidades deben ser comunicados y aceptados por las personas implicadas.
- Identificar contactos con las autoridades, es decir tener claro con quien se debe contactar en caso de un incidente de seguridad. Por ejemplo los distintos cuerpos de seguridad del estado, servicios de protección civil, Agencia Española de Protección de Datos, o cualquier otra autoridad pertinente.
- Identificar grupos de interés especial en materia de seguridad como por ejemplo INCIBE, ENISA, CyberEOP, …, y mantenerse informado en materia de seguridad de la información, por ejemplo, asistiendo a eventos o leyendo noticias y alertas relativas a seguridad de la información, en resumen, estar al día en cuanto a las amenazas existentes y si existen protecciones o recomendaciones al respecto.
- Realizar evaluaciones de riesgos (desde el punto de vista de la seguridad de la información) al iniciar cualquier proyecto, identificando amenazas, vulnerabilidades y los riesgos asociados al proyecto, y gestionar ichos riesgos tal y como se explicó en el punto 0.
- Establecer normas específicas para el uso de dispositivos móviles como smartphones o portátiles, por ejemplo incluyendo elementos de buenas prácticas y sentido común como: no dejar a la vista estos dispositivos en lugares públicos o coches donde puedan ser sustraídos, limitar su uso fuera de un entorno controlado (por ejemplo oficinas) si dichos equipos contienen información confidencial, prohibición de instalación de software no aprobado por el departamento responsable de los activos, no conectar a redes desconocidas (como redes Wifi públicas), …
- Si se permite el acceso a la información en modalidad de teletrabajo, establecer normas y medidas de seguridad específicas, como, por ejemplo, la limitación de acceso a ciertos activos, garantizar la seguridad de las conexiones, acceso a un entorno virtualizado que no permita extraer información, restricciones de la configuración de los servicios de

red inalámbricos, establecer revisiones periódicas de los activos empleados, …

Controles asociados:

- 6.1.1 - Roles y responsabilidades en seguridad de la información
- 6.1.2 - Segregación de tareas
- 6.1.3 - Contacto con las autoridades
- 6.1.4 - Contacto con grupos de interés especial
- 6.1.5 - Seguridad de la información en la gestión de proyectos
- 6.2.1 - Política de dispositivos móviles
- 6.2.2 - Teletrabajo

3.2.3. Seguridad relativa a los recursos humanos

Como he mencionado en puntos anteriores el factor humano es el origen de la mayoría de los incidentes de seguridad, por lo que este dominio adquiere una relevancia crítica, ya que servirá para mitigar el riesgo de robo, fraude o uso indebido de los activos de la información.
El objeto de este control es describir y documentar la normativa y procedimientos que aseguren que empleados, contratistas y terceros comprenden sus responsabilidades y obligaciones en materia de seguridad de la información, garantizando además que estas son suficientes y adecuadas. Estos procedimientos deben cubrir desde los procesos anteriores de la contratación, los procesos durante el tiempo que permanezcan empleados en la organización y una vez que haya finalizado la relación.

Un elemento clave es la ejecución de procesos formativos y de concienciación en materia de seguridad de la información, que permiten dar un nivel de conocimiento en materia de seguridad de la información a los usuarios que evite o mitigue los errores humanos.

Tareas:

- Realizar un análisis de los antecedentes presentados por los nuevos candidatos (siempre acorde a la legislación vigente), por ejemplo:
    - Confirmando que tanto la carrera profesional como la formación indicada en el currículo son verídicas.
    - Investigando en las empresas en las que afirma haber trabajado en su currículo, asegurando su veracidad, y validando si existen buenas referencias.
    - Intentando averiguar si ha tenido responsabilidad en algún incidente de seguridad
    - Asegurar que tiene la capacitación necesaria para el desempeño de sus funciones.

Si bien esta tarea puede llegar a ser compleja es importante adecuarla a las necesidades del puesto y al tipo/cantidad de información a la que tendrá acceso. Una alternativa a asumir estas funciones internamente es subcontratar el servicio a empresas especializadas.

- Establecer acuerdos de confidencialidad y asegurar que son entendidos y aceptados tanto por personal interno como externo, es decir con empleados, subcontratistas y terceros, garantizando así el cumplimiento de las normas y políticas definidas por la organización.
- Establecimiento, por parte de dirección del obligado cumplimiento de las normas y políticas en materia de seguridad definidas en la organización. Una buena manera es incluirlas como anexo en los contratos. No obstante, estas políticas y normas siempre deben ser accesibles por los empleados y contratistas.
- Establecer procesos formativos en materia de seguridad de la información, estos procesos pueden ir enfocados a adquirir conocimientos técnicos o a promover el conocimiento, entendimiento y seguimiento de las normas y políticas internas definidas.
- Establecer procesos de concienciación en materia de seguridad, cuyo fin es que el personal adquiera buenos hábitos y que sea consciente de las repercusiones de un incidente de seguridad. Un buen punto de partida podría ser el kit de concienciación facilitado por el INCIBE: https://www.incibe.es/protege-tu-empresa/kit-concienciacion.
- Establecer procesos disciplinarios que puedan ser ejecutados en caso de que un empleado esté implicado en un incidente o brecha de seguridad, estos procedimientos pueden estar basados en amonestaciones, siempre amparados en la legislación vigente en materia de despidos y sanciones.
- Establecer acuerdos de no divulgación de información tras el cese en la empresa, deber de secreto profesional, recordando las responsabilidades legales que persisten a pesar de la finalización de un contrato.

Controles asociados:

- 7.1.1 - Investigación de antecedentes
- 7.1.2 - Términos y condiciones de contratación
- 7.2.1 - Responsabilidades de la dirección
- 7.2.2 - Concienciación, educación y capacitación en seguridad de la información
- 7.2.3 - Proceso disciplinario
- 7.3.1 - Responsabilidad del cese o cambio

3.2.4. Gestión de activos

El objeto principal de este dominio de control es la protección de los activos de información de la organización.

Tareas:

- Identificar los activos de la organización mediante un inventario. Es necesario disponer de un procedimiento de etiquetado (acorde a su clasificación), que permita identificar un activo.
- Clasificar dichos activos en base al valor que tienen para la organización, por ejemplo:
    - En base a confidencialidad los podemos clasificar como públicos, internos (solo para la organización) y privados.
    - En base a la disponibilidad los podemos clasificar como críticos, medios o leves en base al impacto de su no disponibilidad cause a la organización (por ejemplo afectando a la operativa normal, o implicaciones legales o económicas)
    - En base a la integridad, los podemos clasificar igualmente como críticos, medios y leves, en base al impacto de su pérdida de exactitud y completitud cause a la organización

    Si bien he utilizado distintas denominaciones, lo ideal es utilizar las mismas, para facilitar el entendimiento en la organización, por ejemplo algo tan simple como Alto, Medio y Bajo, identificando adicionalmente las necesidades y acciones derivadas de dicha clasificación.
- Establecer un responsable para cada uno de los activos (también denominado propietario).
- Establecer mediante normas o políticas cuáles son los usos correctos permitidos de los mismos, basándose en la clasificación previamente realizada.
- Establecer procedimientos de entrega y devolución de los activos, que contemplen por además el borrado de la información.
- Establecer políticas específicas para soportes extraíbles como llaves USB, discos duros externos, cintas, … Estas políticas o medidas deben contemplar:
    - Procedimientos de autorización para su uso.
    - Medidas de seguridad para su almacenamiento.
    - Medidas de seguridad para su traslado.
    - Procesos de eliminación del contenido o su destrucción.
    - Registrar e inventariar dichos dispositivos.
    - Controlar que información puede ser copiada a un medio extraíble.
    - …

Controles asociados:

- 8.1.1 - Inventario de activos
- 8.1.2 - Propiedad de los activos

- 8.1.3 - Uso aceptable de los activos
- 8.1.4 - Devolución de activos
- 8.2.1 - Clasificación de la información
- 8.2.2 - Etiquetado de la información
- 8.2.3 - Manipulado de la información
- 8.3.1 - Gestión de soportes extraíbles
- 8.3.2 - Eliminación de soportes
- 8.3.3 - Soportes físicos en tránsito

3.2.5. Control de acceso

El objetivo principal de este dominio es controlar el acceso a la información mediante una buena gestión de usuarios de los sistemas, componentes o aplicaciones, de forma que se garantice la debida protección de la información frente a accesos no autorizados.

Tareas:

- Definir una política de control de accesos, basando está en una política de mínimos privilegios. Un buen sistema a la hora de asegurar que los requisitos son los mínimos es contestar a: Para desempeñar su función, el usuario …
  - ¿necesita conocer esta información?
  - ¿necesita utilizar esta aplicación o servicio?
  - ¿durante cuánto tiempo necesita esta información?
  - ¿se pueden aplicar limitaciones horarias de acceso?
  -

  Si bien es recomendable una política de denegación por defecto, hay que buscar el equilibrio entre seguridad y funcionalidad. Esta política debe ser revisada y actualizada periódicamente, asegurando que la concesión de los privilegios no excede en tiempo a la necesidad de los mismos.
- Establecer procedimientos para la solicitud de accesos y privilegios, incluyendo tanto un sistema de aprobación, como un sistema de revocación.
- Planificar revisiones periódicas de autenticación de usuarios y privilegios, eliminando los privilegios que se detecten que ya no son necesarios (por ejemplo, que un usuario ha cambiado de puesto o función), deshabilitando los usuarios que ya no requieran acceso a una aplicación o incluso a ninguna información (por ejemplo, aquellos que han causado baja).
- Establecer roles y responsabilidades por perfil de usuario, separando por ejemplo administradores de usuarios estándar, y donde se especifique la no distribución o compartición de la información de autenticación.

Limitando el acceso al código fuente de las aplicaciones desarrolladas internamente.

