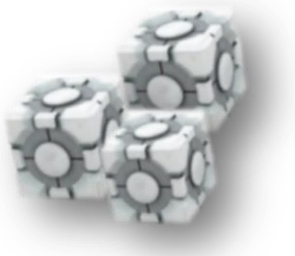
# GUÍA DE CONTROLES DE CIBERSEGURIDAD PARA LA PROTECCIÓN INTEGRAL DE LA PYME

Diciembre 2017



**Trabajo Fin de Máster**

Antonio Oliván Huerva

ESTA PÁGINA SE DEJÓ INTENCIONADAMENTE EN BLANCO

TRABAJO FIN DE MASTER

# Guía de controles de ciberseguridad para la protección integral de la PYME

---

*©Antonio Oliván Huerva*
*Diciembre 2017*

Tutor: Marco Antonio Lozano Merino
Campo de aplicación: TFM-Ad hoc
Máster Interuniversitario en Seguridad de las Tecnologías de la Información y de las Comunicaciones (MISTIC)
UOC / UAB / URV / UIB

*© Antonio Oliván Huerva, 2017*

***NOTA**: Este documento no puede ser copiado sin la previa autorización escrita del autor.*

# Índice

**1. Introducción ..... 1**

**2. Objetivos ..... 2**

2.1. Metodología ..... 2

**3. Planificación ..... 4**

3.1. Tareas ..... 4

3.2. Planificación de las Tareas ..... 5

**4. Normativas, guías y estándares ..... 6**

4.1. ISO 27001:2013 ..... 6

4.2. COBIT ..... 8

4.3. NIST SP 800-53 ..... 9

**5. Gestión de Riesgos ..... 10**

5.1. Análisis de riesgos ..... 10

5.2. Elementos del análisis ..... 11

5.3. Resultado de los análisis ..... 12

5.4. Ataques informáticos habituales recibidos por las PYME ..... 13

5.5. Ciberseguros para PYME ..... 15

**6. General Data Protection Regulation (GDPR) ..... 16**

6.1. Niveles de seguridad de protección según el Real Decreto 1720/2007 ..... 16

6.2. Relación entre la GDPR y la ISO/IEC 27002:2013 ..... 18

**7. Guía de controles de fácil implantación (ISO27K) ..... 40**

7.1. Declaración de Aplicabilidad (DdA) ..... 40

7.2. Guía de controles para PYME ..... 41

**8. Aplicación de la guía (supuesto ficticio) ..... 66**

8.1. Organigrama de la empresa ..... 67

8.2. Instalaciones ..... 69

8.3. Equipamiento informático (hardware / software) ..... 71

8.4. Aplicación de los controles para *Ibones de Aragón S.L.* ..... 72

**9. Conclusiones ..... 99**

9.1. Trabajo futuro ..... 99

**10. Referencias ..... 100**

**11. Anexos ..... 103**

11.1. Acrónimos ..... 103

11.2. REF-05-01.1 – Política de seguridad ..... 105
11.3. REF-06-01.1 – Roles y responsabilidades ..... 108
11.4. REF-06-01.3 – Lista de contactos ..... 109
11.5. REF-07-01.2 – Acuerdo de confidencialidad y no divulgación ..... 110
11.6. REF-07-02.2 – Calendario de cursos de seguridad ..... 112
11.7. REF-08-02.1 – Clasificación de la información ..... 113
11.8. REF-11-01.2 – Acceso a las instalaciones ..... 114
11.9. Lista de controles ISO/IEC 27002:2013 ..... 115

# 1. Introducción

*Las PYME necesitan proteger su información. ¿Qué debo tener en cuenta?*

La relevancia de los servicios TIC en todo el mundo es incuestionable. Las PYME no son ajenas ni mucho menos. Para el desarrollo de sus negocios,las PYME requieren de dichos servicios para el soporte de sus actividades inherentes al negocio. Desafortunadamente, se ven afectadas por todo tipo de ataques a sus sistemas informáticos: malware, spam, phising, ransomware, etc. Aunque no existe la posibilidad de ser 100% seguros, deben poner todo el esfuerzo en conseguir una máxima protección de sus activos. Para lograr este objetivo, conviene identificar una serie de controles específicos para la seguridad TIC.

Existen varias normas, estándares o guías vigentes que cubren muchos aspectos de ciberseguridad. El problema surge a la hora de aplicar alguna de ellas debido a que las PYME no suelen disponer de un presupuesto o conocimiento para aplicarlo. Se recomienda pues, proporcionar una guía de controles defácil implantación en una PYME.

La serie de normas ISO/IEC 27000 podría ser una solución. Es una referencia mundial y permite una certificación a partir de ISO27001:2013 [1]. Ahora bien, La ISO 27002 dispone de una cantidad enorme de controles por lo que las empresas se pueden ver desbordadas.Afortunadamente, la ISO27001 es aplicable a cualquier tipo de organización independientemente de su tamaño. Se permite que la organización aplique todo aquello que sea necesario una vez realizado un análisis de riesgos. Es decir, la organización podrá realizar una selección de aquellos controles que considere oportunos y descartar los que no necesite [12].

| **ISO/IEC 27001 (2013)** |
|---|
| 14 Dominios |
| 35Objetivos de control |
| 114 Controles |

Gracias a la aplicación de los controles, se podría implantar un Sistema de Gestion de Seguridad de la Información (SGSI) cuyos beneficios son múltiples para cualquier organización. Entre otros:

- Cumplimiento de la ley vigente
- Mejora de la imagen corporativa
- Publicidad positiva
- Continuidad de negocio
- Optimización de recursos y costes
- Compromiso con la mejora continua

Por otra parte, conviene recordar que la regulación europea,General Data Protection Regulation (GDPR) entrará en vigor a partir de Mayo de 2018[6]. Esta ley reemplaza la Directiva 95/46/EC sobre la protección de los individuos con respecto al procesamiento de los datos personales y la libre circulación de dichos datos [7]. Toda organización estaobligada a adaptar su infraestructura a la nueva ley. En caso de no cumplirla, podría ser penalizada con unas multas muy elevadas, hasta un máximo de 20 millones de euros o hasta un 4% del volumen de negocio anual de la empresa que no cumpla con los requisitos legales.

# 2. Objetivos

*¿Cómo puedo llevar a cabo el trabajo?*

El objetivo de este TFM es proporcionar una guía de controles de ciberseguridad de fácil implantación en una PYME. Teniendo en cuenta que existen diversas normas, conviene conocer la lista de controles más importantes para después seleccionar aquella que pueda ser más interesante a la organización. A tal efecto se propone seguir la serie de normas ISO/IEC 27000. Como se puede observar en los siguientes apartados, la ISO27002 dispone de una cantidad notable de controles de los cuales se realizará una selección de aquellos más fácilmente aplicables a una PYME.

El punto de partida es mostrar la relevancia de la gestión de riesgos como pilar fundamental para el control de la seguridad de todo tipo de organización. Seguidamente se pone énfasis en la la regulación GDPR que debe ser tenida en consideración por todo tipo de organización a partir de mayo de 2018 a riesgo de recibir penalizaciones en caso de no aplicarse.

Igualmente es preciso apuntar que el coste de la implantación de la ISO27001 depende de muchos factores y que pueden determinar la elección de algunos controles:

- Tamaño de la organización (en nuestro caso PYME)
- Legislación o normativas (entre otras la GDPR)
- Madurez organizativa de la misma (¿dispone ya de alguna certificación, estándar, etc?)
- Tipo de información que gestiona la compañía (¿es una empresa del sector médico? ¿sector educativo?)
- Equipo especialmente dedicado a la gestión de la seguridad informática
- Infraestructura de la organización (¿se dispone de alguna herramienta que ayude a su implantación?)

## 2.1. Metodología

Inicialmente se presenta un pequeño estado del arte en cuanto a las normas más ampliamente utilizadas:

- Familia de estándares ISO/IEC 27000 [1]: tiene un número más o menos limitado de controles, su estandar 27001 es certificable, tiene reconocimiento internacional y se puede aplicar a todo tipo de empresas. Además describe como implantar un SGSI.
- COBIT 5 [2]: dispone de más controles que la ISO/IEC 27000, no dispone de certificación oficial. Su alcance es mucho mayor al englobar todos los procesos de la gestión TIC lo cual supone una restricción a la fácil implantación de controles.
- NIST [3]: dispone de una cantidad inmensa de controles, no dispone de certificación oficial y se recomienda para alguna organización federal de los Estados Unidos.

Por todo ello, ISO/IEC 27000 es la elegida para el desarrollo de la guía propuesta para este TFM.

Posteriormente se introduce el concepto de la gestión de los riesgos al ser fundamental para la elección de los controles. Una breve sección se focaliza en los tipos de ataques que sufren las PYME. Se identifican los sistemas de seguridad más utilizados y se recalca la problemática a nivel tecnológico por parte de las PYME. Apenas se

dedican recursos a la ciberseguridad y no se dedica esfuerzo a la transformación digital. También se menciona el uso cada vez más extendido de los ciberseguros.

La GDPR es un punto muy importante a la hora de identificar aquellos controles necesarios para todas las empresas. De ahí la pequeña introducción a la norma y su posible relación con la familia ISO/IEC 27000 (en concreto la ISO/IEC 27002).De esta manera se permite comprender el porqué algunos controles son seleccionados y otros sin embargo son desestimados.

Finalmente se propone la guía de controles de fácil implantación y un supuesto ficticio que aplica la guía propuesta.

# 3. Planificación

*¿Cuándo y por dónde empiezo?*

Todo proyecto requiere de una planificación. Este proceso permite definir la gestión del tiempo, defición de las actividades o tareas a realizar, su secuencia para llevarlas a cabo, la estimación de los recursos y la duración de las actividades [4]. El desglose del trabajo permite descomponer el proyecto en partes más pequeñas y manejables, identificadas como tareas en este Trabajo Fin de Máster.

Para el desarrollo de este TFM, se han desglosado las tareas en función de las Prácticas de Evaluación Continua (PEC) a entregar durante el semestre Septiembre 2017 – Enero 2018. De cara a facilitar su lectura, cada una de las tareas principales se muestra en su correspondiente capítulo.

## 3.1. Tareas

Se presentan las siguientes tareas:

| | Tarea | Descripción |
|---|---|---|
| **PEC1** | • Introducción<br>• Objetivos<br>• Planificación<br>• Normativas, guías y estándares más relevantes | Se indica la problemática a la que se enfrentan las PYME para abordar la seguridad TIC así como los objetivos que se persiguen con la realización de este TFM.<br>La planificación muestra las tareas a realizar y los tiempos estimados.<br>Por otra parte, se introducen las normativas vigentes más relevantes que sirven como base para este TFM. |
| **PEC2** | • Gestión de riesgos<br>• General Data Protection Regulation (GDPR) | Se presenta la necesidad de realizar una eficiente gestión de los riesgos de cualquier organización.<br>Se explica la regulación que entra en vigor en mayo de 2018 y a la que se tienen que acoger todas las empresas en la Unión Europea (UE) |
| **PEC3** | • Guía de controles de fácil implantación (ISO27K) | Se propone una guía que recoge los controles de seguridad de fácil implementación para una PYME en función de la ISO27002 |
| **PEC4** | • Aplicación de la guía en empresa ficticia<br>• Conclusiones | Se presenta un supuesto ficticio según la guía propuesta.<br>Las conclusiones recogen las propuestas mostradas a lo largo del TFM |
| **PEC5** | • Presentación y vídeo | La presentación y vídeo contienen una síntesis del TFM.<br>Nótese que no forman parte de este documento |

*Tabla 1 – Lista de tareas*

## 3.2. Planificación de las Tareas

En la siguiente figura se muestra el plan preliminar de las tareas a realizar en este TFM. Se debe tener en cuenta que el plan puede sufrir modificaciones a lo largo de su desarrollo.

GANTT CHART

| | Task Name | Start | Finish |
|---|---|---|---|
| 1 | Introducción | Wed 20/09/17 | Sun 24/09/17 |
| 2 | Objetivos | Mon 25/09/17 | Tue 26/09/17 |
| 3 | Metodología | Wed 27/09/17 | Wed 27/09/17 |
| 4 | Planificación | Thu 28/09/17 | Thu 28/09/17 |
| 5 | Tareas | Fri 29/09/17 | Sun 01/10/17 |
| 6 | Planificación de las Tareas | Mon 02/10/17 | Wed 04/10/17 |
| 7 | Normativas, guías y estándares | Thu 05/10/17 | Mon 09/10/17 |
| 8 | Gestión de Riesgos | Tue 10/10/17 | Wed 18/10/17 |
| 9 | General Data Protection Regulation (GDPR) | Thu 19/10/17 | Sat 28/10/17 |
| 10 | Relación entre la GDPR y la ISO27001 | Mon 30/10/17 | Mon 06/11/17 |
| 11 | Guía de controles de fácil implantación (ISO27K) | Tue 07/11/17 | Tue 14/11/17 |
| 12 | Implantación de la ISO27001 | Thu 16/11/17 | Wed 22/11/17 |
| 13 | Lista de controles | Thu 23/11/17 | Mon 04/12/17 |
| 14 | Aplicación de la guía (supuesto ficticio) | Tue 05/12/17 | Thu 28/12/17 |
| 15 | Conclusiones | Fri 29/12/17 | Fri 29/12/17 |
| 16 | Trabajo futuro | Sat 30/12/17 | Sat 30/12/17 |
| 17 | Presentación y vídeo | Mon 01/01/18 | Mon 08/01/18 |

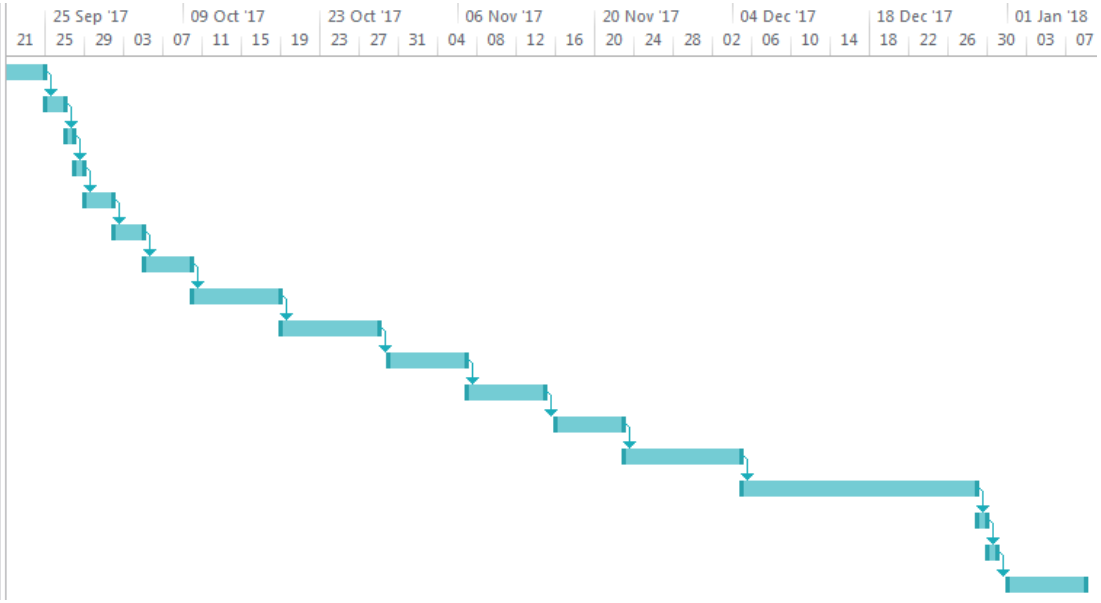



*Imagen 1 – Planificación de las tareas*

# 4. Normativas, guías y estándares

*¿Cuáles son las normativas, guías o estándares más relevantes que podría utilizar?*

Existen varias normativas, guías o estándares recomendables para la gestión de las TIC. No obstante, algunas ponen su foco únicamente en la seguridad de la información, y otras hacen ciertas referencias a la misma aunque su principal interés forme parte de la estrategia de negocio para la gestión de las TIC. También existe, en alguna de ellas, la posibilidad de obtener una certificación en caso de cumplir con los requisitos exigidos o simplemente se pueden obtener certificados a nivel personal (no la organización). Surge el dilema, ¿cuál es la que realmente conviene a mi organización? Si estamos en la Unión Europea, ¿conviene seguir una norma de Estados Unidos? ¿Qué norma es más fácil de aplicar en términos de coste y duración?

Ante estas preguntas conviene realizar el ejercicio de conocerlasnormas más relevantes y sus listas de controles, al menos de forma sucinta, para comprender las razones por las que se ha optado por trabajar con la ISO27001:2013 en este TFM.

## 4.1. ISO 27001:2013

La familia ISO/IEC 27000 fue desarrollada por la ISO (International Standards Organization) y la IEC (InternationalElectrotechnical Comisión). Este conjunto de guías y estándares están relacionados con las TIC en el ámbito de la seguridad [1]. Todas ellas han sido creadas por expertos bajo la supervisión de la ISO/IEC. Proporcionan un marco de gestión de la seguridad de la información utilizable por cualquier tipo de organización independiente del tamaño de la misma.

Las normas están relacionadas de la siguiente forma:

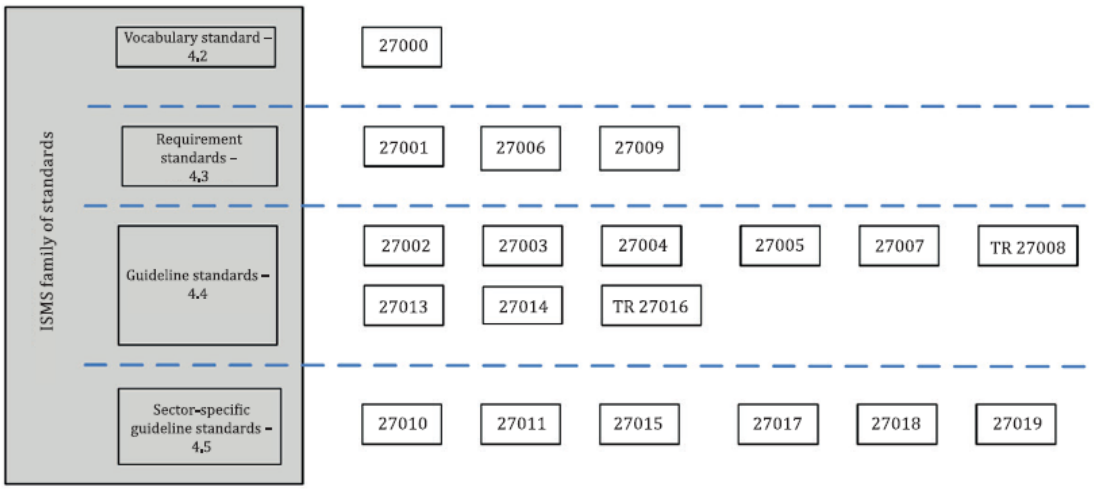



*Imagen 2 – Familia de normas ISO/IEC 27000*

Los dos estándares más relevantes que contienen la lista de controles son:

- ISO/IEC 27001 – describe como implantar un SGSI que servirá para gestionar los controles y riesgos de la seguridad de la información dentro de una organización. Especifica los requisitos para establecer, implementar, operar, monitorizar, revisar, mantener y mejorar el SGSI dentro del contexto de los riesgos de negocio de la organización.Los objetivos de control y la lista de controles derivan y están alineados con los que están en la lista de la ISO/IEC 27002. Su anexo A resume dichos objetivos de control y la lista. Esta norma puede ser certificable. Punto muy importante para cualquier organización que desee tener un reconocimiento internacional respecto al tratamiento de los datos.

| ISO/IEC 27001 (2013) |
|---|
| 14 Dominios |
| 35 Objetivos de control |
| 114 Controles |

- ISO/IEC 27002 – es una guía de buenas prácticas que describe los objetivos de control y controles recomendables y comúnmente aceptados en la seguridad de la información y que, de hecho, son los que utiliza la norma ISO/IEC 27001[1].

Existen muchas ventajas en caso de implantar un SGSI [12][15]:

- Menor riesgo de pérdida de información
- Revisión continua de los riesgos de forma periódica
- Uso de una metodología para la gestión de la seguridad informática
- Se definen medidas de seguridad para el acceso a la información
- Integración con otros sistemas de gestión ya normalizados
- Cumplimiento con la ley vigente
- Proporcionar confianza interna a la organización
- Simplificar las evaluaciones sobre los productos o servicios de la entidad
- Factor diferenciador frente a la competencia
- Reducción de auditorías de segundas partes
- Cumplimiento de requerimientos del mercado
- Abaratamiento de las primas de riesgo de seguros
- Fomento de las medidas de seguridad

La ISO/IEC 27001 proporciona reconocimiento y aceptación a nivel mundial y por lo tanto puede ser utilizada sin límites internacionales. La capacidad de certificación a nivel empresarial es un valor añadido.

[1] *La lista de controles está disponible en el anexo de este documento.*

La siguiente figura muestra la encuesta de certificaciones realizada por ISO relativo al período 2006-2016 para ISO/IEC 27001 a nivel mundial:

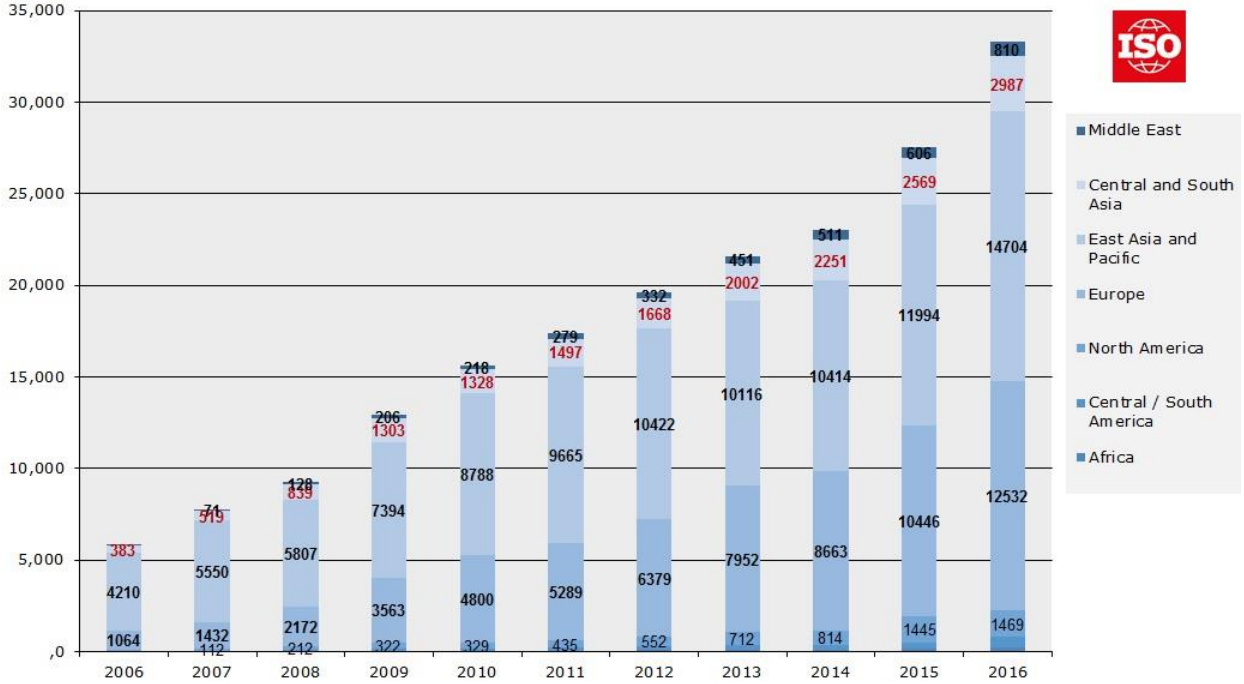



*Imagen 3 – Certificaciones ISO/IEC 27000 en todo el mundo (2006-2016) [1]*

## 4.2. COBIT

Es un marco de trabajo de buenas prácticas creado por la Asociacion Profesional Internacional ISACA para la gestión TIC y la gobernanza TIC [2]. Ofrece un conjunto de controles sobre las TIC y las organiza en un marco de trabajo lógico de procesos IT relacionados. Este catálogo no es auditable por sí mismo.

Al igual que la ISO/IEC 27002, COBIT proporciona información sobre lo que se está gestionando. No obstante, mientras la ISO/IEC 27002 se centra sólo en la Seguridad de la Información, COBIT tiene un alcance mucho mayor puesto que engloba todos los procesos de la gestión TIC.

Se suele utilizar para la ejecución de políticas y procedimientos clave de la organización así como para mapear controles, problemas técnicos y riesgos. De hecho ayuda a la optimización del coste de los servicios TIC, contribuye al cumplimiento de las leyes, regulaciones y acuerdos y facilita una buena gestión de las tecnologías de la información.

| COBIT 5 |
| --- |
| 4 dominios |
| 34 procesos |
| 210 objetivos de control |

Es un estándar aceptado a nivel global que permite implementarse en empresas de todo tipo de tamaño de forma parcial como la ISO/IEC 27002 sin necesitar un análisis completo y compromiso por parte de la administración.

No existe una certificación para las organizaciones como tal. Sin embargo, existen niveles de certificación a título individual (persona física):

- Certified Information Systems Auditor Learn more about CISA (CISA)
- Certified Information Security Manager Learn more about CISM (CISM)
- Certified in the Governance of Enterprise IT (CGEIT)
- Certified in Risk and Information Systems Control (CRISC)

Este marco de trabajo debería utilizarse en caso de que la organización quisiera comprender y alinear los objetivos de negocio y sus servicios TIC.

## 4.3. NIST SP 800-53

El NIST Special Publication 800-53 (NIST SP 800-53) ofrece un conjunto mínimo de controles para todos los sistemas de información federales de Estados Unidos excepto para los concernientes a la Seguridad Nacional [3]. Fue creado por el NIST, agencia no regulatoria del Departamento de Comercio de los Estados Unidos, responsable del desarrollo de estándares, guías y otras publicaciones relativos a la seguridad de la información.

Cubre tres niveles principales: técnico, gestión y operacional. Esos controles aseguran que el ciclo de seguridad de la información requerida es perseguido por los servicios federales de la información: Iniciación, Adquisición / Desarrollo, Implementación / Evaluación, Operaciones / Mantenimiento y Eliminación.

| **NIST SP800-53** |
|---|
| (***Revision 4***) |
| 19 familias |
| 965 controles |

Uno de los puntos fuertes de NIST es que proporciona una masiva colección de documentación para implementar un entorno de seguridad robusto ya que NIST se creó con el fin de ser utilizado por las agencias federales de Estados Unidos. Pero es una desventaja desde el punto de vistafinanciero ya que con tan ingente cantidad de controles lo hace un tanto inviable o cuando menos poco interesante para pequeñas organizaciones.

No tiene la posibilidad de certificación. En su lugar ofrece una serie de guías que permiten cumplir con los requisitos de los sistemas de información federal que es obligarorio para todas las instituciones gubernamentales en Estados Unidos

NIST sería recomendable cuando sea necesario implementar controles de seguridad en profundidad y en alguna organización federal de los Estados Unidos independientemente de su tamaño.

# 5. Gestión de Riesgos

*¿Por qué la gestión de riesgos es tan importante para la protección de la información?*

Si una organización tiene el firme interés de desarrollar una gestión de seguridad de la información para todos sus activos, la gestión de riesgos debería ser un pilar fundamental en su política. A pesar de todo, y aunque existe mucha literatura al respecto, algunas empresas no lo consideran lo suficientemente relevante. "Es un coste muy elevado que no nos podemos permitir", "no sufrimos tantos ataques diarios", "ya tenemos la capacidad de respuesta rápida a cualquier tipo de incidente", "si dedico tantos recursos a la seguridad, ¿quién realizará las operaciones diarias?". Éstos son los típicos comentarios, por lo general de la alta dirección de cualquier empresa, cuando se presenta la idea de aplicar una adecuada política de seguridad.

Las siguientes subsecciones introducen el concepto de riesgo de una forma sucinta. Ayudarán a la comprensión sobre como abordar los controles de seguridad que convendría aplicar y que se reflejan en la guía que se proponeen este TFM.

## 5.1. Análisis de riesgos

El análisis es la primera etapa dentro de la gestión de los riesgos. Es la encargada de identificar y evaluar los riesgos de manera tanto cualitativa como cuantitativa. Inicialmente se procede a distinguir aquellos activos que se necesitan proteger, los posibles ataques y vulnerabilidades que pueden sufrir y,en la manera de lo posible, se estudia la forma de protegerlos.

Se debe tener en cuenta los costes a los que se enfrentaría la organización:

1) costes para proteger los activos de aquellos riesgos identificados;
2) costes que se deberían asumir si se materializa el riesgo al no estar los activos protegidos.

Existen varias estrategias de respuesta a los riesgos:

- Aceptar – la organización asume que se encuentra bajo riesgo y aun así no ejecuta ninguna acción. Suele utilizarse en aquellas amenazas menos importantes ya que el coste que acarrearía su materialización es aceptable. No obstante, sería recomendable definir una serie de procedimientos a seguir en la organización en caso de que el evento ocurra.
- Transferir – el riesgo se transfiere a un tercero, por ejemplo a un seguro, que asumirá la responsabilidad de la gestión. De todas formas, la organización no debería dejar de prestarle atención puesto que sigue existiendo. Se recomendaría realizar un seguimiento al igual que con el resto que no han sido transferidos.
- Mitigar – la organización aplica los controles que considere oportunos para reducir el impacto del riesgo si llegará a materializarse. No se habría eliminado del todo, pero podría ser asumido por la organización
- Evitar – la organización intenta eliminar ese riesgo completamente y para ello implanta todos los controles necesarios. Sería la solución idónea aunque obviamente es la más costosa en recursos.

## 5.2. Elementos del análisis

Para proceder con el análisis de los riesgos conviene identificar aquellos elementos que son comunes en múltiples metodologías [13]:

- Activos – son todo tipo de elementos de la organización utilizados para el desarrollo de sus actividades de negocio. Son la parte fundamental del análisis de los riesgos.
- Amenazas –representan a aquellos factores externos que pueden producir daños en la organización. Se suelen definir 3 tipos de origen: humano, natural o entorno.
- Vulnerabilidades –son aquellos factores internos que identifican las debilidades de los activos previamente identificados.
- Controles –son los elementos de seguridad implantados por las organizaciones para proteger los activos y reducir los riesgos potenciales.
- Riesgos –sería la probabilidad de la organización de sufrir daños en sus activos en función de las amenazas y vulnerabilidades. El valor de los mismos incrementaría su riesgo: mayor valor, mayor riesgo.
- Requisitos de seguridad –serían las necesidades de la organización para poder reducir los riesgos y que serían la base de los controles de seguridad.
- Valor de los activos–sería la valoración económica de los activos, la cual tendría relación directa con el nivel de riesgo de los mismos.

La relación de estos elementos es fundamental para la gestión de los riesgos la cual suele existir en cualquier metodología. Se muestra en la figurasiguiente:

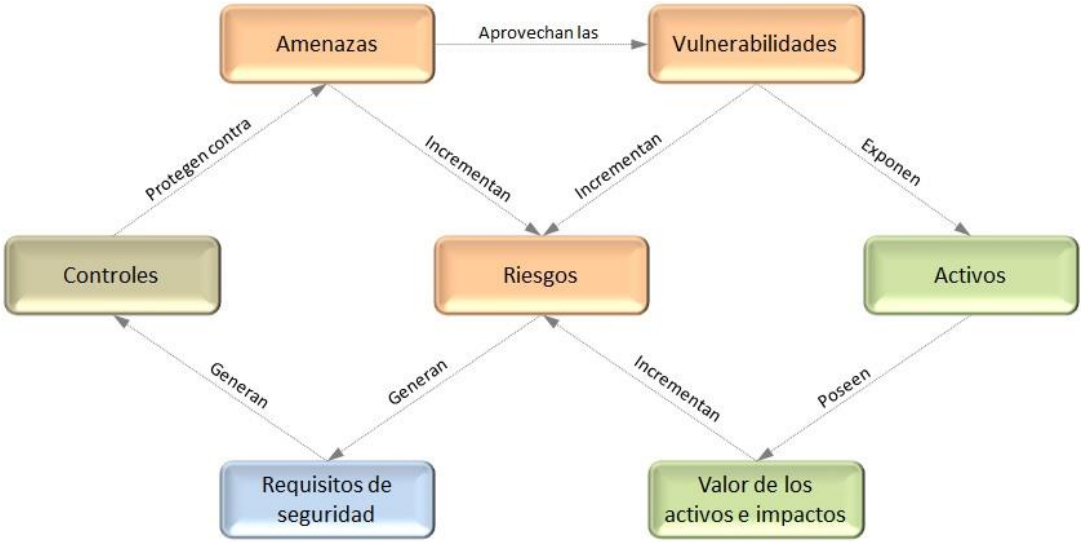



*Imagen 4 – Elementos del análisis de riesgos*

## 5.3. Resultado de los análisis

Existen distintas metodologías que permiten realizar análisis de los resultados. Si bien no es el objeto de este TFM presentarlas, resulta interesante indicar algunas características [13]:

- MAGERIT –es una metodología abierta creada por el Ministerio de Administraciones Públicas (MAP) de España que se ofrece como marco de trabajo y guía para las administraciones públicas aunque se puede aplicar a cualquier tipo de organización independientemente del lugar. Lo más relevante es que permite mostrar los riesgos a nivel económico. Sin embargo, este mismo hecho hace que su aplicación sea muy costosa [5].
- NIST – esta metodología, ya mencionada brevemente en el capítulo anterior, tiene la ventaja de realizar las valoraciones de manera cualitativa en lugar de económica. Su aplicación pues, resulta mucho más sencilla.

  El cálculo de los riesgos está basado en la probabilidad y su impacto (alto, medio y bajo):

| **Probabilidad / Impacto** | Impacto bajo | Impacto medio | Impacto alto |
|---|---|---|---|
| Alta | Bajo | Medio | Alto |
| Media | Bajo | Medio | Medio |
| Baja | Bajo | Bajo | Bajo |

*Tabla 2 – Nivel de riesgo en función de probabilidad e impacto*

  Los tres niveles de riesgos requerirán aplicar ciertas medidas de seguridad. En caso de ser Alto se intentará, en la medida de lo posible, evitarlo o cuando menos reducirlo; si es Medio se aplicarán controles en un tiempo razonable; y si es Bajo, se estudiará si se tiene que utilizar algún control.

  Esta metodología es más sencilla que MAGERIT y podría recomendarse para realizar un análisis a muy alto nivel y posteriormente profundizar con otro tipo de metodología.
- CRAMM – esta metodología es también fácil de aplicar puesto que no realiza valoraciones económicas sino numéricas (por lo general entre 1 y 5) en función del valor de los activos, la estimación de las probabilidades y la estimación de los impactos:

  Riesgo = Valor + Probabilidad + Impacto

  Una de las ventajas es que permite priorizar los riesgos en función de su valor. Pero se aconsejaría realizar un proceso posterior para convertir esos valores numéricos en económicos.
- OCTAVE – la forma de mostrar los resultados es diferente a las otras metodologías. Éstos se presentan en un árbol de riesgos para conocer el camino crítico en el que la organización debe actuar primero. Gracias a ello se permite analizar todo tipo de situaciones. No obstante se tiene que repetir el ciclo para encontrar el proceso crítico y de esta forma reducir todos los riesgos.