- Planificar revisiones periódicas de autenticación de usuarios y privilegios en aplicaciones. Donde se modificaran las contraseñas correspondientes en caso de haberse visto comprometidas.
- Establecer una política de contraseñas, donde se defina su complejidad, longitud, caducidad, política de bloqueo de cuenta tras intentos fallidos, …, y donde se informe del carácter personal de las credenciales (esto último puede incluirse en contratos), y de las medidas necesarias para protegerlas, como, por ejemplo:
  - No utilizar registros de las mismas (post-its, escribirlas en un cuaderno, …)
  - Cambiar la contraseña si se considera que ha sido comprometida.
  - Evitar la reutilización de la misma contraseña para distintos sistemas/aplicaciones.
  - Establecer contraseñas de calidad (muy ligado a la formación y la concienciación)
- Registrar intentos de sesión fallidos y analizar las causas/orígenes.

Controles asociados:

- 9.1.1 - Política de control de acceso
- 9.1.2 - Política de uso de los servicios de red
- 9.2.1 - Registro y baja de usuario
- 9.2.2 - Provisión de acceso de los usuarios
- 9.2.3 - Gestión de privilegios
- 9.2.4 - Gestión de la información secreta de autentificación de los usuarios
- 9.2.5 - Revisión de los derechos de acceso de usuario
- 9.2.6 - Retirada de los derechos de acceso
- 9.3.1 - Uso de la información secreta de autenticación
- 9.4.1 - Restricción del acceso a la información
- 9.4.2 - Procedimientos seguros de inicio de sesión
- 9.4.3 - Sistema de gestión de contraseñas
- 9.4.4 - Uso de las utilidades con privilegios del sistema
- 9.4.5 - Control de acceso al código fuente de los programas

3.2.6. Criptografía.

El objetivo principal de este dominio es gestionar correctamente los elementos criptográficos utilizados para proteger la seguridad de la información, desde el punto de vista de la confidencialidad e integridad.

Tareas:

- Intentar cifrar tanto las comunicaciones como el almacenamiento de información que pueda ser considerada sensible o crítica para la organización. Es decir, hay que identificar sobre qué información es necesaria emplear claves criptográficas.
- Utilizar algoritmos de cifrado robustos (en la medida de lo posible)
- Establecer un procedimiento de gestión de claves criptográficas, en el cual se identifiquen los custodios de las mismas y los procedimientos a seguir para su generación, renovación, cambio o eliminación. Este procedimiento deberá incluir información de su uso y protección.

Controles asociados:

- 10.1.1 - Política de uso de controles criptográficos.
- 10.1.2 – Gestión de claves.

3.2.7. Seguridad física y del entorno

El objetivo principal de este dominio es controlar el acceso físico tanto a la información (activos) como a las instalaciones, mediante una buena gestión de accesos y riesgos, de forma que se garantice la debida protección de la información frente a accesos no autorizados, robos o daños causados por amenazas físicas y ambientales.

Tareas:

- Definir una política de control de accesos físicos, que identifique las áreas seguras, y que recoja un registro de acceso tanto a las áreas seguras como a las instalaciones en general, y que garantice que personal externo o no autorizado estará acompañado durante su estancia en las instalaciones. Esta política deberá contemplar áreas de entrega y carga de manera específica, por tratarse de puntos sensibles para la seguridad física.
- Aislar los elementos críticos en áreas seguras, que les protejan no solo contra accesos no autorizados, sino también contra amenazas físicas y ambientales.
- Aplicar barreras físicas que impiden el libre acceso a personal no autorizado a las instalaciones (Muros, vallas, alarmas, cerraduras, …).
- Establecer medidas contra amenazas ambientales o fiscas como :
    - extintores y detectores de humo contra el fuego.
    - climatizadores contra temperaturas extremas o alta humedad.

    - Sistemas de alarma contra posibles robos o accesos no autorizados (sistemas de control de presencia, volumétricos, detectores de actividad, …)

  y que estos elementos de protección sean revisados periódicamente.
- Establecer planes de emergencia ante incidentes físicos, que recojan entre otros: planes de evacuación, puertas de emergencia, planes de continuidad (ver 3.2.13 Aspectos de seguridad de la información para la gestión de la continuidad del negocio), …
- Evaluar otros impactos ambientales como terremotos, inundaciones, avalanchas,… Y establecer medidas y políticas acordes.
- De igual manera que protegemos las instalaciones se deben proteger los activos, por ejemplo, frente a cortes de luz, inundaciones, hábitos nocivos para los equipos como comer. Beber o fumar cerca de un equipo, ….
- Establecer una política de escritorios y pantallas limpios, que informe al usuario de los riesgos de dejar llaves USB o documentación impresa sobre los escritorios, o el dejar sin bloquear su escritorio ante una ausencia (aunque sea corta). Para el bloqueo de pantalla, se recomienda que el proceso sea automático y que no dependa del usuario final. En esta política podemos hacer hincapié también en el no abandono de documentación en las impresoras, o establecer sistemas que no liberen el documento impreso hasta que el usuario esté presente físicamente para recogerlo.
- Monitorizar los servicios contratados a terceros, como por ejemplo electricidad, comunicaciones, …, así como que los equipos se mantienen adecuadamente, para garantizar que el servicio prestado es acorde con las necesidades de la organización.
- Proteger el cableado, evitando su exposición, en la medida de lo posible, a elementos electromagnéticos o accesos físicos. Por ejemplo, mediante el uso de canalizaciones apropiadas, separar los cables de comunicaciones de los cables de tensión, asegurar los puntos de conexión y evitar la conexión de dispositivos no autorizados, ...
- Mantener un registro de entrega de activos a personal tanto interno como externo, registrando tanto su entrega como su recogida.
- Asegurar la eliminación de la información previamente existente en el caso de la reutilización de activos.

Controles asociados:

- 11.1.1 - amenazas físicas y ambientales.
- 11.1.2 – amenazas físicas y ambientales.
- 11.1.3 - Seguridad de oficinas, despachos y recursos.
- 11.1.4 - Protección contra las amenazas externas y ambientales.

- 11.1.5 - El trabajo en áreas seguras
- 11.1.6 - Áreas de carga y descarga
- 11.2.1 - Emplazamiento y protección de equipos.
- 11.2.2 – Instalaciones de suministro.
- 11.2.3 - Seguridad del cableado.
- 11.2.4 - Mantenimiento de los equipos.
- 11.2.5 - Retirada de materiales propiedad de la empresa.
- 11.2.6 - Seguridad de los equipos fuera de las instalaciones.
- 11.2.7 – Reutilización o eliminación de equipos.
- 11.2.8 – Equipo de usuario desatendido.
- 11.2.9 – Política de puesto de trabajo despejado y pantalla limpia.

3.2.8. Seguridad de las operaciones

El objetivo de este dominio es asegurar que los elementos en los que se realizan las operaciones, tengan definidos todos los procedimientos, que se realiza una planificación de recursos de los sistemas para minimizar el riesgo de fallo, que estén protegidos frente a código malicioso, que se realizan verificaciones periódicas de vulnerabilidades y que se establecen precauciones para evitar que las actividades de auditoría afecten las operaciones, mediante el registro de eventos, y por supuesto que se crean procedimientos para la generación de copias de seguridad y su recuperación.

Tareas:

- Documentar todos los procedimientos necesarios que garanticen el conocimiento de:
  - La forma de trabajar en general, es decir procesamiento y manejo de la información.
  - Relaciones entre procesos
  - Herramientas necesarias
  - Tiempos de ejecución
- Identificar y documentar los responsables de los procesos, y que aprueben los cambios realizados en las operaciones.
- Establecer un procedimiento de cambio para los sistemas, que incluya;
  - Planificación y definición de tareas
  - Sistema de aprobación
  - Comunicación a los interesados
  - Elementos afectados por el cambio
  - Un procedimiento de vuelta de atrás en caso de que tras implementar el cambio se detecten anomalías en los sistemas, que permita volver al punto anterior al cambio sin impacto.

- Para asegurar la disponibilidad y el rendimiento de los sistemas es necesario realizar una gestión de la capacidad, es decir:
    - Monitorizar y medir los recursos disponibles
    - Realizar periódicamente análisis de dichos consumos para prevenir futuras necesidades y optimizar su uso.
- Si la organización tiene desarrollo de productos, conviene separar los entornos de desarrollo, pruebas y producción. Si se trata de desarrollo de software, conviene:
    - Utilizar usuarios distintos para cada entorno
    - Asegurar que los datos de producción no son usados en otros entornos que no sea el productivo. Si se necesitan datos para otros entornos (desarrollo o pruebas) sería necesario tratar los datos productivos antes de introducirlos en un entorno distinto al productivo, este tratamiento podría der por ejemplo de anonimización o al menos modificar los datos con algún proceso que genere datos aleatorios, preservando la privacidad de los datos personales.
- Para proteger a la organización frente a códigos maliciosos, y mantener gestionadas las vulnerabilidades existentes, conviene:
    - Instalar sistemas antimalware que se actualicen diariamente y que realicen análisis de forma periódica.
    - Establecer políticas que no permitan la instalación de software no autorizado por la organización.
    - Establecer políticas de actualización periódica de los sistemas.
    - Revisar periódicamente la existencia de nuevas vulnerabilidades en los sistemas, e intentar subsanarlas, o en caso de imposibilidad establecer medidas adicionales que mitiguen la explotación de la misma.
    - Filtrar la navegación Web para impedir el acceso de códigos maliciosos desde sitios web de internet, pudiendo llegar incluso a bloquearla totalmente en aquellos sistemas que no la requieran para el desempeño de su función.
    - Establecer filtros antispam que impidan el acceso de códigos maliciosos desde el correo electrónico.
    - Incluir en el plan de formación/concienciación en materia de seguridad de la información relativa a código maliciosos y cómo actuar, por ejemplo: Identificar correos sospechosos en los que no abrir adjuntos ni pulsar en los enlaces contenidos, no introducir llaves USB “desconocidos”, aislar el equipo al detectar un malware, ...
- Establecer una política de copias de seguridad que garantice la recuperación de la información crítica de la compañía en caso de

producirse un incidente de seguridad que provoque pérdida o falta de integridad de la información. En esta política hay que contemplar:

  - Los activos de información a respaldar.
  - La periodicidad de las copias
  - La ubicación donde almacenar las copias. Hay que tener en cuenta que si se produce un incidente en el lugar donde se encuentra la información en producción y se almacenan en el mismo sitio las copias de seguridad, estas pueden verse igualmente afectadas por el incidente, pudiendo no poder cumplir su función.
  - Las medidas de seguridad necesarias para proteger las copias realizadas.
  - La periodicidad con la que se realizan pruebas de comprobación en las que se validan las copias realizadas garantizando que pueden ser restauradas y que la información protegida es recuperable en caso de necesidad.

- Se debe implementar un sistema de monitorización que:
  - Permita registrar los eventos con la información necesaria: evento concreto, fecha, hora, usuario, sistema implicado,…, es decir que permite realizar una trazabilidad de los eventos e identificar la autoría de los mismos. Entre los eventos más importantes se encuentran:
    - Los intentos de acceso a un sistema, registrando tanto los exitosos como los fallidos, así como las desconexiones posteriores.
    - Las acciones realizadas sobre el sistema
    - Alertas generadas por el sistema
    - Encendido y apagado de sistemas o servicios.
    - …
  - Proteja los eventos recogidos tanto frente a pérdida, manipulación o degradación.
  - Puesto que los administradores disponen de permisos especiales sobre los sistemas, se deben, en la medida de lo posible, limitar los permisos de estos sobre los registros, impidiendo su borrado o desactivación.
- Para asegurar que los registros/eventos anteriores puedan ser correlados es necesario que todos los sistemas de la organización estén sincronizados contra una fuente horaria común.
- Antes de instalar un nuevo software (o una actualización) sobre un sistema de la organización se recomienda probarlo sobre un entorno no productivo, y en cualquier caso aplicando siempre la gestión de cambios definida que permita volver a la situación anterior al cambio.
  - Incluir en el programa de auditorías, auditorias, que auditarán desde un punto de vista técnico que los controles aplicados

cumplen con su función, pero siempre garantizando que las mismas no impactaran (o al menos mínimamente) sobre los sistemas auditados.

Controles asociados:

- 12.1.1 - Documentación de procedimientos de operación.
- 12.1.2 – Gestión de cambios.
- 12.1.3 - Gestión de capacidades.
- 12.1.4 - Separación de los recursos de desarrollo, prueba y operación.
- 12.2.1 - Controles contra el código malicioso.
- 12.3.1 - Copias de seguridad de la información.
- 12.4.1 - Registro de eventos.
- 12.4.2 - Protección de la información de registro
- 12.4.3 - Registros de administración y operación
- 12.4.4 - Sincronización del reloj
- 12.5.1 - Instalación del software en explotación.
- 12.6.1 - Control de las vulnerabilidades técnicas
- 12.6.2 - Restricción en la instalación de software.
- 12.7.1 - Control de auditoria de sistemas de información

3.2.9. Seguridad de las comunicaciones

El objetivo de este dominio es asegurar que todos los elementos implicados en el procesamiento y en la transmisión de información están protegidos mediante los controles adecuados. Para conseguir este objetivo es necesario gestionar las redes de comunicaciones, garantizando entre otras cosas que no hay accesos no controlados.

Tareas:

- Definir un procedimiento de gestión de los equipos de red que incluya los roles y responsabilidades asociadas. Adicionalmente a los elementos físicos (Router, switch, …) se debe contemplar la propia transmisión de la información.
- Definir controles de acceso que garanticen la autenticidad, por ejemplo, mediante el uso de fatores múltiples de autenticación.
- Estos procedimientos y controles definidos deben ser de aplicabilidad también para los sistemas de mensajería (correo electrónico, chats, redes sociales, …).
- Segmentar la red en la medida de lo posible permitiendo establecer distintos dominios de seguridad con distintas políticas y restricciones. Los criterios para segmentar una red se deben basar en:
    - Criterios de visibilidad

    - Criterios de aislamiento
    - Control de datos entrantes y salientes de cada segmento
    - Asegurar la denegación por defecto, es decir si un tráfico no está permitido explícitamente, debe ser denegado.
- Establecer por contrato acuerdos de servicio con el proveedor de servicios de red y monitorizar su cumplimiento de manera regular.
- Definir procedimientos para el intercambio de información con terceros, que protejan la información tanto desde el punto de vista de integridad y confidencialidad (por ejemplo, mediante el uso de sistemas cifrados que garanticen el intercambio), y desde el punto de vista de la disponibilidad (por ejemplo, empleando elementos redundantes), asegurando que los procedimientos definidos son acordes a la legislación aplicable.
- Dichos procedimientos deben ser reforzados con acuerdos de confidencialidad y no divulgación que identifiquen:
    - La naturaleza de la información a transmitir.
    - La responsabilidad de cada una de las partes
    - Las normas técnicas y legales aplicables
    - Los requisitos de cifrado
    - El deber de secreto, incluso una vez finalizada la relación actual.
    - …

Controles asociados:

- 13.1.1 - Controles de red.
- 13.1.2 – Seguridad de los servicios de red.
- 13.1.3 - Segregación en redes.
- 13.2.1 - Políticas y procedimientos de intercambio de información.
- 13.2.2 - Acuerdos de intercambio.
- 13.2.3 - Mensajería electrónica.
- 13.2.4 - Acuerdos de confidencialidad

3.2.10. Adquisición, desarrollo y mantenimiento de los sistemas de información

El objetivo de este dominio es asegurar que los requisitos de los sistemas de información a desarrollar, a mejorar o que se van a adquirir son identificados y asegurar que la seguridad de la información es contemplada en todo el ciclo de vida de desarrollo de sistemas de información.

Tareas:

- Contemplar los distintos requisitos necesarios:
  - Necesidades del negocio.
  - Necesidades de seguridad, garantizando sus tres pilares básicos: confidencialidad, integridad y disponibilidad.
  - Controles de accesos, privilegios,…
  - Cumplimiento (legal, contractual,…)
  - Seguridad en la comunicación con terceros.
  - …
- Definir una política de desarrollo seguro, que contemple la seguridad en todo el ciclo de vida del desarrollo de software. Esta política, debe contemplar;
  - La metodología empleada
  - La seguridad en los distintos entornos (desarrollo, pruebas, integración, preproducción, producción, …)
  - Gestión del código fuente, por ejemplo con el uso de repositorios que gestionan tanto la seguridad (quien accede a qué y con qué permisos), como el versionado del software.
  - Análisis de riesgos asociado al software a desarrollar, que incluya por un lado las medidas a implementar en el propio desarrollo así como las medidas necesarias que garanticen que este se desarrolla en un entorno seguro.
  - Elaboración de código seguro en base a buenas prácticas y los estándares de la industria.
  - La necesidad de establecer un plan de pruebas que incluya no solo pruebas funcionales sino también pruebas de seguridad
  - Un sistema de aprobación para la inclusión de nuevas funcionalidades en el proceso de desarrollo.
  - …
- Aplicar los procesos definidos de gestión del cambio para las actualizaciones o instalaciones de nuevo software, que garanticen que se han realizado los cambios según las especificaciones, y que en caso contrario contemple un proceso de vuelta al punto anterior al cambio.

- Si se subcontratan desarrollos a terceras partes, identificar igualmente los requisitos necesarios y establecer los acuerdos contractuales y las cláusulas de confidencialidad necesarias que garanticen el cumplimiento de las políticas de seguridad durante todo el ciclo de vida de desarrollo, pudiendo incluso exigir auditorias de seguridad para confirmar su cumplimiento.
- Realizar revisiones periódicas de los privilegios establecidos sobre los repositorios.
- Al igual que ya se comentó en el punto 3.2.8, separar los entornos de desarrollo de los entornos productivos, garantizando que ni se transfieren usuarios y permisos de desarrollo a producción, ni se transfieren datos de producción a desarrollo. Para asegurar este punto es recomendable el uso de datos simulados en lugar de datos reales, o que al menos los daos utilizados no permitan identificar a una persona de manera inequívoca. En el caso de que sea necesario emplear datos reales, será necesario contar con la aprobación de los propietarios de dicha información y establecer las mismas medidas de seguridad aplicadas en el entorno productivo, como por ejemplo la firma de cláusulas de confidencialidad.
- Establecer controles adicionales si las comunicaciones con terceros se realizan mediante redes públicas (Internet), como por ejemplo:
    - Cifrado de los datos.
    - Uso de protocolos seguros.
    - Limitación de los datos a enviar.
    - Limitar los orígenes y destinos con acceso.
    - Establecer procedimientos que validen al tercero como autenticado (firma electrónica, factores múltiples de autenticación,…).
    - …

Controles asociados:

- 14.1.1 - Análisis de requisitos y especificaciones de Seguridad de la información.
- 14.1.2 - Securizar los servicios de aplicaciones en redes públicas.
- 14.1.3 - Protección de las transacciones de servicios de aplicaciones.
- 14.2.1 - Política de desarrollo seguro.
- 14.2.2 - Procedimiento de control de cambios en sistemas
- 14.2.3 - Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo
- 14.2.4 - Restricciones a los cambios en los paquetes de software
- 14.2.5 - Principios de ingeniería de sistemas seguros
- 14.2.6 - Entorno de desarrollo seguro

- 14.2.7 - Externalización del desarrollo de software
- 14.2.8 - Pruebas funcionales de seguridad
- 14.2.9 - Pruebas de aceptación de sistemas
- 14.3.1 - Protección de los datos de prueba

3.2.11. Relación con proveedores

El objetivo de este dominio es extender las medidas de seguridad necesarias a la cadena de proveedores de la organización para garantizar la eficacia de la misma, ya que estos podrán acceder a información de la empresa (y parte de esta puede ser incluso confidencial).