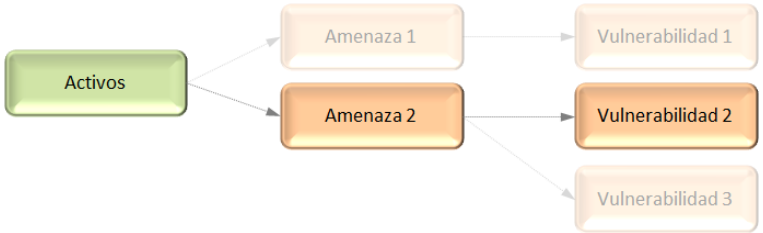



*Imagen 5 – Árbol de riesgos OCTAVE*

## 5.4. Ataques informáticos habituales recibidos por las PYME

Las PYME sufren multitud de ataques de forma continua. Es evidente que conviene realizar una gestión de los riesgos siguiendo una política que la organización debería asumir como parte fundamental de su negocio. Si nos atenemos a algunas cifras obtenidas de diversas encuestas en 2016, existen varios ataques destacados que incluyen, desde varios tipos de malware (p. ej. virus, troyanos, spyware, ransomware, etc) a fuga de información [16]:

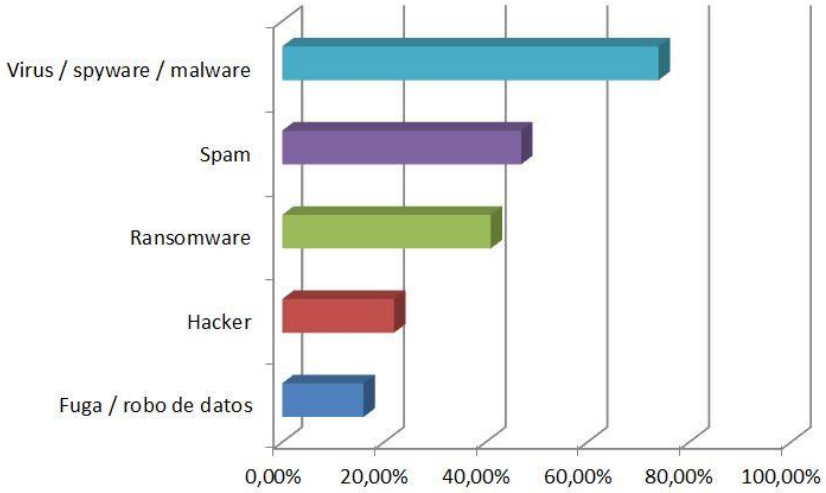



*Imagen 6 – Ataques informáticos habituales*

Los ataques aquí mostrados podrían ser contrarrestados con una serie de controles de seguridad que cuando menos conseguirían mitigar o evitar los riesgos. De hecho algunas organizaciones ya los aplican pero principalmente se pone énfasis en sistemas de seguridad software o hardware tal y como refleja la figura siguiente [16]:

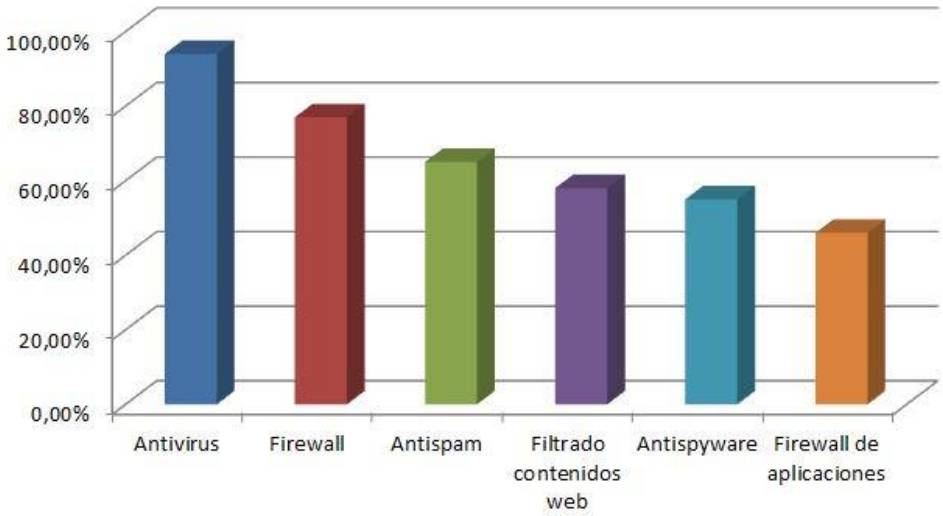



*Imagen 7 – Sistemas de seguridad más usados por las PYME*

De todas formas, se suelen olvidar o no considerar otros controles igualmente necesarios como por ejemplo: formación y concienciación de los empleados, definición de una política de seguridad a nivel corporativo, realización de revisiones periódicas de dicha política, realización de auditorías internas (e incluso externas), etc.

Otro punto es que, teniendo en cuenta el uso actual y futuro previstode los servicios de información por cualquier tipo de organización, es presumible que las cifras relativas a los ataques se incrementen en el tiempo. Y más, considerando la lenta transformación digital de las PYME [16]:

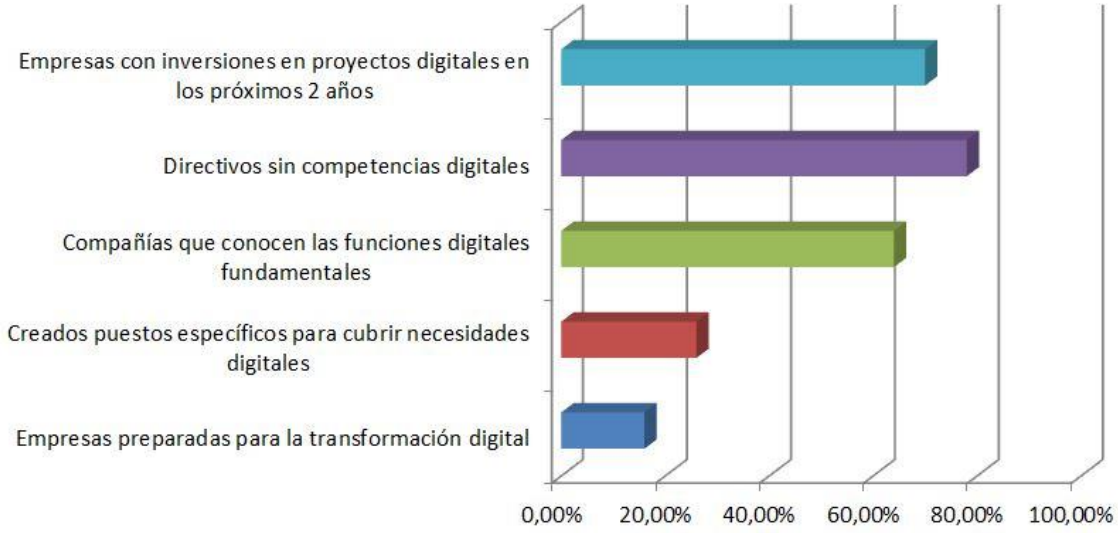



*Imagen 8 – Transformación digital de las PYME*

Se aprecia claramente que las PYME necesitan realizar una inversión enciberseguridad y en concreto en los recursos dedicados. Esta afirmación se ve reflejada en la siguiente imagen [16]:

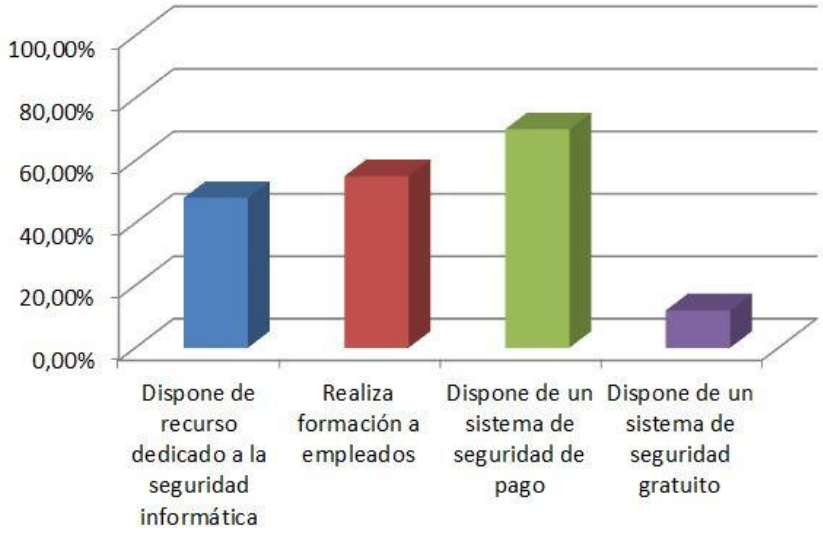



*Imagen 9 – Recursos dedicados a la ciberseguridad*

## 5.5. Ciberseguros para PYME

Como se ha comentado, algunas organizaciones aplican controles de forma que se puedan evitar o mitigar los riesgos de seguridad. En cualquier caso, existe la posibilidad de transferir ese riesgo a un tercero. Por ejemplo, contratando un seguro.

Existen varias aseguradoras que ofrecen diferentes coberturas. Entre otras:

- Costes y gastos por la restauración de los sistemas
- Eliminación de virus
- Interrupción del negocio
- Responsabilidad civil (privacidad, multimedia o publicidad)
- Daños propios y a terceros
- Protección y recuperación de datos
- Gestión de ransomware (ciberextorsión)
- Interrupción del negocio
- Gestión del daño reputacional
- Penalizaciones por incumplimiento contractual
- Robo de información por ataque de piratería
- Gastos por investigación forense
- Seguridad en la red de la compañía
- Multas por sanciones regulatorias
- Consultoría y asesoría sobre seguridad de información

Los precios también dependen del tamaño de la organización. Existen algunos que sólo cubren a las PYME pero su servicio es el más básico. El mayor problema surge a la hora de la contratación por ser un proceso largo.

Lo que sí coinciden muchos analistas es que el mercado de los ciberseguros está en auge. Estados Unidos es el mercado más desarrollado puesto que tiene más de 10 años de experiencia [17]. España todavía está entrando de manera moderada aunque se prevé que con la nueva regulación GDPR, las PYME considerarán el uso de ciberseguros como una razón de peso incluso aplicando algunas sus propios controles de seguridad.Sirva como detalle que la industria sanitaria, educación, turismo, juego, servicios, energía y utilities han incrementado su contratación incluyendo, en algunos casos, coberturas especiales [18].

# 6. General Data Protection Regulation (GDPR)

*¿Qué es y por qué afecta la GDPR a las PYME?*

La General Data Protection Regulation (GDPR) (o Reglamento General de Protección de Datos, RGPD) es una normativa que reemplaza la Directiva Europea95/46/EC sobre la protección de los individuos con respecto al procesamiento de los datos personales y la libre circulación de dichos datos. Será de obligado cumplimiento para las empresas de todo tipo de tamaño y sector. En caso contrario podrían ser penalizadas con unas multas muy elevadas de un máximo de 20 millones de Euros o, hasta un 4% del volumen de negocio actual de la empresa que no cumpla los requisitos legales (artículo 83).Fue adoptada el 27 de abril de 2016 y entrará en vigor el 25 de mayo de 2018 después de un período de transición. No es necesario que los Estados Miembros de la UE aprueben ninguna legislación al ser directamente vinculante.

Las PYME españolas están actualmente sujetas a la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (LOPDP) [8], la cual, tal y como indica su artículo 1, tiene por objeto garantizar y proteger, en lo que concierne al tratamiento de los datos personales, las libertades públicas y los derechos fundamentales de las personas físicas, y especialmente de su honor e intimidad personal y familiar. Es más, existe el reglamento de obligado cumplimiento aprobado por el Real Decreto 1720/2007 que incrementa la protección a los datos personales [9]. Este reglamento contempla en su artículo 80 tres niveles de seguridad: básico, medio y alto. Con la aprobación de la GDPR, deberán estar así mismo sujetas a esta regulación de la UE y por ello deberán estar preparadas antes de su aplicación. De ahí ese período de transición de 2 años.

## 6.1. Niveles de seguridad de protección según el Real Decreto 1720/2007

Los niveles que se presentan a continuación son incrementales. Es decir, el nivel más alto deberá adoptar las medidas de seguridad de los niveles inferiores.

### NIVEL BÁSICO

- Funciones y obligaciones del personal – Los usuarios o perfiles de usuarios con acceso a datos de carácter personal y sistemas de información deberán estar claramente identificados. El responsable del tratamiento adoptará medidas para el conocimiento comprensible de las normas de seguridad (*art. 89*).
- Registro de incidencias – Deberá existir un procedimiento de notificación y gestión de las incidencias que afecten a los datos de carácter personal y establecer un registro con la información de la incidencia (*art. 90*).
- Control de acceso – Los usuarios tendrá acceso solamente la los recursos que necesiten. Se definirán claramente los perfiles de usuario y sus accesos permitidos (*art. 91*).
- Gestión de soportes y documentos – Los soportes y documentos que contengan datos de carácter personal deberán identificar el tipo de información que contienen y podrán ser etiquetados si la información es especialmente sensible. Su salida y traslado deberá ser autorizada por el responsable del fichero (*art. 92*).

- Identificación y autenticación – El responsable del fichero o tratamiento deberá adoptar las medidas que garanticen la correcta identificación y autenticación de los usuarios. Se establecerá la periodicidad del cambio de contraseñas(*art. 93*).
- Copias de respaldo y recuperación – Se deberán establecer procedimientos de copia de respaldo como mínimo semanal. El responsable del fichero verificará cada seis meses la aplicación de los procedimientos de copia y recuperación (*art. 94*).

## NIVEL MEDIO

- Responsable de seguridad – Se deberá designar uno o varios responsables de seguridad para controlar las medidas de seguridad (*art. 95*).
- Auditoría – Los sistemas de información deberán someterse al menos cada 2 años a una auditoria interna o externa para dictaminar la adecuación de las medidas y controles a la Ley. Los informes serán analizados por el responsable de seguridad competente (*art. 96*).
- Gestión de soportes y documentos – Deberá establecerse un sistema de registro de entrada y salida de soportes (*art. 97*).
- Identificación y autenticación – El responsable del fichero o tratamiento establecerá un mecanismo que limite la posibilidad de intentar reiteradamente el acceso no autorizado al sistema de información (*art. 98*).
- Control de acceso físico – Exclusivamente el personal autorizado en el documento de seguridad podrá tener acceso a los lugares donde se hallen instalados los equipos físicos que den soporte a los sistemas de información (*art. 99*).
- Registro de incidencias – Deberán registrarse, además de las incidencias como indica el artículo 90, los procedimientos realizados de recuperación de datos cuya ejecución requerirá la autorización del responsable del fichero (*art. 100*).

## NIVEL ALTO

- Gestión y distribución de soportes – La identificación se deberá realizar utilizando sistemas de etiquetado comprensibles para identificar su contenido. La distribución se realizará cifrando los datos o utilizando otro mecanismo. Se deberá evitar el tratamiento de datos en dispositivos portátiles que no permitan su cifrado (*art. 101*).
- Copias de respaldo y recuperación – Deberá conservarse una copia de respaldo de los datos así como los procedimientos de recuperación utilizando elementos que garanticen su integridad y recuperación (*art. 102*).
- Registro de accesos – Se registran todos los accesos realizados bajo el control directo del responsable de seguridad. El período de conservación será de 2 años (*art. 103*).
- Telecomunicaciones – La transmisión de datos de carácter personal a través de redes públicas o redes inalámbricas de comunicaciones electrónicas se realizará cifrando dichos datos o bien utilizando cualquier otro mecanismo (*art. 104*).

## 6.2. Relación entre la GDPR y la ISO/IEC 27002:2013

Con motivo de la aplicación de la normativa GDPR, y en caso de que la organización esté interesada en utilizar la familia ISO/IEC 27000, se sugiere presentar una relación entre ambas. La tabla siguiente introduce de forma muy resumida los artículos de la norma y los objetivos de control según la ISO/IEC 27002:2013 que podrían tener una relación directa[2]. Para detalles más concretos se recomienda acceder directamente a la normativa GDPR [6] y a la familia ISO/IEC 27000 [1].

| GDPR | | ISO/IEC 27002:2013 |
|---|---|---|
| **Artículo** | **Título del artículo y breve descripción** | **Objetivos de control relacionados** |
| *Capítulo I – Disposiciones Generales* | | |
| 1 | Objeto<br>Se muestra el objetivo de la normativa relativa a la protección de los datos personales y la circulación de los mismos. Protege los derechos y libertades de las personas físicas donde la libre circulación de los datos personales no podrá ser restringida ni prohibida. | 18.1 Cumplimiento con los requisitos legales y contractuales<br>Evitar incumplimientos de obligaciones legales, estatutarias, reglamentarias o contractuales relacionadas con la seguridad de la información y con cualquier requisito de seguridad. |
| 2 | Ámbito de aplicación material<br>Se especifica donde se aplica. En concreto al tratamiento total o parcialmente automatizado de los datos personales así como aquellos incluídos en un fichero. | 5.1 Dirección de gestión para la seguridad de la información<br>Proporciona dirección de gestión y soporte para la seguridad de la información de acuerdo con los requisitos de negocio, leyes y regulaciones relevantes.<br>8.2 Clasificación de la información<br>Asegurar que la información recibe un nivel apropiado de protección de acuerdo con su importancia para la organización.<br>8.3 Manipulación de media<br>Prevenir la divulgación, modificación, eliminación o destrucción no autorizada de la información almacenada en los medios.<br>9.1 Requisitos de negocio para el control de acceso<br>Limitar el acceso a la información y las instalaciones de procesamiento de la información.<br>10.1 Controles criptográficos<br>Asegurar el uso apropiado y efectivo de la criptografía para proteger la confidencialidad, autenticación y/o la integridad de la información.<br>12.3 Copias de respaldo<br>Proteger contra la pérdida de datos.<br>13.2 Transferencia de información<br>Mantener la seguridad de información transferida dentro de la organización y con cualquier entidad externa.<br>14.3 Datos de prueba<br>Asegurar la protección de los datos utilizados para las pruebas. |

[2] *Se debe tener en consideración que es una interpretación de ambas. Por tanto, se aconsejaría realizar una revisión final por un departamento legal.*

| GDPR | | ISO/IEC 27002:2013 |
|---|---|---|
| **Artículo** | **Título del artículo y breve descripción** | **Objetivos de control relacionados** |
| 3 | Ámbito territorial<br>La aplicación será en toda la UE independientemente de tratar esos datos personales en la UE o fuera de ella. | 5.1 Dirección de gestión para la seguridad de la información<br>Proporciona dirección de gestión y soporte para la seguridad de la información de acuerdo con los requisitos de negocio, leyes y regulaciones relevantes.<br>15.1 Seguridad de la información en las relaciones con los proveedores<br>Asegurar la protección de los activos de la organización que son accesibles por los proveedores.<br>18.1 Cumplimiento con los requisitos legales y contractuales<br>Evitar incumplimientos de obligaciones legales, estatutarias, reglamentarias o contractuales relacionadas con la seguridad de la información y con cualquier requisito de seguridad. |
| 4 | Definiciones<br>Se definen una serie de términos que se utilizan a lo largo del reglamento. | N / A |
| *Capítulo II – Principios* | | |
| 5 | Principios relativos al tratamiento<br>Se especifican características de los datos personales: como serán tratados, recogidos, deberán ser adecuados, exactos, pertinentes, etc.<br>Por otro lado, el responsable deberá tener una responsabilidad proactiva ("controller"). | 5.1 Dirección de gestión para la seguridad de la información<br>Proporciona dirección de gestión y soporte para la seguridad de la información de acuerdo con los requisitos de negocio, leyes y regulaciones relevantes.<br>6.1 Organización interna<br>Establecer un marco de trabajo de gestión para iniciar y controlar la implementación y la operación de la seguridad de la información dentro de la organización.<br>8.1 Responsabilidad por los activos<br>Identificar activos organizativos y definir responsabilidades de protección apropiadas.<br>8.2 Clasificación de la información<br>Asegurar que la información recibe un nivel apropiado de protección de acuerdo con su importancia para la organización.<br>9.2 Gestión de acceso de usuarios<br>Asegurar el acceso de usuario autorizado y prevenir el acceso no autorizado a los sistemas y servicios.<br>9.3 Responsabilidades de los usuarios<br>Asegurar que los usuarios sean responsables para la salvaguarda de la información de autenticación.<br>9.4Control de acceso a sistemas y aplicaciones<br>Prevenir el acceso no autorizado a los sistemas y aplicaciones.<br>10.1 Controles criptográficos<br>Asegurar el uso apropiado y efectivo de la criptografía para proteger la confidencialidad, autenticación y/o la integridad de la información.<br>14.3 Datos de prueba<br>Asegurar la protección de los datos utilizados para las pruebas.<br>17.1 Continuidad de seguridad de la información<br>La continuidad de la seguridad de la información debe integrarse en los sistemas de la gestión de la continuidad del negocio de la organización. |
| 6 | Licitud del tratamiento<br>Para que el tratamiento de los datos sea lícito se deben cumplir unas condiciones como por ejemplo: consentimiento del interesado, que el tratamiento | 5.1 Dirección de gestión para la seguridad de la información<br>Proporciona dirección de gestión y soporte para la seguridad de la información de acuerdo con los requisitos de negocio, leyes y regulaciones relevantes. |