Tareas:

- Contemplar en el análisis de riesgos que se realice, los activos de información afectados por las relaciones con terceros y la información a la que tienen acceso (intentando siempre que sea la mínima necesaria) y analizar las amenazas derivadas de dicha situación.
- Incluir en los contratos con terceros, condiciones para la gestión segura de la información de la organización, en base a los requisitos definidos internamente. Incluir cláusulas de confidencialidad en los contratos. (tanto con proveedores como con clientes). Ejemplos de cláusulas que se pueden incluir en los contratos:
  - Derechos de auditoria: Que permitirá realizar auditorías de seguridad de manera periódica a los proveedores. O solicitar al propio proveedor la demostración de cumplimiento, presentando una evidencia irrefutable como por ejemplo el informe de una auditoria realizado por un tercero competente en la materia.
  - Notificación de incidentes: Garantizando que el proveedor comunicará a la organización, cualquier vulnerabilidad de su seguridad de la información que pueda afectar o afecte a información de la organización.
  - Cadena de suministro, garantizando que el proveedor exige a sus proveedores los mismos requisitos de seguridad.
  - Aceptación de las políticas y procedimientos definidas en la organización.
- Establecer los controles necesarios para mitigar los riesgos analizados, por ejemplo, analizar sus medidas de seguridad, evaluar sus antecedentes, situación financiera, planes de continuidad que disponga, certificaciones en materia de seguridad de las que disponga, auditorias de ciberseguridad a las que se someta, … Puede solicitar a sus proveedores información relacionada con sus procedimientos como, por ejemplo:
  - Procedimientos de contratación

  - Procedimientos de devolución o destrucción de la información a la finalización del acuerdo.
  - Planes de formación en seguridad de la información
  - Procedimientos de gestión de cambios
  - Procedimientos de gestión de incidencias
  - Planes de continuidad, de emergencia y de recuperación de desastres
  - …
- Si el proveedor accede físicamente a las instalaciones de la organización deberá quedar reflejado en los procedimientos y políticas de control de acceso definidas en el domino de “Seguridad física”.
- Definir los procedimientos necesarios para responder ante un incidente de seguridad de la información, e identificar los responsables que participen en dicho proceso, así como aquellas personas/departamentos/organismos que deban ser informados.
- Monitorizar de manera periódica el cumplimiento y la efectividad de los controles implementados.
- Hacer conocedor a los proveedores de los procedimientos y las políticas definidas en la organización. Por ejemplo, la gestión de incidentes de seguridad.
- Asegurarse de que la “cadena de seguridad de la información” se propaga a los proveedores de nuestros proveedores. Bien a través de los propios procesos de seguridad de nuestros proveedores, o bien por clausulas adicionales en los contratos de prestación de servicios.
- Establecer procesos que aseguran la información tras la prestación del servicio por parte de un proveedor, por ejemplo, estipulando la devolución de activos, la destrucción de información facilitada, y por supuesto revocando los posibles accesos al entorno de la organización habilitados durante la prestación del servicio.

Controles asociados:

- 15.1.1 - Política de seguridad de la información en relaciones con los proveedores.
- 15.1.2 - Requisitos de seguridad en contratos con terceros.
- 15.1.3 Cadena de suministro en tecnologías de la información y comunicaciones.
- 15.2.1 Supervisión y revisión de los servicios prestados por terceros.
- 15.2.2 Gestión de cambios en los servicios prestados por terceros.

3.2.12. Gestión de incidentes de seguridad de la información

El objetivo de este dominio es implementar medidas que permitan ofrecer una rápida detección y respuesta ante un incidente de seguridad de la información, es decir que afecte a la integridad, confidencialidad o disponibilidad de la información.

Para dar una respuesta apropiada a un incidente de seguridad, se deberían seguir los siguientes pasos:

Ilustración 9: Proceso de gestión de incidentes (18)

- Durante la fase de preparación, identificar a los responsables implicados y definir los procedimientos a seguir en caso de ocurrencia.
- En la fase de detección y análisis, se recopila la información disponible del incidente de las distintas fuentes disponibles, por un lado, aquella información que nos alerta de la existencia de un incidente (detección) y por otro, información que nos permita conocer con exactitud el problema y ayude a su resolución (análisis). En esta fase también cobra un papel importante la comunicación, es decir ¿Quién debe estar informado de incidente?, pensando no solo en personal interno sino también elementos externos como por ejemplo la Agencia Española de Protección de Datos en el caso de que el incidente implique datos personales.
- En la fase de Contención, resolución y recuperación se aplicarán las medidas necesarias para minimizar el alcance del incidente (contención), las medidas necesarias para eliminar el incidente (resolución) y las medidas necesarias para volver a la situación anterior al incidente (Recuperación).
- Por último, en las acciones posteriores al cierre, se realizarán tareas de análisis, para obtener información del incidente que ayude a protegerse frente a reincidencias del mismo o similares y evitar que dicha situación se repita.

Tareas:

- Definir los procedimientos necesarios para responder ante un incidente de seguridad de la información, e identificar los responsables que participen en dicho proceso, así como aquellas personas/departamentos/organismos que deban ser informados.
- Definir un procedimiento de gestión de incidentes que permita la clasificación y priorización de los mismos, y que este sea comunicado a toda la organización (por ejemplo, incluyéndolo en el plan de formación) y partes interesadas (por ejemplo, los proveedores)
- Establecer una herramienta de gestión de incidentes, que permita el registro de los mismos y centralizar toda la información recopilada que permita realizar análisis del mismo (tanto durante el incidente como a posteriori), y mantener informado a los implicados del estado del incidente. Este registro de incidentes nos permitirá utilizar la solución de incidentes anteriores como base de conocimiento para futuros eventos que se produzcan e incluso para entrenar al personal implicado para reducir los tiempos de resolución y minimizar el impacto.
- Establecer un adecuado procedimiento de recopilación de evidencias, hay que tener en cuenta que un incidente de seguridad puede desembocar en acciones legales, y como consecuencia es importante asegurar las evidencias recogidas durante el proceso de gestión del incidente.
- Definir un plan de comunicación ante incidentes.

Controles asociados:

- 16.1.1 - Responsabilidades y procedimientos.
- 16.1.2 - Notificación de los eventos de seguridad de la información.
- 16.1.3 - Notificación de puntos débiles de la seguridad.
- 16.1.4 - Evaluación y decisión sobre los eventos de seguridad de información.
- 16.1.5 - Respuesta a incidentes de seguridad de la información.
- 16.1.6 - Aprendizaje de los incidentes de seguridad de la información.
- 16.1.7 - Recopilación de evidencias.

3.2.13. Aspectos de seguridad de la información para la gestión de la continuidad del negocio

El objetivo de este dominio es garantizar, mediante la implantación de medidas concretas, que el negocio pueda seguir desempeñando su labor en caso de sufrir un incidente de seguridad y que la recuperación frente a dicho incidente se realice en el menor plazo de tiempo posible y con el menor impacto, manteniendo la Seguridad de la Información definida. Esto se consigue facilitando la toma de decisiones en situaciones de crisis al haber simulado situaciones similares y haber documentado las posibles soluciones y acciones a realizar por adelantado.

La función de un plan de continuidad es tener la capacidad de gestionar n incidente de seguridad de la información, recuperando los sistemas de información afectados manteniendo los niveles de seguridad de la información establecidos.

Tareas:

- El primer paso es identificar los riesgos que tengan impacto sobre los procesos críticos de la organización y definir planes de recuperación y actuación ante dichas situaciones, que sean acordes a la organización y sus recursos. En dichos planes se debe identifica a las personas responsables y el papel que van a desempeñar en los mismos.
- Establecer simulacros periódicos de los planes de recuperación anteriormente definidos, para:
  - Validar su eficacia
  - Garantizar que los implicados son conscientes de sus responsabilidades
  - Mejora de los mismos tras analizar los resultados del simulacro.
- Es muy importante contemplar la continuidad de la seguridad de la información, es decir los planes de continuidad y recuperación que se definan, deben incluir la recuperación y continuidad de los controles de seguridad necesarios y definidos por la organización.
- Implementar sistemas redundantes que garanticen la disponibilidad de los sistemas existentes que tengan mayor criticidad y que requieran que el tiempo de indisponibilidad tienda a cero, y probar periódicamente que dichos sistemas de redundancia aplicados funcionan, para asegurar que el día en que realmente vayan a ser necesarios realicen su función cuando el sistema principal sufra una contingencia o desastre.

Controles asociados:

- 17.1.1 - Planificación de la continuidad de seguridad de la información.
- 17.1.2 - Implementar la continuidad de la seguridad de la información.
- 17.1.3 - Pruebas, mantenimiento y reevaluación de los planes de continuidad del negocio.
- 17.2.1 - Disponibilidad de instalaciones de procesamiento de información.

3.2.14. Cumplimiento

El objetivo de este dominio es por un lado evitar incumplimientos legales, garantizando estatutos, regulaciones u obligaciones contractuales y de cualesquiera requisitos de seguridad de la información que apliquen a la organización, y por otro velar por que los procedimientos y políticas definidas son implementados y cumplidos por la organización.