| GDPR | | ISO/IEC 27002:2013 |
|---|---|---|
| **Artículo** | **Título del artículo y breve descripción** | **Objetivos de control relacionados** |
| | seanecesario en la ejecución de un contrato o misión, necesario para la satisfacción de intereses legitimos, etc.<br>Los Estados miembros podrán mantener o introducir disposiciones más específicas y el tratamiento tendrá que ser establecido por el Derecho de la Unión o de los Estados miembros. | 14.1 Requisitos de seguridad de los sistemas de información<br>Asegurar que la seguridad de la información es una parte integral de los sistemas de información en todo el ciclo de vida. Esto además incluye los requisitos para los sistemas de información los cuales proporcionan servicios sobre redes públicas.<br>18.1 Cumplimiento con los requisitos legales y contractuales<br>Evitar incumplimientos de obligaciones legales, estatutarias, reglamentarias o contractuales relacionadas con la seguridad de la información y con cualquier requisito de seguridad. |
| 7 | Condiciones para el consentimiento<br>El interesado deberá dar libremente el consentimiento explícito para el tratamiento de sus datos y tendrá la posibilidad de retirar su consentimiento en cualquier momento. | 5.1 Dirección de gestión para la seguridad de la información<br>Proporciona dirección de gestión y soporte para la seguridad de la información de acuerdo con los requisitos de negocio, leyes y regulaciones relevantes.<br>8.2 Clasificación de la información<br>Asegurar que la información recibe un nivel apropiado de protección de acuerdo con su importancia para la organización.<br>8.3 Manipulación de media<br>Prevenir la divulgación, modificación, eliminación o destrucción no autorizada de la información almacenada en los medios.<br>12.1 Procedimientos operacionales y responsabilidades<br>Asegurar operaciones correctas y seguras de las instalaciones de procesado de la información.<br>13.2 Transferencia de información<br>Mantener la seguridad de información transferida dentro de la organización y con cualquier entidad externa.<br>14.3 Datos de prueba<br>Asegurar la protección de los datos utilizados para las pruebas.<br>15.1 Seguridad de la información en las relaciones con los proveedores<br>Asegurar la protección de los activos de la organización que son accesibles por los proveedores. |
| 8 | Condiciones aplicables al consentimiento del niño en relación con los servicios de la sociedad de la información<br>Se establecen condiciones específicas para el tratamiento de los datos por los niños cuando tenga más de 16 años o bien con el consentimiento o autorización del tutor con la patria potestad. | 5.1 Dirección de gestión para la seguridad de la información<br>Proporciona dirección de gestión y soporte para la seguridad de la información de acuerdo con los requisitos de negocio, leyes y regulaciones relevantes.<br>8.2 Clasificación de la información<br>Asegurar que la información recibe un nivel apropiado de protección de acuerdo con su importancia para la organización.<br>8.3 Manipulación de media<br>Prevenir la divulgación, modificación, eliminación o destrucción no autorizada de la información almacenada en los medios.<br>12.1 Procedimientos operacionales y responsabilidades<br>Asegurar operaciones correctas y seguras de las instalaciones de procesado de la información.<br>13.2 Transferencia de información<br>Mantener la seguridad de información transferida dentro de la organización y con cualquier entidad externa.<br>14.3 Datos de prueba<br>Asegurar la protección de los datos utilizados para las pruebas. |

| GDPR | | ISO/IEC 27002:2013 |
|---|---|---|
| **Artículo** | **Título del artículo y breve descripción** | **Objetivos de control relacionados** |
| | | 15.1 Seguridad de la información en las relaciones con los proveedores<br>Asegurar la protección de los activos de la organización que son accesibles por los proveedores. |
| 9 | Tratamiento de categorías especiales de datos personales<br>Se prohíbe el tratamiento de los datos que revelen el origen étnico o racial, opiniones políticas, convicciones religiosas o filosóficas, etc. No obstante, se podrá realizar en caso de que el interesado diera el consentimiento explícito. | 5.1 Dirección de gestión para la seguridad de la información<br>Proporciona dirección de gestión y soporte para la seguridad de la información de acuerdo con los requisitos de negocio, leyes y regulaciones relevantes.<br>8.2 Clasificación de la información<br>Asegurar que la información recibe un nivel apropiado de protección de acuerdo con su importancia para la organización.<br>8.3 Manipulación de media<br>Prevenir la divulgación, modificación, eliminación o destrucción no autorizada de la información almacenada en los medios.<br>12.1 Procedimientos operacionales y responsabilidades<br>Asegurar operaciones correctas y seguras de las instalaciones de procesado de la información.<br>13.2 Transferencia de información<br>Mantener la seguridad de información transferida dentro de la organización y con cualquier entidad externa.<br>14.3 Datos de prueba<br>Asegurar la protección de los datos utilizados para las pruebas.<br>15.1 Seguridad de la información en las relaciones con los proveedores<br>Asegurar la protección de los activos de la organización que son accesibles por los proveedores. |
| 10 | Tratamiento de datos personales relativos a condenas e infracciones penales<br>Los datos relativos a condenas o infracciones penales podrán ser tratados bajo la supervisión de las autoridades públicas o cuando lo autorice el Derecho de la Unión o de los Estados miembros. | 5.1 Dirección de gestión para la seguridad de la información<br>Proporciona dirección de gestión y soporte para la seguridad de la información de acuerdo con los requisitos de negocio, leyes y regulaciones relevantes.<br>8.2 Clasificación de la información<br>Asegurar que la información recibe un nivel apropiado de protección de acuerdo con su importancia para la organización.<br>8.3 Manipulación de media<br>Prevenir la divulgación, modificación, eliminación o destrucción no autorizada de la información almacenada en los medios.<br>14.1 Requisitos de seguridad de los sistemas de información<br>Asegurar que la seguridad de la información es una parte integral de los sistemas de información en todo el ciclo de vida. Esto además incluye los requisitos para los sistemas de información los cuales proporcionan servicios sobre redes públicas.<br>18.1 Cumplimiento con los requisitos legales y contractuales<br>Evitar incumplimientos de obligaciones legales, estatutarias, reglamentarias o contractuales relacionadas con la seguridad de la información y con cualquier requisito de seguridad. |
| 11 | Tratamiento que no requiere identificación<br>No habrá restricciones en el tratamiento de los datos si la persona no puede ser identificada. | 5.1 Dirección de gestión para la seguridad de la información<br>Proporciona dirección de gestión y soporte para la seguridad de la información de acuerdo con los requisitos de negocio, leyes y regulaciones relevantes.<br>8.2 Clasificación de la información |

| GDPR | | ISO/IEC 27002:2013 |
|---|---|---|
| **Artículo** | **Título del artículo y breve descripción** | **Objetivos de control relacionados** |
| | | Asegurar que la información recibe un nivel apropiado de protección de acuerdo con su importancia para la organización.<br>8.3 Manipulación de media<br>Prevenir la divulgación, modificación, eliminación o destrucción no autorizada de la información almacenada en los medios.<br>10.1 Controles criptográficos<br>Asegurar el uso apropiado y efectivo de la criptografía para proteger la confidencialidad, autenticación y/o la integridad de la información.<br>13.2 Transferencia de información<br>Mantener la seguridad de información transferida dentro de la organización y con cualquier entidad externa.<br>14.1 Requisitos de seguridad de los sistemas de información<br>Asegurar que la seguridad de la información es una parte integral de los sistemas de información en todo el ciclo de vida. Esto además incluye los requisitos para los sistemas de información los cuales proporcionan servicios sobre redes públicas.<br>15.1 Seguridad de la información en las relaciones con los proveedores<br>Asegurar la protección de los activos de la organización que son accesibles por los proveedores. |
| *Capítulo III – Derechos del interesado* | | |
| 12 | Transparencia de la información, comunicación y modalidades de ejercicio de los derechos del interesado<br>La información será tratada con transparencia, inteligible y de fácil acceso con un lenguaje claro. El interesado deberá ser informado de sus derechos y de las actualizaciones realizadas sobre sus datos.<br>La información deberá ser gratuita. | 5.1 Dirección de gestión para la seguridad de la información<br>Proporciona dirección de gestión y soporte para la seguridad de la información de acuerdo con los requisitos de negocio, leyes y regulaciones relevantes.<br>8.2 Clasificación de la información<br>Asegurar que la información recibe un nivel apropiado de protección de acuerdo con su importancia para la organización.<br>8.3 Manipulación de media<br>Prevenir la divulgación, modificación, eliminación o destrucción no autorizada de la información almacenada en los medios.<br>12.1 Procedimientos operacionales y responsabilidades<br>Asegurar operaciones correctas y seguras de las instalaciones de procesado de la información.<br>14.1 Requisitos de seguridad de los sistemas de información<br>Asegurar que la seguridad de la información es una parte integral de los sistemas de información en todo el ciclo de vida. Esto además incluye los requisitos para los sistemas de información los cuales proporcionan servicios sobre redes públicas. |
| 13 | Información que deberá facilitarse cuando los datos personales se obtengan del interesado<br>Cuando se obtengan datos personales del interesado, el responsable del tratamiento facilitará toda la información de la identidad y datos de contacto del responsable y delegado de protección de datos, los fines del tratamiento, destinatarios de los datos así como el plazo de conservación y el derecho de supresión, rectificación, limitación. | 5.1 Dirección de gestión para la seguridad de la información<br>Proporciona dirección de gestión y soporte para la seguridad de la información de acuerdo con los requisitos de negocio, leyes y regulaciones relevantes.<br>8.2 Clasificación de la información<br>Asegurar que la información recibe un nivel apropiado de protección de acuerdo con su importancia para la organización.<br>8.3 Manipulación de media |

| GDPR | | ISO/IEC 27002:2013 |
|---|---|---|
| **Artículo** | **Título del artículo y breve descripción** | **Objetivos de control relacionados** |
| | | Prevenir la divulgación, modificación, eliminación o destrucción no autorizada de la información almacenada en los medios.<br>12.1 Procedimientos operacionales y responsabilidades<br>Asegurar operaciones correctas y seguras de las instalaciones de procesado de la información.<br>14.1 Requisitos de seguridad de los sistemas de información<br>Asegurar que la seguridad de la información es una parte integral de los sistemas de información en todo el ciclo de vida. Esto además incluye los requisitos para los sistemas de información los cuales proporcionan servicios sobre redes públicas. |
| 14 | Información que deberá facilitarse cuando los datos personales no se hayan obtenido del interesado<br>Similar al artículo 13 aunque en este caso se refiere a cuando los datos no los haya proporcionado el interesado. Se ofrecerá la información dentro de un plazo razonable a más tardar dentro de un mes o de la primera comunicación con el interesado. | 5.1 Dirección de gestión para la seguridad de la información<br>Proporciona dirección de gestión y soporte para la seguridad de la información de acuerdo con los requisitos de negocio, leyes y regulaciones relevantes.<br>8.2 Clasificación de la información<br>Asegurar que la información recibe un nivel apropiado de protección de acuerdo con su importancia para la organización.<br>8.3 Manipulación de media<br>Prevenir la divulgación, modificación, eliminación o destrucción no autorizada de la información almacenada en los medios.<br>12.1 Procedimientos operacionales y responsabilidades<br>Asegurar operaciones correctas y seguras de las instalaciones de procesado de la información.<br>14.1 Requisitos de seguridad de los sistemas de información<br>Asegurar que la seguridad de la información es una parte integral de los sistemas de información en todo el ciclo de vida. Esto además incluye los requisitos para los sistemas de información los cuales proporcionan servicios sobre redes públicas. |
| 15 | Derecho de acceso del interesado<br>El interesado tendrá derecho a obtener del responsable del tratamiento la confirmación de si se están tratando sus datos personales y de obtener una copia de los mismos.<br>En caso de que los datos sean transferidos a un tercer país u organización internacional, el interesado tendrá derecho a ser informado. | 5.1 Dirección de gestión para la seguridad de la información<br>Proporciona dirección de gestión y soporte para la seguridad de la información de acuerdo con los requisitos de negocio, leyes y regulaciones relevantes.<br>8.1 Responsabilidad por los activos<br>Identificar activos organizativos y definir responsabilidades de protección apropiadas.<br>8.2 Clasificación de la información<br>Asegurar que la información recibe un nivel apropiado de protección de acuerdo con su importancia para la organización.<br>12.1 Procedimientos operacionales y responsabilidades<br>Asegurar operaciones correctas y seguras de las instalaciones de procesado de la información.<br>13.2 Transferencia de información<br>Mantener la seguridad de información transferida dentro de la organización y con cualquier entidad externa.<br>14.1 Requisitos de seguridad de los sistemas de información<br>Asegurar que la seguridad de la información es una parte integral de los sistemas de información en todo el ciclo de vida. Esto además incluye los requisitos para los sistemas de información los cuales proporcionan servicios sobre redes públicas.<br>15.1 Seguridad de la información en las relaciones con los proveedores |

| GDPR | | ISO/IEC 27002:2013 |
|---|---|---|
| **Artículo** | **Título del artículo y breve descripción** | **Objetivos de control relacionados** |
| | | Asegurar la protección de los activos de la organización que son accesibles por los proveedores. |
| 16 | Derecho de rectificación<br>El interesado tendrá el derecho de rectificación de los datos personales inexactos que le conciernan sin dilación alguna por parte del responsable del tratamiento. | 5.1 Dirección de gestión para la seguridad de la información<br>Proporciona dirección de gestión y soporte para la seguridad de la información de acuerdo con los requisitos de negocio, leyes y regulaciones relevantes.<br>8.1 Responsabilidad por los activos<br>Identificar activos organizativos y definir responsabilidades de protección apropiadas.<br>8.2 Clasificación de la información<br>Asegurar que la información recibe un nivel apropiado de protección de acuerdo con su importancia para la organización.<br>12.1 Procedimientos operacionales y responsabilidades<br>Asegurar operaciones correctas y seguras de las instalaciones de procesado de la información.<br>12.3 Copias de respaldo<br>Proteger contra la pérdida de datos.<br>13.2 Transferencia de información<br>Mantener la seguridad de información transferida dentro de la organización y con cualquier entidad externa.<br>14.1 Requisitos de seguridad de los sistemas de información<br>Asegurar que la seguridad de la información es una parte integral de los sistemas de información en todo el ciclo de vida. Esto además incluye los requisitos para los sistemas de información los cuales proporcionan servicios sobre redes públicas.<br>15.1 Seguridad de la información en las relaciones con los proveedores<br>Asegurar la protección de los activos de la organización que son accesibles por los proveedores. |
| 17 | Derecho de supresión («el derecho al olvido»)<br>El interesado tendrá el derecho de supresión de los datos personales que le conciernan sin dilación alguna por parte del responsable del tratamiento. | 5.1 Dirección de gestión para la seguridad de la información<br>Proporciona dirección de gestión y soporte para la seguridad de la información de acuerdo con los requisitos de negocio, leyes y regulaciones relevantes.<br>8.1 Responsabilidad por los activos<br>Identificar activos organizativos y definir responsabilidades de protección apropiadas.<br>8.2 Clasificación de la información<br>Asegurar que la información recibe un nivel apropiado de protección de acuerdo con su importancia para la organización.<br>8.3 Manipulación de media<br>Prevenir la divulgación, modificación, eliminación o destrucción no autorizada de la información almacenada en los medios.<br>12.1 Procedimientos operacionales y responsabilidades<br>Asegurar operaciones correctas y seguras de las instalaciones de procesado de la información.<br>12.3 Copias de respaldo<br>Proteger contra la pérdida de datos.<br>13.2 Transferencia de información<br>Mantener la seguridad de información transferida dentro de la organización y con cualquier entidad externa.<br>14.1 Requisitos de seguridad de los sistemas de información |

| GDPR | | ISO/IEC 27002:2013 |
|---|---|---|
| **Artículo** | **Título del artículo y breve descripción** | **Objetivos de control relacionados** |
| | | Asegurar que la seguridad de la información es una parte integral de los sistemas de información en todo el ciclo de vida. Esto además incluye los requisitos para los sistemas de información los cuales proporcionan servicios sobre redes públicas.<br>15.1 Seguridad de la información en las relaciones con los proveedores<br>Asegurar la protección de los activos de la organización que son accesibles por los proveedores. |
| 18 | Derecho a la limitación del tratamiento<br>El interesado tendrá el derecho de limitación del tratamiento de los datos personales que le conciernan sin dilación alguna por parte del responsable del tratamiento. | 5.1 Dirección de gestión para la seguridad de la información<br>Proporciona dirección de gestión y soporte para la seguridad de la información de acuerdo con los requisitos de negocio, leyes y regulaciones relevantes.<br>8.1 Responsabilidad por los activos<br>Identificar activos organizativos y definir responsabilidades de protección apropiadas.<br>8.2 Clasificación de la información<br>Asegurar que la información recibe un nivel apropiado de protección de acuerdo con su importancia para la organización.<br>12.1 Procedimientos operacionales y responsabilidades<br>Asegurar operaciones correctas y seguras de las instalaciones de procesado de la información.<br>12.3 Copias de respaldo<br>Proteger contra la pérdida de datos.<br>13.2 Transferencia de información<br>Mantener la seguridad de información transferida dentro de la organización y con cualquier entidad externa.<br>14.1 Requisitos de seguridad de los sistemas de información<br>Asegurar que la seguridad de la información es una parte integral de los sistemas de información en todo el ciclo de vida. Esto además incluye los requisitos para los sistemas de información los cuales proporcionan servicios sobre redes públicas.<br>15.1 Seguridad de la información en las relaciones con los proveedores<br>Asegurar la protección de los activos de la organización que son accesibles por los proveedores. |
| 19 | Obligación de notificación relativa a la rectificación o supresión de datos personales o la limitación del tratamiento<br>El responsable del tratamiento tendrá que informar por la rectificación o supresión de los datos personales o limitación del tratamiento de los mismos salvo que sea imposible o exija un esfuerzo desproporcionado. | 5.1 Dirección de gestión para la seguridad de la información<br>Proporciona dirección de gestión y soporte para la seguridad de la información de acuerdo con los requisitos de negocio, leyes y regulaciones relevantes.<br>8.1 Responsabilidad por los activos<br>Identificar activos organizativos y definir responsabilidades de protección apropiadas.<br>12.1 Procedimientos operacionales y responsabilidades<br>Asegurar operaciones correctas y seguras de las instalaciones de procesado de la información.<br>13.2 Transferencia de información<br>Mantener la seguridad de información transferida dentro de la organización y con cualquier entidad externa.<br>14.1 Requisitos de seguridad de los sistemas de información<br>Asegurar que la seguridad de la información es una parte integral de los sistemas de información en todo el ciclo de vida. Esto además incluye los requisitos para los sistemas de información los cuales proporcionan servicios sobre redes públicas.<br>15.1 Seguridad de la información en las relaciones con los proveedores |

| GDPR | | ISO/IEC 27002:2013 |
|---|---|---|
| **Artículo** | **Título del artículo y breve descripción** | **Objetivos de control relacionados** |
| | | Asegurar la protección de los activos de la organización que son accesibles por los proveedores. |
| 20 | Derecho a la portabilidad de los datos<br>El interesado tendrá el derecho de recibir los datos personales que le incumban que haya proporcionado a un responsable del tratamiento en un formato estructurado y de uso común y lectura automática para transmitirlo a otro responsable del tratamiento. | 5.1 Dirección de gestión para la seguridad de la información<br>Proporciona dirección de gestión y soporte para la seguridad de la información de acuerdo con los requisitos de negocio, leyes y regulaciones relevantes.<br>8.3 Manipulación de media<br>Prevenir la divulgación, modificación, eliminación o destrucción no autorizada de la información almacenada en los medios.<br>13.1 Gestión de seguridad de la red<br>Asegurar la protección de la información en redes y en las instalaciones de procesado de la información de soporte.<br>13.2 Transferencia de información<br>Mantener la seguridad de información transferida dentro de la organización y con cualquier entidad externa.<br>14.1 Requisitos de seguridad de los sistemas de información<br>Asegurar que la seguridad de la información es una parte integral de los sistemas de información en todo el ciclo de vida. Esto además incluye los requisitos para los sistemas de información los cuales proporcionan servicios sobre redes públicas.<br>15.1 Seguridad de la información en las relaciones con los proveedores<br>Asegurar la protección de los activos de la organización que son accesibles por los proveedores. |
| 21 | Derecho de oposición<br>El interesado tendrá derecho a oponerse en cualquier momento, por motivos relacionados con su situación particular a que datos personales que le conciernan sean objeto de un tratamiento como en el caso de la mercadotecnia directa o con fines de investigación científica, histórica o fines estadísticos. | 5.1 Dirección de gestión para la seguridad de la información<br>Proporciona dirección de gestión y soporte para la seguridad de la información de acuerdo con los requisitos de negocio, leyes y regulaciones relevantes.<br>8.1 Responsabilidad por los activos<br>Identificar activos organizativos y definir responsabilidades de protección apropiadas.<br>8.2 Clasificación de la información<br>Asegurar que la información recibe un nivel apropiado de protección de acuerdo con su importancia para la organización.<br>12.1 Procedimientos operacionales y responsabilidades<br>Asegurar operaciones correctas y seguras de las instalaciones de procesado de la información.<br>12.3 Copias de respaldo<br>Proteger contra la pérdida de datos.<br>13.2 Transferencia de información<br>Mantener la seguridad de información transferida dentro de la organización y con cualquier entidad externa.<br>14.1 Requisitos de seguridad de los sistemas de información<br>Asegurar que la seguridad de la información es una parte integral de los sistemas de información en todo el ciclo de vida. Esto además incluye los requisitos para los sistemas de información los cuales proporcionan servicios sobre redes públicas.<br>15.1 Seguridad de la información en las relaciones con los proveedores<br>Asegurar la protección de los activos de la organización que son accesibles por los proveedores. |

| GDPR | | ISO/IEC 27002:2013 |
|---|---|---|
| **Artículo** | **Título del artículo y breve descripción** | **Objetivos de control relacionados** |
| 22 | Decisiones individuales automatizadas, incluida la elaboración de perfiles<br>El interesado tendrá derecho a no ser objeto de una decisión basada únicamente en el tratamiento automatizado, incluida la elaboración de perfiles, que produzca efectos jurídicos en él o le afecte significativamente de modo similar. | 5.1 Dirección de gestión para la seguridad de la información<br>Proporciona dirección de gestión y soporte para la seguridad de la información de acuerdo con los requisitos de negocio, leyes y regulaciones relevantes.<br>8.2 Clasificación de la información<br>Asegurar que la información recibe un nivel apropiado de protección de acuerdo con su importancia para la organización.<br>12.1 Procedimientos operacionales y responsabilidades<br>Asegurar operaciones correctas y seguras de las instalaciones de procesado de la información.<br>13.2 Transferencia de información<br>Mantener la seguridad de información transferida dentro de la organización y con cualquier entidad externa.<br>14.1 Requisitos de seguridad de los sistemas de información<br>Asegurar que la seguridad de la información es una parte integral de los sistemas de información en todo el ciclo de vida. Esto además incluye los requisitos para los sistemas de información los cuales proporcionan servicios sobre redes públicas.<br>15.1 Seguridad de la información en las relaciones con los proveedores<br>Asegurar la protección de los activos de la organización que son accesibles por los proveedores. |
| 23 | Limitaciones<br>El Derecho de la Unión o de los Estados miembros que se aplique al responsable o el encargado del tratamiento podrá limitar, a través de medidas legislativas, el alcance de las obligaciones y de los derechos establecidos. | 5.1 Dirección de gestión para la seguridad de la información<br>Proporciona dirección de gestión y soporte para la seguridad de la información de acuerdo con los requisitos de negocio, leyes y regulaciones relevantes.<br>18.1 Cumplimiento con los requisitos legales y contractuales<br>Evitar incumplimientos de obligaciones legales, estatutarias, reglamentarias o contractuales relacionadas con la seguridad de la información y con cualquier requisito de seguridad. |
| *Capítulo IV – Responsable y encargado del tratamiento* | | |
| 24 | Responsabilidad del responsable del tratamiento<br>El responsable del tratamiento aplicará medidas técnicas y organizativas apropiadas a fin de garantizar y poder demostrar que el tratamiento es conforme con la GDPR. Los controles se revisarán y actualizarán en caso necesario. | **NOTA:** prácticamente la totalidad de los objetivos de control. No se identifican en particular. |
| 25 | Protección de datos desde el diseño y por defecto<br>Teniendo en cuenta el estado de la técnica, el coste de la aplicación y la naturaleza, ámbito, contexto y fines del tratamiento, así como los riesgos, deberá proteger los datos desde el diseño y por defecto. | **NOTA:** prácticamente la totalidad de los objetivos de control. No se identifican en particular. |
| 26 | Corresponsables del tratamiento<br>Cuando dos o más responsables determinen conjuntamente los objetivos y los medios del tratamiento serán considerados corresponsables del tratamiento y determinarán de forma transparente sus roles y responsabilidades respectivas. | 5.1 Dirección de gestión para la seguridad de la información<br>Proporciona dirección de gestión y soporte para la seguridad de la información de acuerdo con los requisitos de negocio, leyes y regulaciones relevantes.<br>6.1 Organización interna<br>Establecer un marco de trabajo de gestión para iniciar y controlar la implementación y la operación de la seguridad de la información dentro de la organización. |

| GDPR | | ISO/IEC 27002:2013 |
|---|---|---|
| **Artículo** | **Título del artículo y breve descripción** | **Objetivos de control relacionados** |
| | | 12.1 Procedimientos operacionales y responsabilidades<br>Asegurar operaciones correctas y seguras de las instalaciones de procesado de la información.<br>13.2 Transferencia de información<br>Mantener la seguridad de información transferida dentro de la organización y con cualquier entidad externa.<br>15.1 Seguridad de la información en las relaciones con los proveedores<br>Asegurar la protección de los activos de la organización que son accesibles por los proveedores.<br>16.1 Gestión de incidentes y mejoras de seguridad de la información.<br>Asegurar un enfoque consistente y efectivo para la gestión de los incidentes de seguridad de la información, incluyendo la comunicación sobre eventos y debilidades de seguridad.<br>18.1 Cumplimiento con los requisitos legales y contractuales<br>Evitar incumplimientos de obligaciones legales, estatutarias, reglamentarias o contractuales relacionadas con la seguridad de la información y con cualquier requisito de seguridad. |
| 27 | Representantes de responsables o encargados del tratamiento no establecidos en la Unión<br>Las organizaciones de fuera de la UE deberán designar a los representantes dentro de la Unión que cumplan una serie de requisitos como tratamiento ocasional, manejo a gran escala de categorías especiales de datos y que sea improbable que se entrañe un riesgo para los derechos y libertades de las personas físicas. | 12.1 Procedimientos operacionales y responsabilidades<br>Asegurar operaciones correctas y seguras de las instalaciones de procesado de la información.<br>13.2 Transferencia de información<br>Mantener la seguridad de información transferida dentro de la organización y con cualquier entidad externa.<br>14.1 Requisitos de seguridad de los sistemas de información<br>Asegurar que la seguridad de la información es una parte integral de los sistemas de información en todo el ciclo de vida. Esto además incluye los requisitos para los sistemas de información los cuales proporcionan servicios sobre redes públicas.<br>15.1 Seguridad de la información en las relaciones con los proveedores<br>Asegurar la protección de los activos de la organización que son accesibles por los proveedores.<br>18.1 Cumplimiento con los requisitos legales y contractuales<br>Evitar incumplimientos de obligaciones legales, estatutarias, reglamentarias o contractuales relacionadas con la seguridad de la información y con cualquier requisito de seguridad. |
| 28 | Encargado del tratamiento<br>Se designará un encargado del tratamiento por cuenta de un responsable del tratamiento que ofrezca garantías suficientes del cumplimiento de la GDPR y no recurrirá a otro encargado sin la autorización previa por escrito, específica o general, del responsable. | 5.1 Dirección de gestión para la seguridad de la información<br>Proporciona dirección de gestión y soporte para la seguridad de la información de acuerdo con los requisitos de negocio, leyes y regulaciones relevantes.<br>12.1 Procedimientos operacionales y responsabilidades<br>Asegurar operaciones correctas y seguras de las instalaciones de procesado de la información.<br>15.1 Seguridad de la información en las relaciones con los proveedores<br>Asegurar la protección de los activos de la organización que son accesibles por los proveedores. |
| 29 | Tratamiento bajo la autoridad del responsable o del encargado del tratamiento<br>El encargado del tratamiento y cualquier persona que actúe bajo la autoridad del responsable o del encargadosolo podrán tratar dichos datos siguiendo instrucciones del responsable. | **NOTA:** prácticamente la totalidad de los objetivos de control. No se identifican en particular. |
| 30 | Registro de las actividades de tratamiento | 5.1 Dirección de gestión para la seguridad de la información |

| GDPR | | ISO/IEC 27002:2013 |
|---|---|---|
| **Artículo** | **Título del artículo y breve descripción** | **Objetivos de control relacionados** |
| | El responsable del tratamiento debe llevar un registro de las actividades de tratamiento efectuadas bajo su responsabilidad incluyendo entre otros el nombre y datos del contacto del responsable, fines del tratamiento, descripción de las categorías de interesados y destinatarios, plazos previstos. | Proporciona dirección de gestión y soporte para la seguridad de la información de acuerdo con los requisitos de negocio, leyes y regulaciones relevantes.<br>6.1 Organización interna<br>Establecer un marco de trabajo de gestión para iniciar y controlar la implementación y la operación de la seguridad de la información dentro de la organización.<br>12.1 Procedimientos operacionales y responsabilidades<br>Asegurar operaciones correctas y seguras de las instalaciones de procesado de la información.<br>12.4 Registro y monitorización<br>Registrar eventos y generar evidencias. |
| 31 | Cooperación con la autoridad de control<br>El responsable y el encargado del tratamiento cooperarán con la autoridad de control que lo solicite en el desempeño de sus funciones. | 5.1 Dirección de gestión para la seguridad de la información<br>Proporciona dirección de gestión y soporte para la seguridad de la información de acuerdo con los requisitos de negocio, leyes y regulaciones relevantes.<br>6.1 Organización interna<br>Establecer un marco de trabajo de gestión para iniciar y controlar la implementación y la operación de la seguridad de la información dentro de la organización. |
| 32 | Seguridad del tratamiento<br>El responsable y el encargado del tratamiento aplicarán controles técnicos y organizativos apropiados para garantizar un nivel de seguridad según el riesgo. | **NOTA:** prácticamente la totalidad de los objetivos de control. No se identifican en particular. |
| 33 | Notificación de una violación de la seguridad de los datos personales a la autoridad de control<br>En caso de violación de la seguridad de los datos personales, el responsable del tratamiento la notificará a la autoridad de control competente sin dilación indebida y, de ser posible, a más tardar 72 horas después de que haya tenido constancia de ella. | 5.1 Dirección de gestión para la seguridad de la información<br>Proporciona dirección de gestión y soporte para la seguridad de la información de acuerdo con los requisitos de negocio, leyes y regulaciones relevantes.<br>16.1 Gestión de incidentes y mejoras de seguridad de la información.<br>Asegurar un enfoque consistente y efectivo para la gestión de los incidentes de seguridad de la información, incluyendo la comunicación sobre eventos y debilidades de seguridad.<br>18.1 Cumplimiento con los requisitos legales y contractuales<br>Evitar incumplimientos de obligaciones legales, estatutarias, reglamentarias o contractuales relacionadas con la seguridad de la información y con cualquier requisito de seguridad. |
| 34 | Comunicación de una violación de la seguridad de los datos personales al interesado<br>Cuando sea probable que la violación de la seguridad de los datos personales entrañe un alto riesgo para los derechos y libertades de las personas físicas, el responsable del tratamiento la comunicará al interesado sin dilación indebida. | 5.1 Dirección de gestión para la seguridad de la información<br>Proporciona dirección de gestión y soporte para la seguridad de la información de acuerdo con los requisitos de negocio, leyes y regulaciones relevantes.<br>16.1 Gestión de incidentes y mejoras de seguridad de la información.<br>Asegurar un enfoque consistente y efectivo para la gestión de los incidentes de seguridad de la información, incluyendo la comunicación sobre eventos y debilidades de seguridad.<br>18.1 Cumplimiento con los requisitos legales y contractuales<br>Evitar incumplimientos de obligaciones legales, estatutarias, reglamentarias o contractuales relacionadas con la seguridad de la información y con cualquier requisito de seguridad. |
| 35 | Evaluación de impacto relativa a la protección de datos<br>Cuando sea probable que un tipo de tratamiento entrañe un alto riesgo para los | 5.1 Dirección de gestión para la seguridad de la información<br>Proporciona dirección de gestión y soporte para la seguridad de la información de acuerdo con los |

| GDPR | | ISO/IEC 27002:2013 |
|---|---|---|
| **Artículo** | **Título del artículo y breve descripción** | **Objetivos de control relacionados** |
| | derechos y libertades de las personas físicas, el responsable del tratamiento realizará, antes del tratamiento, una evaluación del impacto en la protección de datos personales. | requisitos de negocio, leyes y regulaciones relevantes.<br>6.1 Organización interna<br>Establecer un marco de trabajo de gestión para iniciar y controlar la implementación y la operación de la seguridad de la información dentro de la organización.<br>8.2 Clasificación de la información<br>Asegurar que la información recibe un nivel apropiado de protección de acuerdo con su importancia para la organización.<br>12.1 Procedimientos operacionales y responsabilidades<br>Asegurar operaciones correctas y seguras de las instalaciones de procesado de la información.<br>13.1 Gestión de seguridad de la red<br>Asegurar la protección de la información en redes y en las instalaciones de procesado de la información de soporte.<br>13.2 Transferencia de información<br>Mantener la seguridad de información transferida dentro de la organización y con cualquier entidad externa.<br>14.1 Requisitos de seguridad de los sistemas de información<br>Asegurar que la seguridad de la información es una parte integral de los sistemas de información en todo el ciclo de vida. Esto además incluye los requisitos para los sistemas de información los cuales proporcionan servicios sobre redes públicas.<br>15.1 Seguridad de la información en las relaciones con los proveedores<br>Asegurar la protección de los activos de la organización que son accesibles por los proveedores. |
| 36 | Consulta previa<br>El responsable consultará a la autoridad de control antes de proceder al tratamiento cuando una evaluación de impacto muestre que el tratamiento entrañaría un alto riesgo si el responsable no toma medidas para para mitigarlo. | 5.1 Dirección de gestión para la seguridad de la información<br>Proporciona dirección de gestión y soporte para la seguridad de la información de acuerdo con los requisitos de negocio, leyes y regulaciones relevantes.<br>6.1 Organización interna<br>Establecer un marco de trabajo de gestión para iniciar y controlar la implementación y la operación de la seguridad de la información dentro de la organización.<br>8.2 Clasificación de la información<br>Asegurar que la información recibe un nivel apropiado de protección de acuerdo con su importancia para la organización.<br>12.1 Procedimientos operacionales y responsabilidades<br>Asegurar operaciones correctas y seguras de las instalaciones de procesado de la información.<br>13.1 Gestión de seguridad de la red<br>Asegurar la protección de la información en redes y en las instalaciones de procesado de la información de soporte.<br>13.2 Transferencia de información<br>Mantener la seguridad de información transferida dentro de la organización y con cualquier entidad externa.<br>14.1 Requisitos de seguridad de los sistemas de información<br>Asegurar que la seguridad de la información es una parte integral de los sistemas de información en todo el ciclo de vida. Esto además incluye los requisitos para los sistemas de información los cuales proporcionan servicios sobre redes públicas. |

| GDPR | | ISO/IEC 27002:2013 |
|---|---|---|
| **Artículo** | **Título del artículo y breve descripción** | **Objetivos de control relacionados** |
| | | 15.1 Seguridad de la información en las relaciones con los proveedores<br>Asegurar la protección de los activos de la organización que son accesibles por los proveedores. |
| 37 | Designación del delegado de protección de datos<br>El responsable y el encargado del tratamiento designarán un delegado de protección de datos si el tratamiento lo lleva a cabo una autoridad u organismo público, si son operaciones de gran escala y aquellos relativos a condenas e infracciones penales. | 5.1 Dirección de gestión para la seguridad de la información<br>Proporciona dirección de gestión y soporte para la seguridad de la información de acuerdo con los requisitos de negocio, leyes y regulaciones relevantes.<br>6.1 Organización interna<br>Establecer un marco de trabajo de gestión para iniciar y controlar la implementación y la operación de la seguridad de la información dentro de la organización.<br>18.1 Cumplimiento con los requisitos legales y contractuales<br>Evitar incumplimientos de obligaciones legales, estatutarias, reglamentarias o contractuales relacionadas con la seguridad de la información y con cualquier requisito de seguridad. |
| 38 | Posición del delegado de protección de datos<br>El responsable y el encargado del tratamiento garantizarán deberán dar soporte al delegado de protección de datos.<br>El delegado de protección de datos estará obligado a mantener el secreto o la confidencialidad en lo que respecta al desempeño de sus funciones. | 5.1 Dirección de gestión para la seguridad de la información<br>Proporciona dirección de gestión y soporte para la seguridad de la información de acuerdo con los requisitos de negocio, leyes y regulaciones relevantes.<br>6.1 Organización interna<br>Establecer un marco de trabajo de gestión para iniciar y controlar la implementación y la operación de la seguridad de la información dentro de la organización.<br>18.1 Cumplimiento con los requisitos legales y contractuales<br>Evitar incumplimientos de obligaciones legales, estatutarias, reglamentarias o contractuales relacionadas con la seguridad de la información y con cualquier requisito de seguridad. |
| 39 | Funciones del delegado de protección de datos<br>El delegado de protección de datos deberá informar y asesorar al responsable y empleados del tratamiento de sus obligaciones según la GDPR y supervisar su cumplimiento así como cooperar con la autoridad de control. | 5.1 Dirección de gestión para la seguridad de la información<br>Proporciona dirección de gestión y soporte para la seguridad de la información de acuerdo con los requisitos de negocio, leyes y regulaciones relevantes.<br>6.1 Organización interna<br>Establecer un marco de trabajo de gestión para iniciar y controlar la implementación y la operación de la seguridad de la información dentro de la organización.<br>18.1 Cumplimiento con los requisitos legales y contractuales<br>Evitar incumplimientos de obligaciones legales, estatutarias, reglamentarias o contractuales relacionadas con la seguridad de la información y con cualquier requisito de seguridad. |
| 40 | Códigos de conducta<br>Los Estados miembros, autoridades de control, Comité y la CE deberán elaborar códigos de conducta destinados a contribuir a la correcta aplicación de la GDPR. | 5.1 Dirección de gestión para la seguridad de la información<br>Proporciona dirección de gestión y soporte para la seguridad de la información de acuerdo con los requisitos de negocio, leyes y regulaciones relevantes.<br>6.1 Organización interna<br>Establecer un marco de trabajo de gestión para iniciar y controlar la implementación y la operación de la seguridad de la información dentro de la organización.<br>18.1 Cumplimiento con los requisitos legales y contractuales<br>Evitar incumplimientos de obligaciones legales, estatutarias, reglamentarias o contractuales relacionadas con la seguridad de la información y con cualquier requisito de seguridad. |