Tareas:

- El primer paso es identificar todas aquellas legislaciones que sean de aplicación para la organización, forma de: leyes laborales, requisitos de seguridad relacionados con TI, derechos de propiedad intelectual y leyes de derechos de autor, privacidad, cifrado de datos y leyes de protección, … (como por ejemplo LOPD, RGPD, LSSI. LPI, Ley general de telecomunicaciones, leyes relativas al comercio electrónico, código penal, …) Este punto puede ser el más complejo, y podría ser conveniente la contratación de este servicio a empresas terceras especializadas que faciliten esta tarea.
- Asegurar que no se incumple con la ley de propiedad intelectual (LPI), mediante la implantación de políticas y normativas en relación al uso de elementos amparados por dicha ley. Un claro ejemplo es el uso de software comercial, para lo cual es recomendable mantener un registro de los activos amparados por LPI y llevar un registro de las licencias adquiridas y disponibles, controlando sus fechas de expiración y limitando la instalación de software no autorizado y controlado. Estas políticas deben ser comunicadas a toda la organización.
- Identificar los registros más críticos de la organización, como por ejemplo:
  - Registros financieros
  - Registros que definen estrategias comerciales.
  - Registros de patentes o diseños industriales.
  - Bases de datos
  - Código fuente de aplicaciones.
  - Registros de auditoria (propios del sistema de Gestión de la Seguridad de la información)

  - Procedimientos de la organización.
  - Archivos cifrados (contraseñas, firmas digitales), y cualquier elemento de cifra.
  - …
- Asegurar la protección de dichos registros, recordando que estos pueden ser tanto digitales como en formato papel. Esta medida va muy ligada al dominio 11, donde se hacía referencia a la protección de los equipos, copias de seguridad, establecimiento de periodos de retención, requisitos de almacenamiento, políticas de eliminación, …
- Asegurar que no se incumple con las distintas leyes en materia de protección de datos personales (LOPD, RGPD), para ello conviene mantener un registro que identifique aquellos elementos que soporten datos de carácter personal y asegurar la protección de todos aquellos elementos.
- Velar por el cumplimiento normativo en materia de controles criptográficos (por ejemplo, La ley de firma electrónica), este punto cobra especial atención en el caso de realizar exportaciones ya que los elementos criptológicos pueden estar sometidos a restricciones geográficas y tener restringido su uso en función del país. También se debe contemplar las necesidades de cifrado sobre ciertos tipos de dato, como puede ser lo establecido en la RGPD al tratar datos clasificados como sensibles: datos de origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, o la afiliación sindical, y el tratamiento de datos genéticos, datos biométricos dirigidos a identificar de manera unívoca a una persona física, datos relativos a la salud o datos relativos a la vida sexual o las orientación sexuales de una persona física. (19)
- Establecer un programa de auditorías internas en las cuales se revisan tanto los procedimientos/políticas definidas como los controles técnicos implantados, que garanticen que la seguridad de la información es implementada y operada de acuerdo con las políticas y procedimientos organizacionales. Es muy recomendable que dichas auditorias sean realizadas por personas que no hayan participado en la elaboración/implementación del elemento a auditar, para asegurar la imparcialidad, adicionalmente el proceso se puede contratar externamente en forma de:
  - Auditorías de cumplimiento: en el caso de tener ciertas condiciones contractuales o internas (por ejemplo certificarse en ISO 27001)
  - Auditorías documentales, que auditarán la documentación existente.
  - Auditorías procedimentales, que auditarán que se siguen los procedimientos definidos en la organización.

  - Auditorías técnicas, que auditarán desde un punto de vista técnico que los controles aplicados cumplen con su función.
  - …
- Asegurar el cumplimiento de todos los procedimientos/políticas son cumplidos por toda la organización. No obstante, si observan incumplimientos, sobre estos se deberá:
  - Identificar las posibles causas que provoquen el incumplimiento, cuyo origen puede sen ser deficiencias y debilidades del sistema.
  - Analizar posibles medidas que puedan corregir la situación.
  - Implementar las acciones y medidas tanto reparadoras como correctivas necesarias.
  - Revisar que estas acciones y medidas han cumplido su cometido.

Controles asociados:

- 18.1.1 Identificación de la legislación aplicable.
- 18.1.2 Derechos de propiedad intelectual (DPI).
- 18.1.3 Protección de los registros de la organización.
- 18.1.4 Protección de datos y privacidad de la información personal.
- 18.1.5 Regulación de los controles criptográficos.
- 18.2.1 Revisión independiente de la seguridad de la información.
- 18.2.2 Cumplimiento de las políticas y normas de seguridad.
- 18.2.3 Comprobación del cumplimiento

4. Conclusiones

Los objetivos de este trabajo se consideran superados al poder presentar al lector una visión del panorama actual en relación a las ciberamenazas existentes y como la pyme es uno de los objetivos claros para la ciberdelincuencia cuyo fin es puramente económico, dejando claro que el valor de la información de cada organización lo marca la propia organización, y como el uso de estándares reconocidos por la industria pueden ayudarnos a realizar esta tarea, consiguiendo así una guía que ayude a las Pymes a establecer sus propios controles de protección frente a las amenazas.

Es importante recordar que para poder cumplir con el objetivo de la seguridad en la pyme, es decir, garantizar la disponibilidad, integridad y la confidencialidad de la información, el establecimiento de la seguridad debe ser una meta en constante movimiento, ya que los propios ciberdelincuentes mejoran en sus técnicas de manera continua, y son más eficaces y avanzados cada día que pasa, por lo que para garantizar la seguridad de la información, es importante recordar que la seguridad no es algo que se mida sólo una vez sino que debe integrarse en un proceso de mejora continua, en el que se analizan necesidades, se implantan medidas, se revisan y se actualizan repitiendo una y otra vez este ciclo.

Como se ha podido observar a lo largo de los controles y medidas mostrados a lo largo de este trabajo, la seguridad no es un todo o nada, es una consecución de tareas que se van complementando para garantizar la seguridad de la información de la organización.

Si consultamos cualquier otra guía de ciberseguridad, marcos de trabajo de ciberseguridad, o mejores prácticas recomendadas por fabricantes y organizaciones del sector, como pueden ser NIST SP 800-53, COBIT, directrices de COSO,…, veremos controles y prácticas muy similares a las mostradas en este trabajo, ya que estas normas o marcos de referencia optan por una mentalidad de prevención donde se combinan procedimientos tanto técnicos como organizativos haciendo siempre referencia a elementos recogidos en la norma de referencia seguida y donde encontraremos acciones similares a las reflejadas en la norma ISO/IEC 27002:2013, donde se suelen destacar acciones como:

- La formación y concienciación de los empleados, como ya ha quedado indicado la mayor fuente de amenazas es el error humano.
- Proteger la información y aquellos activos que la almacenan, estableciendo medidas como la instalación de protecciones antimalware, políticas de actualización de equipos o de escritorio limpio, revisiones de vulnerabilidades, …
- Establecer seguridad perimetral, instalando un firewall que sirva como primera barrera de defensa previniendo accesos no autorizados desde el exterior.

- Establecer medidas para los dispositivos portátiles (móviles, tabletas, …)
- Realizar copias de seguridad, de manera regular que garanticen la continuidad del negocio en caso de incidente.
- Establecer medidas de seguridad física, que protejan los activos de accesos no autorizados, de robos o perdidas, limitar las cuentas con privilegios administrativos, …
- Establecer medidas para securizar las redes WIFI.
- Limitar y securizar los accesos a la información, asegurando de proporcionar a cada usuario acceso solo a la información necesaria para el desempeño de su trabajo.
- Establecer una política de contraseñas seguras, que contemple no solo la complejidad, sino también su caducidad, su deber de secreto, y establecer sistemas de múltiple factor de autenticación en la medida de lo posible.
- Documentar todas las políticas, normas, procedimientos y elementos que formen parte del plan de protección frente a amenazas definido.
- ...

En cuanto a las líneas de trabajo futuro, sería muy recomendable completar los tareas definidas, con las buenas prácticas y controles recogidos en la norma ISO/IEC 27032:2012, la cual, si bien define dominios distintos, como muestra el listado siguiente, la gran mayoría se integran y complementan a los presentados hasta ahora de la norma ISO/IEC 27002:2013, como se puede observar en el anexo recogido en el anexo 7.3 de este documento.

- Controles a nivel de aplicación: gestión de sesiones, cookies, revisiones de código, validación de datos, protección ante ataques, procesos de autenticación, etc.
- Protección de servidores: Incluye instalaciones y configuraciones seguras, gestión de parches y actualizaciones, monitorización, revisiones periódicas, copias de seguridad, etc.
- Controles de usuario final: Incluye actualizaciones de sistemas operativos, herramientas antimalware, protección del correo electrónico, gestión del uso de aplicaciones, herramientas y configuraciones de seguridad (como firewall personales), formación, etc.
- Controles frente a ataques de ingeniería social: Incluye programas de formación y concienciación a los usuarios.

Es importante resaltar que esta norma entra en un detalle más técnico y establece controles más específicos que lo recogido en la norma ISO/IEC 27002:2013, como por ejemplo todo el apartado 12.5 previniendo ataques de ingeniería social (aunque muchos controles ya han sido recogidos por la norma ISO/IEC 27002:2013) o el 12.6 Preparación para la Ciberseguridad, que hace mención a protecciones frente a la Darknet.

Por último, pensando desde un punto de vista práctico para una organización, si se han conseguido implementar estos controles y hemos conseguido los objetivos de seguridad marcados, puede ser un buen momento para plantearse la certificación bajo la norma ISO/IEC 27001:2013, ya que esta permite crear un marco de control de la seguridad basado en un sistema de gestión de seguridad de la información del que formaran parte todas las medidas técnicas y organizativas asociadas a los controles de la norma ISO/IEC 27002:2013, que han sido identificadas en este trabajo.

El hecho de certificarse puede mejorar la confianza y la reputación empresarial y puede ser un factor diferenciador frente a la competencia. Esta confianza no solo es hacia factores externos, con una clara visión comercial, si no también internamente dentro de la organización, ya que el mero hecho de analizar y gestionar los riesgos y aplicar controles en base a los mismos, nos va a permitir no sobredimensionar la inversión en seguridad. No obstante, el factor más importante para la organización debe ser que la organización dispondrá de un Sistema de Gestión de la Seguridad de la Información (SGSI), que le permitirá planificar, supervisar y por ende mejorar su nivel de seguridad de la información frente a las numerosas amenazas y riesgos existentes.

5. Glosario

Activo: algo que tiene valor para la organización.

Botnet: Es una red de máquinas infectadas (bots) y que se agrupan para realizar actividades maliciosas: Envío de SPAM, ataques de DDoS,…

Ciberamenaza: todo elemento o acción capaz de atentar contra la seguridad de la información.
Ciberataque: ataque realizado mediante el uso de tecnología con el fin de tomar el control, desestabilizar o dañar un sistema informático.

Ciberdelincuente: Persona que mediante el uso de tecnología comete delitos para lucrarse.

Ciberespacio: es un mundo virtual que contiene los entornos de internet, personas, organizaciones, actividades y toda clase de tecnología, dispositivos y redes interconectados entre sí (ISO/IEC 27032:2012)

Ciberespionaje: El acto de espionaje usando como medio Internet.

Ciberseguridad: Es la seguridad en un mundo digital-virtual, para prevenir los ciberataques que provienen de nuevas amenazas y riesgos

DoS: ataque que tiene como objetivo agotar los recursos de un sistema para que no estén disponibles para sus usuarios.

Hacker: Persona experta en el manejo de computadoras, que se ocupa de la seguridad de los sistemas y de desarrollar técnicas de mejora. (20)

Malware: Código malicioso que puede instalarse en un dispositivo y causar daños a los componentes de este.

Pharming: Con un objetivo similar al phising, dirigiendo peticiones contra sitios maliciosos, este ataque realiza una suplantación de servicios DNS, bien sea manipulando el fichero hosts de los equipos, o bien atacando a los propios servidores DNS.

Phishing: Un ataque que tiene como objetivo atraer a los usuarios a sitios maliciosos para robar de forma encubierta nombres de usuario, contraseñas y credenciales financieras.

Ransomware: malware que cifra los archivos de un equipo para pedir un rescate económico a cambio.

Spear Phising: Es una modalidad de phising cuyo objetivo es un perfil específico de alto nivel en la empresa.

Spyware: Es un tipo específico de malware, que captura y monitoriza los movimientos del usuario en un equipo informático, y que posteriormente envía los datos recopilados a un tercero (sin consentimiento del propietario de los mismos).

SCAM: Del inglés, estafa. Comúnmente se utiliza para referirse a estafas en las cuales se emplean medios electrónicos.

SPAM: Correo electrónico no deseado ni solicitado, que comúnmente es enviado masivamente con una finalidad económica.

Vulnerabilidad: Debilidad en un activo que lo hace susceptible de ser atacado

6. Bibliografía

1. **Widup, Suzanne, y otros.** *2018 Verizon Data Breach Investigations Report.* 2018.

2. **Cobb, Stephen.** WeLiveSecurity. [En línea] 4 de 5 de 2015. [Citado el: 24 de 03 de 2019.] WeliveSecurityhttps://www.welivesecurity.com/2015/05/04/national-small-business-week-cybersecurity-survival-guide/.

3. **INCIBE.** Instit¡uto Nacional de Ciberseguridad. [En línea] 02 de 03 de 2018. [Citado el: 29 de 03 de 2019.] https://www.incibe.es/sala-prensa/notas-prensa/incibe-resuelve-mas-123000-incidentes-ciberseguridad-2017.

4. **Hiscox España.** Informe Hiscox-Siniestralidad cibernética 2018. [En línea] 09 de 2018. [Citado el: 10 de 04 de 2019.] https://www.hiscox.es/documentos/Informe-hiscox-siniestralidad-cibernetica.pdf.

5. **Cisco Systems, Inc.** *CISCO CYBERSECURITY SPECIAL REPORT.* San Jose, CA : s.n., 2018.

6. **Federal Bureau of Investigation.** Federal Bureau of Investigation (FBI). [En línea] 1 de 3 de 2012. [Citado el: 11 de 4 de 2019.] https://archives.fbi.gov/archives/news/speeches/combating-threats-in-the-cyber-world-outsmarting-terrorists-hackers-and-spies.

7. **Chambers, John.** World Economic Forum. [En línea] 21 de 1 de 2015. [Citado el: 31 de 5 de 2019.] https://www.weforum.org/agenda/2015/01/companies-fighting-cyber-crime/.

8. **Mar, Rosana en.** Centro de Prensa de ESET España. [En línea] 10 de 02 de 2018. [Citado el: 05 de 31 de 2019.] https://noticias.eset.es/chema-alonso-chief-data-officer-de-telefonica-no-existe-una-empresa-100%25-segura-frente-a-la-ciberdelincuencia.

9. **ENISA.** The European Union Agency for Network and Information Security . [En línea] 28 de 01 de 2019. [Citado el: 07 de 04 de 2019.] https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2018.

10. **Instituo AV-TEST GmbH.** Instituo AV-TEST GmbH. [En línea] 2019. [Citado el: 08 de 04 de 2019.] https://www.av-test.org/en/statistics/malware/.

11. **Malwarebytes.** *Cybercrime tactics and techniques Q1 2017.* Santa Clara, CA : s.n., 2017.

12. **EUROPOL.** *INTERNET ORGANISED CRIME THREAT ASSESSMENT (IOCTA) 2018.* The Hague : European Union Agency for Law Enforcement Cooperation 2018, 2018. ISBN 978-92-95200-94-4.

13. **CVEDetails.** Security Vulnerabilities Published In 2018. [En línea] [Citado el: 24 de 03 de 2019.] https://www.cvedetails.com/vulnerability-list/year-2018/vulnerabilities.html.

14. **PwC.** PwC España. [En línea] [Citado el: 31 de 05 de 2019.] https://www.pwc.es/es/digital/encuesta-mundial-ciberseguridad-2018.html.

15. **International Organization for Standardization.** *Information technology — Security techniques — Information security management systems — Overview and vocabulary.* Geneva : ISO copyright office, 2014. ISO/IEC 27000:2014(E).

16. **comité técnico AEN/CTN 71Tecnología de la información.** *ISO/IEC 27001:2013: Tecnología de la información. Técnicas de seguridad. Sistemas de Gestión de Seguridad de la Información (SGSI). Requisitos.* Madrid : AENOR, 2014.

17. **Mañas, José A.** *Centro Criptológico Nacional.* s.l. : Ministerio de la presidencia. Gobierno de España, 2013.

18. **INCIBE.** Instituto Nacional de Ciberseguridad. [En línea] 12 de 12 de 2016. [Citado el: 16 de 05 de 2019.] https://www.incibe.es/protege-tu-empresa/blog/estas-preparado-hacer-frente-ciberincidente.

19. **Diario Oficial de la Unión Europea.** Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo. *Agencia Estatal Boletín Oficial del Estado.* [En línea] 4 de 5 de 2016. [Citado el: 17 de 05 de 2019.] https://www.boe.es/doue/2016/119/L00001-00088.pdf.

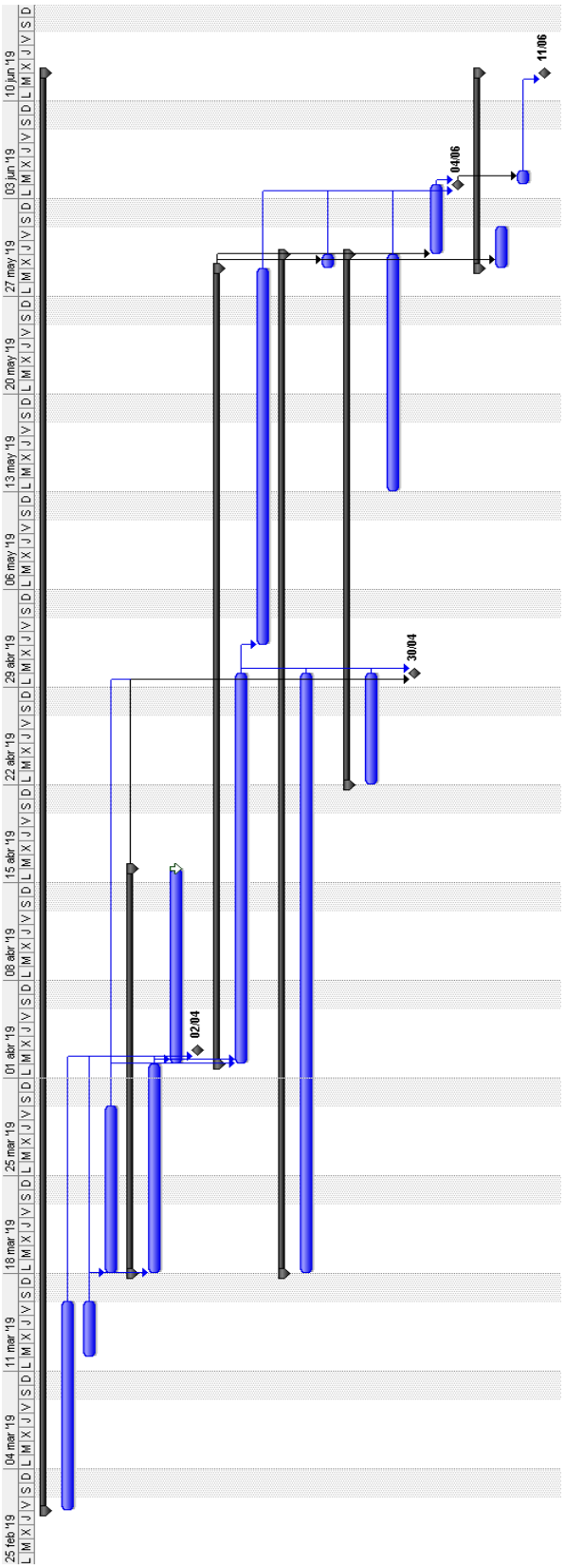
20. **Real Academia de la Lengua.** Diccionario de la lengua española. [En línea] Real Academia de la Lengua. [Citado el: 31 de 05 de 2019.] https://dle.rae.es.

21. **Panda Security.** 2017 en cifras. *2017 en cifras.* [En línea] Panda Security, 4 de 01 de 2018. [Citado el: 29 de 03 de 2019.] https://www.pandasecurity.com/spain/mediacenter/malware/2017-en-cifras/.