| GDPR | | ISO/IEC 27002:2013 |
|---|---|---|
| **Artículo** | **Título del artículo y breve descripción** | **Objetivos de control relacionados** |
| 41 | Supervisión de códigos de conducta aprobados<br>Un organismo acreditado por una autoridad de control competente podrá supervisar el cumplimiento de un código de conducta si ha mostrado su independencia, ha establecido procedimientos para aplicar el código y para tratar las reclamaciones relativas a sus infracciones y no hay conflicto de intereses. | 5.1 Dirección de gestión para la seguridad de la información<br>Proporciona dirección de gestión y soporte para la seguridad de la información de acuerdo con los requisitos de negocio, leyes y regulaciones relevantes.<br>6.1 Organización interna<br>Establecer un marco de trabajo de gestión para iniciar y controlar la implementación y la operación de la seguridad de la información dentro de la organización.<br>18.1 Cumplimiento con los requisitos legales y contractuales<br>Evitar incumplimientos de obligaciones legales, estatutarias, reglamentarias o contractuales relacionadas con la seguridad de la información y con cualquier requisito de seguridad. |
| 42 | Certificación<br>Los Estados miembros, las autoridades de control, el Comité y la CE promoverán la creación de mecanismos de certificación en materia de protección de datos y de sellos y marcas de protección de datos. Las certificaciones serán voluntarias y estarán disponibles a través de un proceso transparente. | 6.1 Organización interna<br>Establecer un marco de trabajo de gestión para iniciar y controlar la implementación y la operación de la seguridad de la información dentro de la organización.<br>18.1 Cumplimiento con los requisitos legales y contractuales<br>Evitar incumplimientos de obligaciones legales, estatutarias, reglamentarias o contractuales relacionadas con la seguridad de la información y con cualquier requisito de seguridad. |
| 43 | Organismo de certificación<br>Los organismos de certificación expedirán y renovarán las certificaciones una vez informada la autoridad de control: si han demostrado su independencia, se han comprometido a respetar los criterios aprobados por la autoridad de control y han establecido una serie de procedimientos. La Comisión Europea (CE) podrá establecer mecanismos para la promoción de las certificaciones. | 6.1 Organización interna<br>Establecer un marco de trabajo de gestión para iniciar y controlar la implementación y la operación de la seguridad de la información dentro de la organización.<br>18.1 Cumplimiento con los requisitos legales y contractuales<br>Evitar incumplimientos de obligaciones legales, estatutarias, reglamentarias o contractuales relacionadas con la seguridad de la información y con cualquier requisito de seguridad. |
| *Capítulo V – Transferencias de datos personales a terceros países u organizaciones internacionales* | | |
| 44 | Principio general de las transferencias<br>Solo se realizarán transferencias de datos personales a un tercer país u organización internacional si el responsable y el encargado del tratamiento cumplen las condiciones establecidas en este capítulo. | N / A |
| 45 | Transferencias basadas en una decisión de adecuación<br>Podrá realizarse transferencia de datos personales a un tercer país u organización internacional cuando la CE haya decidido que se garantice un nivel de protección adecuado. La transferencia no requiere de autorización específica. | 18.1 Cumplimiento con los requisitos legales y contractuales<br>Evitar incumplimientos de obligaciones legales, estatutarias, reglamentarias o contractuales relacionadas con la seguridad de la información y con cualquier requisito de seguridad. |
| 46 | Transferencias mediante garantías adecuadas<br>Si las transferencias de datos personales a un tercer país u organización internacional no garantizan un nivel de protección adecuado según el artículo 45, se podrán realizar según garantías especiales y si los interesados cuentan con derechos exigibles y acciones legales efectivas. | 18.1 Cumplimiento con los requisitos legales y contractuales<br>Evitar incumplimientos de obligaciones legales, estatutarias, reglamentarias o contractuales relacionadas con la seguridad de la información y con cualquier requisito de seguridad. |
| 47 | Normas corporativas vinculantes | 18.1 Cumplimiento con los requisitos legales y contractuales |

| GDPR | | ISO/IEC 27002:2013 |
|---|---|---|
| **Artículo** | **Título del artículo y breve descripción** | **Objetivos de control relacionados** |
| | Las autoridades nacionales podrán aprobar reglas de privacidad vinculantes permitiendo transferencias a países no aprobados. | Evitar incumplimientos de obligaciones legales, estatutarias, reglamentarias o contractuales relacionadas con la seguridad de la información y con cualquier requisito de seguridad. |
| 48 | Transferencias o comunicaciones no autorizadas por el Derecho de la Unión<br>Cualquier sentencia de un órgano jurisdiccional o decisión de una autoridad administrativa de un tercer país relativa al tratamiento de datos personales será reconocida o ejecutable si se basa en un acuerdo internacional. | 18.1 Cumplimiento con los requisitos legales y contractuales<br>Evitar incumplimientos de obligaciones legales, estatutarias, reglamentarias o contractuales relacionadas con la seguridad de la información y con cualquier requisito de seguridad. |
| 49 | Excepciones para situaciones específicas<br>Se presentan excepciones para situaciones específicas relativas a transferencias de datos personales a países no aprobados. | 18.1 Cumplimiento con los requisitos legales y contractuales<br>Evitar incumplimientos de obligaciones legales, estatutarias, reglamentarias o contractuales relacionadas con la seguridad de la información y con cualquier requisito de seguridad. |
| 50 | Cooperación internacional en el ámbito de la protección de datos personales<br>Se creará una cooperación internacional para la aplicación eficaz de la legislación, prestación de asistencia mutua y promoción del intercambio de documentación. | N / A |
| *Capítulo VI – Autoridades de control independientes* | | |
| 51 | Autoridad de control<br>Cada Estado miembro establecerá la responsabilidad de una o varias autoridades públicas independientes de supervisar la aplicación de la GDPR. Cada autoridad de control contribuirá a la aplicación en toda la UE. | N / A |
| 52 | Independencia<br>Cada autoridad de control actuará con total independencia, será ajena a toda influencia externa, ya sea directa o indirecta y se abstendrán de cualquier acción que sea incompatible con sus funciones. Cada autoridad de control estará sujeta a un control financiero. | N / A |
| 53 | Condiciones generales aplicables a los miembros de la autoridad de control<br>Los Estados miembros dispondrán que cada miembro de sus autoridades de control sea nombrado mediante un procedimiento transparente. Cada miembro poseerá la titulación, la experiencia y las aptitudes necesarias. | N / A |
| 54 | Normas relativas al establecimiento de la autoridad de control<br>Cada Estado miembro establecerá por ley: autoridad de control, cualificaciones y condiciones de idoneidad, normas y los procedimientos para nombramientos, duración de mandatos, el carácter renovable o no y las condiciones por las que se rigen las obligaciones. | N / A |
| 55 | Competencia<br>Cada autoridad de control será competente para desempeñar las funciones que se le asignen y ejercer los poderes que se le confieran de conformidad con la GDPR en el territorio de su Estado. Las autoridades de control no serán competentes para controlar las operaciones de tratamiento efectuadas por los | N / A |

| GDPR | | ISO/IEC 27002:2013 |
|---|---|---|
| **Artículo** | **Título del artículo y breve descripción** | **Objetivos de control relacionados** |
| | tribunales en el ejercicio de su función judicial. | |
| 56 | Competencia de la autoridad de control principal<br>La autoridad de control del establecimiento principal o del único establecimiento del responsable o del encargado del tratamiento será competente para actuar como autoridad de control principal para el tratamiento transfronterizo. | N / A |
| 57 | Funciones<br>Cada autoridad de control realizará entre otras las siguientes funciones: controlar la aplicación de la GDPR, promover la sensibilización, asesorar a instituciones públicas, facilitar información, tratar reclamaciones presentadas, elaborar códigos de conducta, llevar registros internos de las infracciones de la GDPR.<br>El desempeño de las funciones de cada autoridad de control será gratuito para el interesado y, en su caso, para el delegado de protección de datos. | N / A |
| 58 | Poderes<br>Cada autoridad de control dispondrá de varios poderes de investigación, correctivos y de autorización y consulta. | N / A |
| 59 | Informe de actividad<br>Cada autoridad de control elaborará un informe anual de sus actividades, que podrá incluir una lista de tipos de infracciones notificadas y de tipos de medidas adoptadas. | N / A |
| *Capítulo VII – Cooperación y coherencia* | | |
| 60 | Cooperación entre la autoridad de control principal y las demás autoridades de control interesadas<br>La autoridad de control principal cooperará con las demás autoridades de control interesadas, esforzándose por llegar a un consenso. La autoridad de control principal y las autoridades de control interesadas se intercambiarán información pertinente y sin dilación. | N / A |
| 61 | Asistencia mutua<br>Las autoridades de control se facilitarán información útil y se prestarán asistencia mutua y sin dilación. Las solicitudes de asistencia deberán contener toda la información necesaria y no cobrarán tasa alguna por las medidas adoptadas. | N / A |
| 62 | Operaciones conjuntas de las autoridades de control<br>Las autoridades de control realizarán, en su caso, operaciones conjuntas, incluidas investigaciones conjuntas y medidas de ejecución conjuntas. El Estado miembro de la autoridad de control de acogida asumirá la responsabilidad de acuerdo con el Derecho del Estado miembro en cuyo territorio se desarrollen las operaciones. | N / A |
| 63 | Mecanismo de coherencia<br>Las autoridades de control cooperarán entre sí y, en su caso, con la CE, en el | N / A |

| GDPR | | ISO/IEC 27002:2013 |
|---|---|---|
| **Artículo** | **Título del artículo y breve descripción** | **Objetivos de control relacionados** |
| | marco del mecanismo de coherencia establecido. | |
| 64 | Dictamen del Comité<br>El Comité emitirá un dictamen siempre que una autoridad de control competente proyecte adoptar alguna medida. | N / A |
| 65 | Resolución de conflictos por el Comité<br>El Comité adoptará una decisión vinculante siempre que una autoridad de control interesada haya manifestado una objeción pertinente y motivada, haya puntos de vista enfrentados sobre cuál de las autoridades de control interesadas es competente para el establecimiento principal y cuando una autoridad de control competente no solicite dictamen al Comité. El presidente del Comité notificará sin dilación indebida la decisión contemplada. | N / A |
| 66 | Procedimiento de urgencia<br>Si una autoridad de control interesada considera urgente intervenir para proteger los derechos y las libertades de interesados, podrá adoptar inmediatamente medidas provisionales en su propio territorio con una validez que no podrá ser superior a tres meses. La autoridad de control comunicará sin dilación las medidas y los motivos de su adopción. | N / A |
| 67 | Intercambio de información<br>La Comisión podrá adoptar actos de ejecución de ámbito general para especificar las modalidades de intercambio de información por medios electrónicos entre las autoridades de control, y entre dichas autoridades y el Comité. | N / A |
| 68 | Comité Europeo de Protección de Datos<br>Se crea el Comité Europeo de Protección de Datos («Comité»), como organismo de la Unión, que gozará de personalidad jurídica. Estará representado por su presidente y compuesto por el director de una autoridad de control de cada Estado miembro y por el Supervisor Europeo de Protección de Datos o sus representantes respectivos. | N / A |
| 69 | Independencia<br>El Comité actuará con total independencia en el desempeño de sus funciones o el ejercicio de sus competencias. | N / A |
| 70 | Funciones del Comité<br>El Comité garantizará la aplicación coherente de la GDPR, entre otras: supervisar y garantizar la correcta aplicación de la GDPR, asesorar a la CE, emitir directrices, recomendaciones y buenas prácticas, alentar la elaboración de códigos de conducta y el establecimiento de mecanismos de certificación, promover la cooperación y los intercambios bilaterales y multilaterales efectivos de información, promoverá el intercambio de conocimientos y documentación. | N / A |

| GDPR | | ISO/IEC 27002:2013 |
|---|---|---|
| **Artículo** | **Título del artículo y breve descripción** | **Objetivos de control relacionados** |
| 71 | Informes<br>El Comité elaborará un informe anual en materia de protección de las personas físicas en lo que respecta al tratamiento en la UE y, si procede, en terceros países y organizaciones internacionales. | N / A |
| 72 | Procedimiento<br>El Comité tomará sus decisiones por mayoría simple de sus miembros y adoptará su reglamento interno por mayoría de dos tercios de sus miembros. | N / A |
| 73 | Presidencia<br>El Comité elegirá por mayoría simple de entre sus miembros un presidente y dos vicepresidentes cuyos mandatos serán de 5 años de duración y podrán renovarse una vez. | N / A |
| 74 | Funciones del presidente<br>El presidente desempeñará las siguientes funciones: convocar las reuniones del Comité, notificar las decisiones adoptadas y garantizar el ejercicio puntual de las funciones. | N / A |
| 75 | Secretaría<br>El Comité contará con una secretaría, de la que se hará cargo el Supervisor Europeo de Protección de Datos que ejercerá sus funciones siguiendo las instrucciones del presidente. Prestará apoyo analítico, administrativo y logístico al Comité. | N / A |
| 76 | Confidencialidad<br>Los debates del Comité serán confidenciales cuando el mismo lo considere necesario | N / A |
| *Capítulo VIII – Recursos, responsabilidad y sanciones* | | |
| 77 | Derecho a presentar una reclamación ante una autoridad de control<br>Todo interesado tendrá derecho a presentar una reclamación ante una autoridad de control en el Estado miembro en el que tenga su residencia habitual, lugar de trabajo o lugar de la supuesta infracción, si considera que el tratamiento de datos personales que le conciernen infringe la GDPR. | N / A |
| 78 | Derecho a la tutela judicial efectiva contra una autoridad de control<br>Toda persona física o jurídica tendrá derecho a la tutela judicial efectiva contra una decisión jurídicamente vinculante de una autoridad de control que le concierna | N / A |
| 79 | Derecho a la tutela judicial efectiva contra un responsable o encargado del tratamiento<br>Todo interesado tendrá derecho a la tutela judicial efectiva cuando considere que sus derechos han sido vulnerados como consecuencia de un tratamiento de sus | N / A |

| GDPR | | ISO/IEC 27002:2013 |
|---|---|---|
| **Artículo** | **Título del artículo y breve descripción** | **Objetivos de control relacionados** |
| | datos personales. | |
| 80 | Representación de los interesados<br>El interesado tendrá derecho a dar mandato a una entidad, organización o asociación sin ánimo de lucro que actúe en el ámbito de la protección de los derechos y libertades en materia de protección de los datos personales, para que presente en su nombre una reclamación y ejerza sus derechos, entre otros, a ser indemnizado. | N / A |
| 81 | Suspensión de los procedimientos<br>Cuando un tribunal de un Estado miembro tenga información ante un tribunal de otro Estado miembro de un procedimiento relativo a un mismo asunto, se pondrá en contacto con dicho tribunal de otro Estado miembro para confirmar la existencia de dicho procedimiento. Cualquier tribunal competente distinto de aquel ante el que se ejercitó la acción en primer lugar podrá suspender su procedimiento. | N / A |
| 82 | Derecho a indemnización y responsabilidad<br>Toda persona que haya sufrido daños y perjuicios por una infracción de la GDPR tendrá derecho a recibir del responsable o el encargado del tratamiento una indemnización por los daños y perjuicios sufridos. | 18.1 Cumplimiento con los requisitos legales y contractuales<br>Evitar incumplimientos de obligaciones legales, estatutarias, reglamentarias o contractuales relacionadas con la seguridad de la información y con cualquier requisito de seguridad. |
| 83 | Condiciones generales para la imposición de multas administrativas<br>La autoridad de control garantizará que la imposición de las multas administrativas por las infracciones de la GDPR sean, en cada caso individual, efectivas, proporcionadas y disuasorias.<br>Las multas serán de 20 000 000 EUR como máximo o de una cuantía equivalente al 4 % como máximo del volumen de negocio total anual global del ejercicio financiero anterior, optándose por la de mayor cuantía. | 18.1 Cumplimiento con los requisitos legales y contractuales<br>Evitar incumplimientos de obligaciones legales, estatutarias, reglamentarias o contractuales relacionadas con la seguridad de la información y con cualquier requisito de seguridad. |
| 84 | Sanciones<br>Los Estados miembros podrán establecer otras sanciones que no se sancionen según el artículo 83 y deberán ser efectivas, proporcionadas y disuasorias. | 18.1 Cumplimiento con los requisitos legales y contractuales<br>Evitar incumplimientos de obligaciones legales, estatutarias, reglamentarias o contractuales relacionadas con la seguridad de la información y con cualquier requisito de seguridad. |
| *Capítulo IX – Disposiciones relativas a situaciones específicas de tratamiento* | | |
| 85 | Tratamiento y libertad de expresión y de información<br>Los Estados miembros conciliarán por ley el derecho a la protección de los datos personales con el derecho a la libertad de expresión y de información, incluido el tratamiento periodístico y académico, artístico o literario. | 18.1 Cumplimiento con los requisitos legales y contractuales<br>Evitar incumplimientos de obligaciones legales, estatutarias, reglamentarias o contractuales relacionadas con la seguridad de la información y con cualquier requisito de seguridad. |
| 86 | Tratamiento y acceso del público a documentos oficiales<br>Los datos de documentos personales en posesión por algún organismo público podrán ser comunicados por dicha autoridad, organismo o entidad de conformidad con el Derecho de la Unión o de los Estados miembros. | 18.1 Cumplimiento con los requisitos legales y contractuales<br>Evitar incumplimientos de obligaciones legales, estatutarias, reglamentarias o contractuales relacionadas con la seguridad de la información y con cualquier requisito de seguridad. |