22. **Panda Security;.** Panda Security. *27% of all recorded malware appeared in 2015.* [En línea] Panda Security, 25 de 01 de 2016. [Citado el: 29 de 03 de 2019.] https://www.pandasecurity.com/mediacenter/press-releases/all-recorded-malware-appeared-in-2015/.

7. Anexos

7.1. Planificación



7.2. Lista de controles ISO/IEC 27002:2013

5. POLÍTICAS DE SEGURIDAD.
5.1 Directrices de la Dirección en seguridad de la información.
5.1.1 Conjunto de políticas para la seguridad de la información.
5.1.2 Revisión de las políticas para la seguridad de la información.
6. ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMAC.
6.1 Organización interna.
6.1.1 Asignación de responsabilidades para la segur. de la información.
6.1.2 Segregación de tareas.
6.1.3 Contacto con las autoridades.
6.1.4 Contacto con grupos de interés especial.
6.1.5 Seguridad de la información en la gestión de proyectos.
6.2 Dispositivos para movilidad y teletrabajo.
6.2.1 Política de uso de dispositivos para movilidad.
6.2.2 Teletrabajo.
7. SEGURIDAD LIGADA A LOS RECURSOS HUMANOS.
7.1 Antes de la contratación.
7.1.1 Investigación de antecedentes.
7.1.2 Términos y condiciones de contratación.
7.2 Durante la contratación.
7.2.1 Responsabilidades de gestión.
7.2.2 Concienciación, educación y capacitación en seguridad de la información.
7.2.3 Proceso disciplinario.
7.3 Cese o cambio de puesto de trabajo.
7.3.1 Cese o cambio de puesto de trabajo.
8. GESTIÓN DE ACTIVOS.
8.1 Responsabilidad sobre los activos.
8.1.1 Inventario de activos.
8.1.2 Propiedad de los activos.
8.1.3 Uso aceptable de los activos.
8.1.4 Devolución de activos.
8.2 Clasificación de la información.
8.2.1 Directrices de clasificación.
8.2.2 Etiquetado y manipulado de la información.
8.2.3 Manipulación de activos.
8.3 Manejo de los soportes de almacenamiento.
8.3.1 Gestión de soportes extraíbles.
8.3.2 Eliminación de soportes.
8.3.3 Soportes físicos en tránsito.
9. CONTROL DE ACCESOS.
9.1 Requisitos de negocio para el control de accesos.
9.1.1 Política de control de accesos.
9.1.2 Control de acceso a las redes y servicios asociados.
9.2 Gestión de acceso de usuario.
9.2.1 Gestión de altas/bajas en el registro de usuarios.
9.2.2 Gestión de los derechos de acceso asignados a usuarios.
9.2.3 Gestión de los derechos de acceso con privilegios especiales.
9.2.4 Gestión de información confidencial de autenticación de usuarios.

9.2.5 Revisión de los derechos de acceso de los usuarios.
9.2.6 Retirada o adaptación de los derechos de acceso
9.3 Responsabilidades del usuario.
9.3.1 Uso de información confidencial para la autenticación.
9.4 Control de acceso a sistemas y aplicaciones.
9.4.1 Restricción del acceso a la información.
9.4.2 Procedimientos seguros de inicio de sesión.
9.4.3 Gestión de contraseñas de usuario.
9.4.4 Uso de herramientas de administración de sistemas.
9.4.5 Control de acceso al código fuente de los programas.
10. CIFRADO.
10.1 Controles criptográficos.
10.1.1 Política de uso de los controles criptográficos.
10.1.2 Gestión de claves.
11. SEGURIDAD FÍSICA Y AMBIENTAL.
11.1 Áreas seguras.
11.1.1 Perímetro de seguridad física.
11.1.2 Controles físicos de entrada.
11.1.3 Seguridad de oficinas, despachos y recursos.
11.1.4 Protección contra las amenazas externas y ambientales.
11.1.5 El trabajo en áreas seguras.
11.1.6 Áreas de acceso público, carga y descarga.
11.2 Seguridad de los equipos.
11.2.1 Emplazamiento y protección de equipos.
11.2.2 Instalaciones de suministro.
11.2.3 Seguridad del cableado.
11.2.4 Mantenimiento de los equipos.
11.2.5 Salida de activos fuera de las dependencias de la empresa.
11.2.6 Seguridad de los equipos y activos fuera de las instalaciones.
11.2.7 Reutilización o retirada segura de dispositivos de almacenamiento.
11.2.8 Equipo informático de usuario desatendido.
11.2.9 Política de puesto de trabajo despejado y bloqueo de pantalla.
12. SEGURIDAD EN LA OPERATIVA.
12.1 Responsabilidades y procedimientos de operación.
12.1.1 Documentación de procedimientos de operación.
12.1.2 Gestión de cambios.
12.1.3 Gestión de capacidades.
12.1.4 Separación de entornos de desarrollo, prueba y producción.
12.2 Protección contra código malicioso.
12.2.1 Controles contra el código malicioso.
12.3 Copias de seguridad.
12.3.1 Copias de seguridad de la información.
12.4 Registro de actividad y supervisión.
12.4.1 Registro y gestión de eventos de actividad.
12.4.2 Protección de los registros de información.
12.4.3 Registros de actividad del administrador y operador del sistema.
12.4.4 Sincronización de relojes.
12.5 Control del software en explotación.
12.5.1 Instalación del software en sistemas en producción.
12.6 Gestión de la vulnerabilidad técnica.

12.6.1 Gestión de las vulnerabilidades técnicas.
12.6.2 Restricciones en la instalación de software.
12.7 Consideraciones de las auditorías de los sistemas de información.
12.7.1 Controles de auditoría de los sistemas de información.
13. SEGURIDAD EN LAS TELECOMUNICACIONES.
13.1 Gestión de la seguridad en las redes.
13.1.1 Controles de red.
13.1.2 Mecanismos de seguridad asociados a servicios en red.
13.1.3 Segregación de redes.
13.2 Intercambio de información con partes externas.
13.2.1 Políticas y procedimientos de intercambio de información.
13.2.2 Acuerdos de intercambio.
13.2.3 Mensajería electrónica.
13.2.4 Acuerdos de confidencialidad y secreto.
14. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN.
14.1 Requisitos de seguridad de los sistemas de información.
14.1.1 Análisis y especificación de los requisitos de seguridad.
14.1.2 Seguridad de las comunicaciones en servicios accesibles por redes públicas.
14.1.3 Protección de las transacciones por redes telemáticas.
14.2 Seguridad en los procesos de desarrollo y soporte.
14.2.1 Política de desarrollo seguro de software.
14.2.2 Procedimientos de control de cambios en los sistemas.
14.2.3 Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo.
14.2.4 Restricciones a los cambios en los paquetes de software.
14.2.5 Uso de principios de ingeniería en protección de sistemas.
14.2.6 Seguridad en entornos de desarrollo.
14.2.7 Externalización del desarrollo de software.
14.2.8 Pruebas de funcionalidad durante el desarrollo de los sistemas.
14.2.9 Pruebas de aceptación.
14.3 Datos de prueba.
14.3.1 Protección de los datos utilizados en pruebas.
15. RELACIONES CON SUMINISTRADORES.
15.1 Seguridad de la información en las relaciones con suministradores.
15.1.1 Política de seguridad de la información para suministradores.
15.1.2 Tratamiento del riesgo dentro de acuerdos de suministradores.
15.1.3 Cadena de suministro en tecnologías de la información y comunicaciones.
15.2 Gestión de la prestación del servicio por suministradores.
15.2.1 Supervisión y revisión de los servicios prestados por terceros.
15.2.2 Gestión de cambios en los servicios prestados por terceros.
16. GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN.
16.1 Gestión de incidentes de seguridad de la información y mejoras.
16.1.1 Responsabilidades y procedimientos.
16.1.2 Notificación de los eventos de seguridad de la información.
16.1.3 Notificación de puntos débiles de la seguridad.
16.1.4 Valoración de eventos de seguridad de la información y toma de decisiones.
16.1.5 Respuesta a los incidentes de seguridad.
16.1.6 Aprendizaje de los incidentes de seguridad de la información.
16.1.7 Recopilación de evidencias.

17. ASPECTOS DE SEGURIDAD DE LA INFORMACION EN LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO.
17.1 Continuidad de la seguridad de la información.
17.1.1 Planificación de la continuidad de la seguridad de la información.
17.1.2 Implantación de la continuidad de la seguridad de la información.
17.1.3 Verificación, revisión y evaluación de la continuidad de la seguridad de la información.
17.2 Redundancias.
17.2.1 Disponibilidad de instalaciones para el procesamiento de la información.
18. CUMPLIMIENTO.
18.1 Cumplimiento de los requisitos legales y contractuales.
18.1.1 Identificación de la legislación aplicable.
18.1.2 Derechos de propiedad intelectual (DPI).
18.1.3 Protección de los registros de la organización.
18.1.4 Protección de datos y privacidad de la información personal.
18.1.5 Regulación de los controles criptográficos.
18.2 Revisiones de la seguridad de la información.
18.2.1 Revisión independiente de la seguridad de la información.
18.2.2 Cumplimiento de las políticas y normas de seguridad.
18.2.3 Comprobación del cumplimiento

7.3. Correspondencia entre la normas ISO/IEC 27002:2013 y ISO/IEC 27032:2012

La siguiente tabla recoge la relación entre los distintos controles de la norma ISO/IEC 27002:2013 y las recomendaciones presentadas en la norma ISO/IEC 27032:2012.