| GDPR | | ISO/IEC 27002:2013 |
|---|---|---|
| **Artículo** | **Título del artículo y breve descripción** | **Objetivos de control relacionados** |
| 87 | Tratamiento del número nacional de identificación<br>Los Estados miembros podrán determinar adicionalmente condiciones específicas para el tratamiento del número nacional de identificación personal. | 18.1 Cumplimiento con los requisitos legales y contractuales<br>Evitar incumplimientos de obligaciones legales, estatutarias, reglamentarias o contractuales relacionadas con la seguridad de la información y con cualquier requisito de seguridad. |
| 88 | Tratamiento en el ámbito laboral<br>Los Estados miembros podrán, a través de disposiciones legislativas o de convenios colectivos, establecer normas específicas para garantizar la protección de los derechos y libertades de los trabajadores. | 18.1 Cumplimiento con los requisitos legales y contractuales<br>Evitar incumplimientos de obligaciones legales, estatutarias, reglamentarias o contractuales relacionadas con la seguridad de la información y con cualquier requisito de seguridad. |
| 89 | Garantías y excepciones aplicables al tratamiento con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos<br>El tratamiento con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos estará sujeto a las garantías adecuadas para respetar la minimización de los datos personales y la seudonimización. | 18.1 Cumplimiento con los requisitos legales y contractuales<br>Evitar incumplimientos de obligaciones legales, estatutarias, reglamentarias o contractuales relacionadas con la seguridad de la información y con cualquier requisito de seguridad. |
| 90 | Obligaciones de secreto<br>Los Estados miembros podrán adoptar normas específicas relativas a la obligación de secreto profesional o a otras obligaciones de secreto equivalentes. | 18.1 Cumplimiento con los requisitos legales y contractuales<br>Evitar incumplimientos de obligaciones legales, estatutarias, reglamentarias o contractuales relacionadas con la seguridad de la información y con cualquier requisito de seguridad. |
| 91 | Normas vigentes sobre protección de datos de las iglesias y asociaciones religiosas<br>Las normas vigentes sobre protección de datos de las iglesias y asociaciones religiosas podrán seguir aplicándose, siempre que sean conformes con la GDPR. | 18.1 Cumplimiento con los requisitos legales y contractuales<br>Evitar incumplimientos de obligaciones legales, estatutarias, reglamentarias o contractuales relacionadas con la seguridad de la información y con cualquier requisito de seguridad. |
| *Capítulo X – Actos delegados y actos de ejecución* | | |
| 92 | Ejercicio de la delegación<br>Los poderes para adoptar actos delegados otorgados a la CE serán por tiempo indefinido a partir del 24 de mayo de 2016 y podrán ser revocados en cualquier momento por el Parlamento Europeo (PE) o por el Consejo. | 18.1 Cumplimiento con los requisitos legales y contractuales<br>Evitar incumplimientos de obligaciones legales, estatutarias, reglamentarias o contractuales relacionadas con la seguridad de la información y con cualquier requisito de seguridad. |
| 93 | Procedimiento de comité<br>La CE estará asistida por un comité en el sentido del Reglamento (UE) nº 182/2011. | 18.1 Cumplimiento con los requisitos legales y contractuales<br>Evitar incumplimientos de obligaciones legales, estatutarias, reglamentarias o contractuales relacionadas con la seguridad de la información y con cualquier requisito de seguridad. |
| *Capítulo XI – Disposiciones Finales* | | |
| 94 | Derogación de la Directiva 95/46/CE<br>Se deroga la Directiva 95/46/CE con efecto a partir del 25 de mayo de 2018. | 18.1 Cumplimiento con los requisitos legales y contractuales<br>Evitar incumplimientos de obligaciones legales, estatutarias, reglamentarias o contractuales relacionadas con la seguridad de la información y con cualquier requisito de seguridad. |
| 95 | Relación con la Directiva 2002/58/CE<br>La GDPR no impondrá obligaciones adicionales a las personas físicas o jurídicas en materia de tratamiento de datos en ámbitos en los que estén sujetas a | 18.1 Cumplimiento con los requisitos legales y contractuales<br>Evitar incumplimientos de obligaciones legales, estatutarias, reglamentarias o contractuales relacionadas |

| GDPR | | ISO/IEC 27002:2013 |
|---|---|---|
| **Artículo** | **Título del artículo y breve descripción** | **Objetivos de control relacionados** |
| | obligaciones específicas con el mismo objetivo establecidas en la Directiva 2002/58/CE. | con la seguridad de la información y con cualquier requisito de seguridad. |
| 96 | Relación con acuerdos celebrados anteriormente<br>Los acuerdos internacionales relativos a la transferencia de datos personales acordados por los Estados miembros antes del 24 de mayo de 2016 seguirán en vigor hasta que sean modificados, sustituidos o revocados. | 18.1 Cumplimiento con los requisitos legales y contractuales<br>Evitar incumplimientos de obligaciones legales, estatutarias, reglamentarias o contractuales relacionadas con la seguridad de la información y con cualquier requisito de seguridad. |
| 97 | Informes de la Comisión<br>A más tardar el 25 de mayo de 2020 y posteriormente cada cuatro años, la CE presentará al PE y al Consejo un informe sobre la evaluación y revisión del presente Reglamento. Los informes se harán públicos. | 18.1 Cumplimiento con los requisitos legales y contractuales<br>Evitar incumplimientos de obligaciones legales, estatutarias, reglamentarias o contractuales relacionadas con la seguridad de la información y con cualquier requisito de seguridad. |
| 98 | Revisión de otros actos jurídicos de la Unión en materia de protección de datos<br>La CE presentará propuestas legislativas para modificar otros actos jurídicos de la UE en materia de protección de datos personales, a fin de garantizar la protección uniforme y coherente de las personas físicas en relación con el tratamiento. | 18.1 Cumplimiento con los requisitos legales y contractuales<br>Evitar incumplimientos de obligaciones legales, estatutarias, reglamentarias o contractuales relacionadas con la seguridad de la información y con cualquier requisito de seguridad. |
| 99 | Entrada en vigor y aplicación<br>Se indica la fecha de entrada en vigor de la GDPR. Será aplicable a partir del 25 de mayo de 2018. | 18.1 Cumplimiento con los requisitos legales y contractuales<br>Evitar incumplimientos de obligaciones legales, estatutarias, reglamentarias o contractuales relacionadas con la seguridad de la información y con cualquier requisito de seguridad. |

*Tabla 3 – Relación entre la GDPR y la ISO/IEC 27002*

# 7. Guía de controles de fácil implantación (ISO27K)

*La ISO27002:2013 dispone de muchos controles. ¿Se necesitan aplicar todos ellos?*

En secciones previas se ha introducido la necesidad de realizar una gestión de riesgos como punto de partida para la selección de los controles que se van a aplicar en la organización. Es de imaginar que, dependiendo del tamaño, madurez, recursos, etc., podrán existir un número indeterminado de controles y por lo tanto, se tendrán que seleccionar los relevantes para la organización. Si nos atenemos a los 114 controles disponibles en la ISO/IEC 27002:2013 se tratará de un arduo trabajo para una PYME. Además, será necesario tener en cuenta las regulaciones a las que se ven sometidas. El capítulo anterior ha introducido el concepto de la GDPR y una posible relación con la ISO/IEC 27002:2013 que nos ayudará a realizar la selección de al menos aquellos objetivos de control que sería recomendable considerar para la guía y que en modo alguno debería sustituir la selección de controles basada en una evaluación de los riesgos específicos que afronta la organización.

Las siguientes secciones exponen la importancia de crear el documento de Declaración de Aplicabilidad (DdA), conocido en su acepción inglesa como Statement of Aplicability (SoA), y se propone una guía de aplicación de controles para las PYME.

## 7.1. Declaración de Aplicabilidad (DdA)

La Declaración de Aplicabilidad (DdA) es un documento con una relevancia fundamental de cara a la implementación de una política de seguridad de la organización puesto que es el enlace entre la gestión de los riesgos y la implementación de la política. Sugiere los controles a aplicar y como se llevará a cabo. Forma parte de la lista de documentos obligatorios para el cumplimiento del estándar ISO/IEC 27001.

Algunos de los beneficios son los siguientes:

- Permite identificar aquellos controles que son requeridos por varias razones (p.ej. regulaciones, contractos con proveedores, procesos internos, etc), y no solamente por la necesidad de ser mitigados después de realizarse el análisis de riesgos.
- Permite justificar las razones por las que se aplican unos controles o bien se excluyen.
- El documento es relativamente sencillo comparado con un informe de evaluación de riesgos. Se puede actualizar de manera relativamente fácil y rápida.
- Además de indicar si los controles han sido seleccionados o excluídos, describe como puede ser aplicado. Normalmente se puede hacer referencia a alguna política, procedimiento o proceso, etc.
- Si la organización quiere implementar un SGSI, deberá disponer de una DdA.
- Suele ser utilizado para las auditorias internas o externas para el seguimiento de la política de seguridad de la información.
- Se puede reducir el número de documentos.
- Puede ayudar a las organizaciones a trabajar de una forma sistemática.
- Permite realizar una comparativa de los controles actualmente implementados con los recomendados en el estándar ISO/IEC 27001.

Una DdA puede tener el formato que interese a la organización, esto es, no existe un modelo predefinido. No obstante se recomiendan como mínimo los que contiene la tabla siguiente:

| Control | Seleccionado | Justificación selección | Implementado | Justificación exclusión | Referencia |
|---|---|---|---|---|---|
| A6.1.1 | ✔ | Se requiere definir los roles y responsabilidades de los recursos humanos que forman parte de la organización. | ✔ | | REF-01-02.3 Roles-Responsabilidades |
| A15.2.2 | ✘ | | | Los proveedores no disponen acceso a los activos ni existe una gestión de servicios con ellos. | |

*Tabla 4 – Ejemplo de formato de DdA*

## 7.2. Guía de controles para PYME

En el capítulo anterior se ha realizado el ejercicio de presentar la relación entre la GDPR, regulación de obligatorio cumplimiento para las PYME y la ISO/IEC 27002:2013. La gran mayoría de controles deberían ser utilizados para cumplir la GDPR pero también se puede dar el caso que, si la empresa está interesada en poder obtener la certificación ISO27001, debería tener en cuenta que algunos controles deberían ser aplicados de forma obligatoria y otros serían recomendables.

La guía que se propone identificará por objetivo de control, aquellos controles que se consideran necesarios para cumplir con la regulación, aquellos que tienen documentos obligatorios para el cumplimiento de la ISO/IEC 27001:2013 y una serie de recomendaciones que ayudan a su implementación.

Por tanto, los valores relativos a la GDPR son como sigue:

- Obligatorio – Se considera obligatorio para el cumplimiento de la regulación.
- No obligatorio – Se considera no estrictamente necesario.

Con respecto a la ISO/IEC 27001:2013:

- Sí – Se considera un control necesario puesto que produce o contribuye a crear documentos o registros obligatorios para el cumplimiento de la ISO27001.
- No – Puede producir documentos que no son obligatorios para el cumplimiento de la ISO/IEC 27001:2013 (aunque algunos pueden ser de uso común).

En cualquier caso, como ya se ha indicado anteriormente, si las organizaciones quieren aplicar la ISO/IEC 27001:2013, tendrán la posibilidad de indicar aquellos controles que se han utilizado y los que no se requieren. La Declaración de Aplicabilidad mostraría las razones.

Esta guía servirá como base para el supuesto ficticio que se muestra en el siguiente capítulo.

## 5.1 Dirección de gestión para la seguridad de la información

Proporciona dirección de gestión y soporte para la seguridad de la información de acuerdo con los requisitos de negocio, leyes y regulaciones relevantes.

| | GDPR | Docs / Regs ISO27001 |
|---|---|---|
| 5.1.1 Políticas para la seguridad de la información | Obligatorio | Sí |
| 5.1.2 Revisión de las políticas para seguridad de la información | Obligatorio | Sí |

**Notas y recomendaciones**

Es un objetivo de control fundamental puesto que establece las políticas de seguridad que deberá llevar a cabo la organización según los requisitos de negocio y las legislaciones vigentes. Deberá recoger el compromiso de la alta dirección.

Se debe por otra parte considerar que se tendría que revisar su contenido de manera regular para asegurar el correcto funcionamiento de la seguridad de la información.

Estas políticas deberían recoger gran parte del resto de objetivos de control aquí presentados. Algunos ejemplos de aspectos a considerar podrían ser: gestión de acceso de identidad, clasificación de los activos, seguridad física del entorno, sistemas de backup, formación a los empleados, controles de encriptación, seguridad en las comunicaciones, gestión de las vulnerabilidades técnicas, etc.

Recomendaciones [14]

- Aplicar un ciclo de vida para la revisión de su contenido (creación, discusión, aprobación y finalmente difusión y consolidación).
- No utilizar una política de seguridad de otra compañía. Se debe crear una propia según los objetivos de negocio.
- La dirección debe aprobarla y estar comprometida en su aplicación en todo momento.
- Comunicar a toda la organización y otras partes que accedan a información que requiera una seguridad. Se deberá exigir así mismo su aplicación.
- No es necesario que sea muy extensa para evitar que no se lea.
- Hacer referencia a las normativas que sean posibles de aplicación (p.ej. GDPR o LOPDP).
- Revisar la política de manera periódica.

## 6.1 Organización interna

Establecer un marco de trabajo de gestión para iniciar y controlar la implementación y la operación de la seguridad de la información dentro de la organización.

| | GDPR | Docs / Regs ISO27001 |
|---|---|---|
| 6.1.1 Roles y responsabilidades para la seguridad de información | Obligatorio | No |
| 6.1.2 Separación de deberes | Obligatorio | No |
| 6.1.3 Contacto con las autoridades | Obligatorio | No |
| 6.1.4 Contacto con grupos de interés especial | No obligatorio | No |
| 6.1.5 Seguridad de la información en la gestión de proyectos | No obligatorio | No |

**Notas y recomendaciones**

La organización deberá definir las responsabilidades y roles de los responsables de la información. Un aspecto fundamental es la asignación de un responsable de la seguridad que se encargará de la coordinación y control de todas las medidas de seguridad. De igual forma será precisa la identificación de todos los procesos y asignarles un responsable de los mismos. Esta información debería ser recogida en un documento.

Se debería establecer una separación de deberes para evitar acciones no deseadas en los activos de la organización.

El contacto con las autoridades de control es fundamental de manera que, en caso de incidente de seguridad, se puedan tomar acciones adecuadas. Principalmente las autoridades de supervisión y las encargadas para el cumplimiento de las leyes. El contacto con grupos de interés no es especialmente necesario aunque podría ayudar en la comprensión y gestión futura de la seguridad de la información. Si la política de seguridad establecida en el objetivo de control 5.1, la gestión de proyectos podría aplicar de manera directa la seguridad a la hora del tratamiento de los datos.

Recomendaciones

- Identificar los procesos y asignar un responsable por cada uno de ellos.
- Intentar evitar que haya una colusión de deberes aun siendo una PYME donde puede ser difícil hacer la separación de deberes.
- El responsable de la seguridad debe tener conocimiento de los objetivos de negocio.
- El responsable de la seguridad debe encargarse de la asignación de los activos según los objetivos de negocio.
- Definir procedimientos de contacto con las autoridades los pasos a seguir en caso de incidente de seguridad (p. ej. a quien contactar, cuando). De igual forma, se podría informar a otros grupos de interés.
- Si la organización dispone de un CERT, establecer contacto con otros CERTs para compartir información.
- Participar en conferencias sobre seguridad de información para afianzar contactos con grupos de interés.

## 6.2 Dispositivos móviles y teletrabajo

Asegurar la seguridad del teletrabajo y el uso de los aparatos móviles.

| | GDPR | Docs / Regs ISO27001 |
|---|---|---|
| 6.2.1 Política para dispositivos móviles | No obligatorio | No |
| 6.2.2 Teletrabajo | No obligatorio | No |

**Notas y recomendaciones**

No se considera obligatorio en tanto en cuanto no se trabaje con dispositivos móviles y se pueda teletrabajar. Ahora bien, considerando el amplio uso de las nuevas tecnologías, es un objetivo a tener muy en cuenta. La política "Bring Your Own Device" (BYOD), esto es, uso de aparatos personales para acceso a activos de las compañía, está comenzando a ser ampliamente utilizada (p.ej. acceso a email u otras aplicaciones corporativas).

La organización debería establecer medidas de control en caso de no utilización de los equipos disponibles en las instalaciones de la compañía.

Recomendaciones

- Identificar los dispositivos móviles con acceso a las aplicaciones corporativas.
- Limitar el acceso a ciertas aplicaciones corporativas.
- Impedir la instalación de aplicaciones sin la aprobación del administrador.
- Obligatoriedad de actualización de software bien sea en dispositivos móviles o maquinas para el teletrabajo.
- Uso de VPN u comunicaciones encriptadas para la conexión a cualquier aplicación corporativa sensible.
- En caso de teletrabajo, impedir el acceso a herramientas de almacenamiento en la nube (p.ej. Dropbox).
- Utilizar un seguro que cubra posibles incidencias producidas por el acceso a datos mediante teletrabajo.

## 7.1 Previo al empleo

Asegurar que los empleados y los contratistas comprenden sus responsabilidades y que sean adecuadas para los roles para los que son considerados.

| | GDPR | Docs / Regs ISO27001 |
|---|---|---|
| 7.1.1 Selección | No obligatorio | No |
| 7.1.2 Términos y condiciones del empleo | No obligatorio | Sí |

**Notas y recomendaciones**

A la hora de contratar empleados o bien servicios a otros contratistas, se requiere que exista un control previo para evitar el acceso a información sensible de la compañía. Se deberían estudiar los antecedentes de los potenciales candidatos para considerar que son exactamente lo que la organización necesita. Es estrictamente necesario que se firme como mínimo un acuerdo de confidencialidad y no divulgación de información y se presenten sus responsabilidades y roles que van a tener a partir de la firma del contrato.

Recomendaciones

- Utilizar un formulario con el acuerdo de confidencialidad y no divulgación de la información.
- Presentar las políticas de seguridad de la organización con las obligaciones a las que deberá acogerse el nuevo empleado.
- Presentar las responsabilidades para la clasificación de la información que deberá seguir el nuevo empleado o contratista.
- En la medida de lo posible, solicitar un registro de antecedentes penales (fácilmente obtenible en España en cualquier Gerencia Territorial del Ministerio de Justicia).
- Estudiar la carrera profesional de la persona que opta a un puesto determinado (p.ej. CV, LinkedIn, páginas web en las que comparte información relacionada con el puesto al que aspira).
- Verificar las calificaciones y certificaciones obtenidas (p.ej. título universitario, certificados profesionales, etc).
- Confirmar mediante entrevistas personales que el nuevo recurso o contratista cumple con los requisitos del puesto al que aplica.