Controles ISO/IEC 27002:2013	**Recomendaciones ISO/IEC 27032:2012**
5. POLÍTICAS DE SEGURIDAD.	
5.1 Directrices de la Dirección en seguridad de la información.	
5.1.1 Conjunto de políticas para la seguridad de la información.	12.5.2
5.1.2 Revisión de las políticas para la seguridad de la información.	
6. ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMAC.	
6.1 Organización interna.	
6.1.1 Asignación de responsabilidades para la segur. de la información.	
6.1.2 Segregación de tareas.	
6.1.3 Contacto con las autoridades.	12.5.3.2 y 13.4.2
6.1.4 Contacto con grupos de interés especial.	13.4.2 y 13.4.3
6.1.5 Seguridad de la información en la gestión de proyectos.	
6.2 Dispositivos para movilidad y teletrabajo.	
6.2.1 Política de uso de dispositivos para movilidad.	
6.2.2 Teletrabajo.	
7. SEGURIDAD LIGADA A LOS RECURSOS HUMANOS.	
7.1 Antes de la contratación.	
7.1.1 Investigación de antecedentes.	
7.1.2 Términos y condiciones de contratación.	
7.2 Durante la contratación.	
7.2.1 Responsabilidades de gestión.	12.2.1
7.2.2 Concienciación, educación y capacitación en seguridad de la información.	12.5.3.2 y 12.5.4
7.2.3 Proceso disciplinario.	12.5.2
7.3 Cese o cambio de puesto de trabajo.	
7.3.1 Cese o cambio de puesto de trabajo.	
8. GESTIÓN DE ACTIVOS.	
8.1 Responsabilidad sobre los activos.	
8.1.1 Inventario de activos.	13.2.1, 13.2.2, 13.2.3 y 13.2.4
8.1.2 Propiedad de los activos.	
8.1.3 Uso aceptable de los activos.	
8.1.4 Devolución de activos.	
8.2 Clasificación de la información.	
8.2.1 Directrices de clasificación.	12.5.3.1, 13.2.1, 13.2.2 y 13.2.3
8.2.2 Etiquetado y manipulado de la información.	12.5.3.1

8.2.3 Manipulación de activos.	12.5.3.1
8.3 Manejo de los soportes de almacenamiento.	
8.3.1 Gestión de soportes extraíbles.	
8.3.2 Eliminación de soportes.	
8.3.3 Soportes físicos en tránsito.	
9. CONTROL DE ACCESOS.	
9.1 Requisitos de negocio para el control de accesos.	
9.1.1 Política de control de accesos.	
9.1.2 Control de acceso a las redes y servicios asociados.	
9.2 Gestión de acceso de usuario.	
9.2.1 Gestión de altas/bajas en el registro de usuarios.	
9.2.2 Gestión de los derechos de acceso asignados a usuarios.	12.5.5.a
9.2.3 Gestión de los derechos de acceso con privilegios especiales.	
9.2.4 Gestión de información confidencial de autenticación de usuarios.	
9.2.5 Revisión de los derechos de acceso de los usuarios.	
9.2.6 Retirada o adaptación de los derechos de acceso	
9.3 Responsabilidades del usuario.	
9.3.1 Uso de información confidencial para la autenticación.	
9.4 Control de acceso a sistemas y aplicaciones.	
9.4.1 Restricción del acceso a la información.	13.2.1
9.4.2 Procedimientos seguros de inicio de sesión.	
9.4.3 Gestión de contraseñas de usuario.	
9.4.4 Uso de herramientas de administración de sistemas.	
9.4.5 Control de acceso al código fuente de los programas.	
10. CIFRADO.	
10.1 Controles criptográficos.	
10.1.1 Política de uso de los controles criptográficos.	12.5.5.a , 12.5.5.5.b, 13.2.5 y 13.5.4
10.1.2 Gestión de claves.	13.5.4
11. SEGURIDAD FÍSICA Y AMBIENTAL.	
11.1 Áreas seguras.	
11.1.1 Perímetro de seguridad física.	
11.1.2 Controles físicos de entrada.	
11.1.3 Seguridad de oficinas, despachos y recursos.	
11.1.4 Protección contra las amenazas externas y ambientales.	
11.1.5 El trabajo en áreas seguras.	
11.1.6 Áreas de acceso público, carga y descarga.	
11.2 Seguridad de los equipos.	

11.2.1 Emplazamiento y protección de equipos.	
11.2.2 Instalaciones de suministro.	
11.2.3 Seguridad del cableado.	
11.2.4 Mantenimiento de los equipos.	
11.2.5 Salida de activos fuera de las dependencias de la empresa.	
11.2.6 Seguridad de los equipos y activos fuera de las instalaciones.	
11.2.7 Reutilización o retirada segura de dispositivos de almacenamiento.	
11.2.8 Equipo informático de usuario desatendido.	
11.2.9 Política de puesto de trabajo despejado y bloqueo de pantalla.	
12. SEGURIDAD EN LA OPERATIVA.	
12.1 Responsabilidades y procedimientos de operación.	
12.1.1 Documentación de procedimientos de operación.	
12.1.2 Gestión de cambios.	
12.1.3 Gestión de capacidades.	
12.1.4 Separación de entornos de desarrollo, prueba y producción.	
12.2 Protección contra código malicioso.	
12.2.1 Controles contra el código malicioso.	9.4.2, 12.3.e, 12.4.a, 12.4.c, 12.4.d, 12.4.g y 12.4.h
12.3 Copias de seguridad.	
12.3.1 Copias de seguridad de la información.	
12.4 Registro de actividad y supervisión.	
12.4.1 Registro y gestión de eventos de actividad.	12.3.c y 12.6
12.4.2 Protección de los registros de información.	
12.4.3 Registros de actividad del administrador y operador del sistema.	
12.4.4 Sincronización de relojes.	
12.5 Control del software en explotación.	
12.5.1 Instalación del software en sistemas en producción.	12.5.5.c
12.6 Gestión de la vulnerabilidad técnica.	
12.6.1 Gestión de las vulnerabilidades técnicas.	12.3.b y 12.5.5.c
12.6.2 Restricciones en la instalación de software.	
12.7 Consideraciones de las auditorías de los sistemas de información.	
12.7.1 Controles de auditoría de los sistemas de información.	
13. SEGURIDAD EN LAS TELECOMUNICACIONES.	
13.1 Gestión de la seguridad en las redes.	
13.1.1 Controles de red.	12.6
13.1.2 Mecanismos de seguridad asociados a servicios en red.	12.5.5.b
13.1.3 Segregación de redes.	

13.2 Intercambio de información con partes externas.	
13.2.1 Políticas y procedimientos de intercambio de información.	12.2.a y 13.3.4
13.2.2 Acuerdos de intercambio.	13.2.1, 13.2.2, 13.2.5 y 13.3.3
13.2.3 Mensajería electrónica.	13.3.3 y 12.5.5
13.2.4 Acuerdos de confidencialidad y secreto.	12.5.3.1 y 13.3.3
14. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN.	
14.1 Requisitos de seguridad de los sistemas de información.	
14.1.1 Análisis y especificación de los requisitos de seguridad.	12.3.a y 12.5.5.a
14.1.2 Seguridad de las comunicaciones en servicios accesibles por redes públicas.	12.2.f y 12.5.5.b
14.1.3 Protección de las transacciones por redes telemáticas.	12.5.5.b
14.2 Seguridad en los procesos de desarrollo y soporte.	
14.2.1 Política de desarrollo seguro de software.	
14.2.2 Procedimientos de control de cambios en los sistemas.	12.3.b y 12.4.b
14.2.3 Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo.	
14.2.4 Restricciones a los cambios en los paquetes de software.	12.3.b
14.2.5 Uso de principios de ingeniería en protección de sistemas.	
14.2.6 Seguridad en entornos de desarrollo.	
14.2.7 Externalización del desarrollo de software.	
14.2.8 Pruebas de funcionalidad durante el desarrollo de los sistemas.	12.2.e
14.2.9 Pruebas de aceptación.	
14.3 Datos de prueba.	
14.3.1 Protección de los datos utilizados en pruebas.	
15. RELACIONES CON SUMINISTRADORES.	
15.1 Seguridad de la información en las relaciones con suministradores.	
15.1.1 Política de seguridad de la información para suministradores.	13.3.3, 13.4.2 y 13.4.4
15.1.2 Tratamiento del riesgo dentro de acuerdos de suministradores.	
15.1.3 Cadena de suministro en tecnologías de la información y comunicaciones.	
15.2 Gestión de la prestación del servicio por suministradores.	
15.2.1 Supervisión y revisión de los servicios prestados por terceros.	13.3.6
15.2.2 Gestión de cambios en los servicios prestados por terceros.	

16. GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN.	
16.1 Gestión de incidentes de seguridad de la información y mejoras.	
16.1.1 Responsabilidades y procedimientos.	13.3.5 y 13.4.2
16.1.2 Notificación de los eventos de seguridad de la información.	
16.1.3 Notificación de puntos débiles de la seguridad.	
16.1.4 Valoración de eventos de seguridad de la información y toma de decisiones.	
16.1.5 Respuesta a los incidentes de seguridad.	
16.1.6 Aprendizaje de los incidentes de seguridad de la información.	13.4.4
16.1.7 Recopilación de evidencias.	
17. ASPECTOS DE SEGURIDAD DE LA INFORMACION EN LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO.	
17.1 Continuidad de la seguridad de la información.	
17.1.1 Planificación de la continuidad de la seguridad de la información.	
17.1.2 Implantación de la continuidad de la seguridad de la información.	
17.1.3 Verificación, revisión y evaluación de la continuidad de la seguridad de la información.	
17.2 Redundancias.	
17.2.1 Disponibilidad de instalaciones para el procesamiento de la información.	
18. CUMPLIMIENTO.	
18.1 Cumplimiento de los requisitos legales y contractuales.	
18.1.1 Identificación de la legislación aplicable.	
18.1.2 Derechos de propiedad intelectual (DPI).	12.5.3.1
18.1.3 Protección de los registros de la organización.	
18.1.4 Protección de datos y privacidad de la información personal.	12.5.3.1
18.1.5 Regulación de los controles criptográficos.	
18.2 Revisiones de la seguridad de la información.	
18.2.1 Revisión independiente de la seguridad de la información.	
18.2.2 Cumplimiento de las políticas y normas de seguridad.	
18.2.3 Comprobación del cumplimiento	12.2.d, 12.2.e, 12.3.f, 12.3.g y 12.3.h