## 7.2 Durante el empleo

Asegurar que los empleados y contratistas conozcen y cumplen con sus responsabilidades de seguridad de la información.

| | GDPR | Docs / Regs ISO27001 |
|---|---|---|
| 7.2.1 Responsabilidades de la dirección | No obligatorio | No |
| 7.2.2 Toma de conciencia, educación y formación en la seguridad de la información | No obligatorio | No |
| 7.2.3 Proceso disciplinario | No obligatorio | No |

**Notas y recomendaciones**

No se considera estrictamente necesario aunque sí altamente recomendable. La dirección tiene que promover una cultura enfocada en la aplicación de las medidas de seguridad. Debe asegurar que se definen los roles y responsabilidades de los empleados y dar soporte a las políticas de seguridad de la información.

Se recomienda proporcionar una formación a los empleados y potenciar la concienciación a través de distintos medios como podría ser la asistencia a seminarios, realización de cursos especializados, información disponible en alguna aplicación corporativa, etc. Convendría que dicha información explique las razones por las que el empleado o contratista debe prestar atención a la seguridad de la información, los tipos de controles y procedimientos existentes para el tratamiento de los datos, la necesidad de seguir las normativas vigentes.

Por otra parte, se propone establecer un proceso disciplinario en caso de que se haya violado la seguridad.

Recomendaciones

- Realizar seminarios o cursos sobre seguridad de la información de manera regular y obligatorios. Pueden ser cursos creados *ad hoc* en la organización o incluso utilizar algunos gratuitos disponibles en Internet. No deberían ser técnicos en la medida de lo posible aunque también se podría dar acceso a cursos más especializados dependiendo de la estructura de la organización.
- La dirección debería notificar la obligatoriedad de realizar la formación proporcionada a través de correos corporativos, publicación en la intranet de la compañía si la hay, pequeños folletos explicativos que podrían ser complemento de los cursos ofrecidos, etc.
- En caso de brecha de seguridad, convendría asegurarse que hay un tratamiento adecuado con los empleados responsables del problema. Según como se defina la aplicación del proceso disciplinario podrá ser considerado como disuasorio para evitar la violación de seguridad de manera intencionada pero si se aplica con la misma firmeza en caso de ser producto de una acción involuntaria, podría generar un conflicto interno con los empleados.

## 7.3 Terminación o cambio de empleo

Proteger los intereses de la organización como parte del proceso de cambio o terminación del empleo.

| | GDPR | Docs / Regs ISO27001 |
|---|---|---|
| 7.3.1 Terminación o cambio de responsabilidades de empleo | No obligatorio | No |

**Notas y recomendaciones**

El objetivo de control no se considera obligatorio pero sí recomendable. En caso de que el empleado o contratista deje el empleo, deberá seguir manteniendo las responsabilidades de forma vinculante con la seguridad de la información que había aceptado anteriormente cuando formaba parte de la organización.

Recomendaciones

- Establecer cláusulas de confidencialidad en el contrato del empleado para evitar fugas de información en caso de rescisión de su contrato al menos por cierto período de tiempo.

## 8.1 Responsabilidad por los activos

Identificar activos organizativos y definir responsabilidades de protección apropiadas.

| | GDPR | Docs / Regs ISO27001 |
|---|---|---|
| 8.1.1 Inventario de activos | Obligatorio | Sí |
| 8.1.2 Propiedad de los activos | Obligatorio | No |
| 8.1.3 Uso aceptable de los activos | Obligatorio | Sí |
| 8.1.4 Devolución de activos | Obligatorio | No |

**Notas y recomendaciones**

La organización debería identificar todos sus activos de forma que pueda posteriormente asignarles un propietario que seguirá unas reglas determinadas para su uso.

En caso de rescisión de su contrato, el empleado o contratista tendrá que devolver los activos de los que eran propietarios.

Recomendaciones

- Incluir una cláusula de propiedad intelectual sobre los activos de la organización que se puedan crear en el desempeño de su puesto de trabajo (p.ej. desarrollo de alguna aplicación de software, diseño de una herramienta industrial, etc).
- Incluir una cláusula en el contrato del empleado o contratista de forma que sean conscientes de que todos los activos de los que serán propietarios tendrán que ser devueltos a la extinción de sus contratos.

## 8.2 Clasificación de la información

Asegurar que la información recibe un nivel apropiado de protección de acuerdo con su importancia para la organización.

| | GDPR | Docs / Regs ISO27001 |
|---|---|---|
| 8.2.1 Clasificación de la información | Obligatorio | No |
| 8.2.2 Etiquetado de la información | No obligatorio | No |
| 8.2.3 Manejo de activos | Obligatorio | No |

**Notas y recomendaciones**

La información deberá ser clasificada y etiquetada según lo defina la política de seguridad definida por la organización teniendo en cuenta los objetivos de negocio y los propietarios previamente asignados.

El uso de los activos se deberá llevar a cabo siguiendo los procedimientos adoptados y dependerá de las restricciones de acceso.

Recomendaciones

- Los activos podrían etiquetarse mediante el uso similar de una CMDB.
- Establecer una clasificación de la confidencialidad de la información (p.ej. "público", "interno", "confidencial", etc).
- Disponer de una manera normalizada de etiquetar los activos.
- Tener un registro histórico de los propietarios de los activos.

## 8.3 Manipulación de media

Prevenir la divulgación, modificación, eliminación o destrucción no autorizada de la información almacenada en los medios.

| | GDPR | Docs / Regs ISO27001 |
|---|---|---|
| 8.3.1 Gestión de medios removibles | No obligatorio | No |
| 8.3.2 Eliminación de los medios | Obligatorio | No |
| 8.3.3 Transferencia de medios físicos | No obligatorio | No |

**Notas y recomendaciones**

La organización debería establecer procedimientos para la manipulación de los medios según la clasificación de los activos. Así mismo se requería definir la gestión para los medios que dejan de ser útiles.

En caso de necesitar el traslado de medios físicos, se aconseja establecer una protección mediante servicios de mensajería confiables.

Recomendaciones

- Los medios móviles deberían almacenarse de forma segura como por ejemplo armarios con llave de forma que no se tenga acceso a excepción del propietario.
- Aplicar sistemas de encriptación para la transmisión de información a través de medios móviles como pendrives, discos duros externos, comunicaciones, etc.
- Realizar copias de seguridad de la información para evitar daños en datos sensibles.
- Inutilizar o impedir el uso de aquellos dispositivos móviles que han contenido información sensible y que ya no se necesitan.
- Crear un registro de aquellos medios que han dejado de utilizarse identificando los datos sensibles que contenían para poder realizar un seguimiento.
- Contratar servicios de mensajería con reputación en caso de transferencia de medios físicos. Según el contenido, se deberá considerar un tratamiento específico en el transporte (p.ej. indicando su fragilidad y por tanto, sería tratado como un servicio especial de envío).

## 9.1 Requisitos de negocio para el control de acceso

Limitar el acceso a la información y las instalaciones de procesamiento de la información.

| | GDPR | Docs / Regs ISO27001 |
|---|---|---|
| 9.1.1 Política de control de acceso | Obligatorio | Sí |
| 9.1.2 Política sobre el uso de los servicios de red | Obligatorio | Sí |

**Notas y recomendaciones**

Las organizaciones tienen que establecer una política de control de acceso. El acceso tiene que darse a aquellos usuarios que estén autorizados. Para ello se deberán considerar las aplicaciones de negocio, la clasificación de la información que previamente debe realizarse, las regulaciones a las que la organización está sujeta, la separación de deberes. De igual forma se requiere gestionar la eliminación de los derechos de acceso.

Los servicios de red deberán ser monitorizados e identificados aquellos a los que se tiene acceso. Se deberán establecer procedimientos de conexión.

Recomendaciones

- Tener siempre en cuenta los requisitos de seguridad definidos en la política de seguridad de la organización.
- Establecer una separación de roles para el acceso. Por ejemplo, roles de administración, de usuario, por departamento, por servicios operativos, etc. Algunos de esos roles podrán disponer de ciertos privilegios.
- Revisar con cierta periocidad los derechos de acceso de los usuarios. Puede darse el caso que haya una reorganización de la compañía y por tanto, ante la nueva estructura, los derechos se modifiquen para ciertos usuarios.
- Considerar que los roles puedan ser utilizados en más de un entorno distribuido en red. Es decir, los roles podrán ser los mismos pero convendría gestionarlos de manera centralizada.
- Establecer el tipo de acceso a los entornos distribuidos o a los servicios de la red (p. ej entornos no complejos que utilizan Wifi, VPNs para posibilidad de teletrabajar, MVPN para mantener las sesiones de conexión abiertas si se disponen de varios puntos de acceso WiFi, etc).
- Realizar un seguimiento de los servicios de red de la organización.

## 9.2 Gestión de acceso de usuarios

Asegurar el acceso de usuario autorizado y prevenir el acceso no autorizado a los sistemas y servicios.

| | GDPR | Docs / Regs ISO27001 |
|---|---|---|
| 9.2.1 Registro y cancelación del registro de usuarios | Obligatorio | No |
| 9.2.2 Suministro de acceso de usuarios | No obligatorio | No |
| 9.2.3 Gestión de derechos de acceso privilegiado | No obligatorio | No |
| 9.2.4 Gestión de información de autenticación secreta de usuarios | Obligatorio | No |
| 9.2.5 Revisión de los derechos de acceso de usuarios | No obligatorio | No |
| 9.2.6 Retiro o ajuste de los derechos de acceso | No obligatorio | No |

**Notas y recomendaciones**

Se tienen que definir los procesos para registrar y cancelar el registro de los usuarios, suministrar y gestionar el acceso de los usuarios tanto en su asignación como en su revisión y eliminación.

Recomendaciones

- Los identificadores deben ser únicos y asignados según las operaciones que van a desempeñar en la organización.
- Verificar que no existen identificadores de usuario repetidos.
- En caso de que un usuario deje de colaborar con la organización, eliminar esos identificadores de usuario.
- Las responsables de empleados deben encargarse de dar su autorización de acceso.
- Centralizar la gestión de acceso de usuario en lugar de utilizar sistemas distribuidos.
- Definir la forma de identificar los accesos privilegiados según las operaciones que desempeñen ciertos usuarios así como la manera de eliminarlos sin que por ello afecten a sus actividades.
- Definir un proceso específico para la gestión de información de autenticación secreta de usuarios. Por ejemplo, la autenticación debe ser difícilmente adivinable, en caso de ofrecer una autenticación inicial, obligar a un cambio de contraseña justo en el primer uso de la misma.
- Revisar los derechos de acceso de manera regular.
- Eliminar los derechos de accesos a aquellos empleados o contratistas que han dejado de colaborar en la organización.

## 9.3 Responsabilidades de los usuarios

Asegurar que los usuarios sean responsables para la salvaguarda de la información de autenticación.

| | GDPR | Docs / Regs ISO27001 |
|---|---|---|
| 9.3.1 Uso de la información de autenticación secreta | Obligatorio | No |

**Notas y recomendaciones**

Los usuarios tienen que ser responsables de la información de su autenticación. No deben compartirla bajo ningún concepto.

Recomendaciones

- Los usuarios no deben distribuir la información de su autenticación ni siquiera a sus responsables. Debe considerarse como información personal.
- La información de acceso no debe ser fácilmente accesible. Por ejemplo no debe guardarse en papeles fácilmente accesibles como post-it, no almacenarse en ficheros no encriptados, etc.
- Utilizar contraseñas con una longitud mínima de 8 caracteres utilizando letras mayúsculas, minúsculas, números y simbolos especiales.
- Las contraseñas deben ser difíciles de adivinar. Se pueden utilizar reglas nemotécnicas para evitar que se olviden.
- No utilizar las mismas contraseñas que se utilizan en el ámbito personal y profesional.
- Modificar la contraseña en caso de considerar que se ha visto comprometida por algún medio.

## 9.4 Control de acceso a sistemas y aplicaciones

Prevenir el acceso no autorizado a los sistemas y aplicaciones.

| | GDPR | Docs / Regs ISO27001 |
|---|---|---|
| 9.4.1 Restricción de acceso a la información | Obligatorio | No |
| 9.4.2 Procedimiento de ingreso seguro | Obligatorio | No |
| 9.4.3 Sistema de gestión de contraseñas | Obligatorio | No |
| 9.4.4 Uso de programas utilitarios privilegiados | No obligatorio | No |
| 9.4.5 Control de acceso a códigos fuente de programas | No obligatorio | No |

**Notas y recomendaciones**

El acceso a la información debe restringirse según la política de seguridad de la organización y debe asegurarse la posibilidad de acceder sin necesidad de ofrecer información extra que facilite un posible acceso no autorizado futuro.

En la medida de lo posible se tendrá que limitar el uso de programas de utilidades capaces de proporcionar privilegios de acceso. En caso de uso, se deberán utilizar procedimientos de identificación, autenticación y autorización.

Se tiene que evitar el acceso al código fuente de los programas informáticos para prevenir la introducción de código malintencionado.

Recomendaciones

- Mostrar información al usuario indicando donde puede tener acceso.
- Controlar los derechos de acceso de los usuarios y aplicación según permisos de lectura, escritura y ejecución.
- Aislar aquellos sistemas y aplicaciones sensibles de otras aplicaciones para que no puedan acceder a sus datos.
- Limitar el número de intentos de acceso a las aplicaciones. Por ejemplo, si no se ha introducido correctamente la contraseña en 3 intentos seguidos, impedir que se vuelva a introducir durante los siguientes 30 minutos.
- Establecer controles CAPTCHA para el acceso a determinados sistemas o aplicaciones.
- Ocultar los campos de contraseñas con asteriscos u otros símbolos para evitar ser mostrado en pantalla.
- Si se envían contraseñas a través de la red, siempre deberá ser de modo encriptado.
- Si se detecta un posible acceso no autorizado, se deberá generar un evento de seguridad que informe al menos al responsable de seguridad de la información.
- Cerrar el acceso de la sesión después de un período de inactividad.
- Obligar al usuario a cambiar su contraseña cuando accede la primera vez a un sistema o aplicación.
- En caso de disponer de software creado en la organización, limitar el acceso a su código fuente a aquellas personas con derecho según las políticas de seguridad establecidas.
- Limitar el uso de programas de utilidades que proporcionen privilegios de acceso.

## 10.1 Controles criptográficos

Asegurar el uso apropiado y efectivo de la criptografía para proteger la confidencialidad, autenticación y/o la integridad de la información.

| | GDPR | Docs / Regs ISO27001 |
|---|---|---|
| 10.1.1 Política sobre el uso de controles criptográficos | No obligatorio | No |
| 10.1.2 Gestión de claves | No obligatorio | No |

**Notas y recomendaciones**

La organización debe aplicar una política de encriptación para la protección de la información que siempre deberá proteger la confidencialidad, autenticación y/o la integridad y se deberá utilizar para todo el ciclo de vida tanto para la generación, almacenado o destrucción de las claves.

Recomendaciones

- La dirección debe presentar la necesidad de utilizar comunicaciones encriptadas en todo momento para evitar el acceso no deseado a información sensible. Convendría utilizar VPNs en caso de comunicaciones remotas.
- El nivel de encriptación deberá ser acorde con la información sensible.
- El responsable de la seguridad de información debería gestionar la política de encriptación.
- La gestión de las claves encriptadas debe seguir estándares y/o mejores prácticas.

## 11.1 Áreas seguras

Prevenir el acceso físico no autorizado, daños e interferencias a las instalaciones de procesamiento de información e información de la organización.

| | GDPR | Docs / Regs ISO27001 |
|---|---|---|
| 11.1.1 Perímetro de seguridad física | No obligatorio | No |
| 11.1.2 Controles físicos de entrada | No obligatorio | No |
| 11.1.3 Seguridad de oficinas, recintos e instalaciones | No obligatorio | No |
| 11.1.4 Protección contra amenazas externas y ambientales | No obligatorio | No |
| 11.1.5 Trabajo en áreas seguras | No obligatorio | No |
| 11.1.6 Áreas de carga y descarga | No obligatorio | No |

**Notas y recomendaciones**

Aun no siendo controles obligatorios, es totalmente recomendable que la organización ponga especial interés en la seguridad física de las instalaciones puesto que un acceso no autorizado o bien peligros medioambientales pueden afectar seriamente a la confidencialidad, integridad o disponibilidad de la información.

La organización debe proteger las áreas que tengan una relación directa con la gestión de información sensible por ejemplo utilizando cierres con candado u otro tipo de dispositivo. Su acceso dependerá de los usuarios autorizados. Las zonas de carga y descarga deben tener una protección especial para evitar que personas ajenas a la organización no puedan acceder a información sensible.

Deberá gestionar las entradas y salidas a las instalaciones. Existirá un registro de acceso y se aconseja no dejar a personas ajenas a la organización sin acompante en todo momento.

Conviene no mostrar demasiada información del lugar donde se gestionan los datos sensibles.

Aunque las PYME no tienen un tamaño elevado, las puede haber de unos 200 empleados, por lo tanto en caso de un número similar de trabajadores, se recomendaría llevar una tarjeta identificativa.

La localización de la compañía debería estar en la medida de lo posible alejada de zonas con posibles amenazas medioambientales como inundaciones, avalanchas de lodo, etc.

Recomendaciones

- Separar las zonas de trabajo en las que se dispone de información sensible de aquellas que no la manipulan. Por ejemplo, zona de atención al cliente, zona de almacenamiento de material, zona de área de carga y descarga, zona de equipos informáticos (p.ej. servidores, bases de datos, etc).
- Aplicar barreras físicas de acceso al edificio (p.ej. bolardos, verjas, etc).
- Utilizar un registro de acceso a las instalaciones. Cuando una persona visitante acceda, deberá ser acompañada en todo momento
- Disponer de extintores en todas las plantas. Utilizar alarmas antihumos e incendios
- Disponer de salidas de emergencia.
- No mostrar elementos identificativos de las zonas donde se gestionan datos sensibles. Además, se debe evitar que puedan acceder a ellas visitantes externos.
- Utilizar elementos disuasorios como alarmas contra intrusos, cámaras de circuito de televisión, guardias de seguridad, etc.
- Evitar que las instalaciones se encuentren en zonas susceptibles de sufrir alguna amenaza medioambiental como inundaciones, avalanchas de lodo, incendios, etc. Por ejemplo cerca de ríos o valles.

## 11.2 Equipos

Prevenir la pérdida, el daño, el robo o el compromiso de los activos y la interrupción de las operaciones de la organización.

| | GDPR | Docs / Regs ISO27001 |
|---|---|---|
| 11.2.1 Ubicación y protección de los equipos | No obligatorio | No |
| 11.2.2 Servicios de suministro | No obligatorio | No |
| 11.2.3 Seguridad del cableado | No obligatorio | No |
| 11.2.4 Mantenimiento de equipos | No obligatorio | No |
| 11.2.5 Retirada de activos | No obligatorio | No |
| 11.2.6 Seguridad de equipos y activos fuera de las instalaciones | No obligatorio | No |
| 11.2.7 Eliminación segura o reutilización de equipos | No obligatorio | No |
| 11.2.8 Equipos de usuario desatendidos | No obligatorio | No |
| 11.2.9 Política de escritorio limpio y pantalla limpia | No obligatorio | No |

**Notas y recomendaciones**

Estos controles también son muy recomendables. En este caso se refiere a los equipos en lugar de las instalaciones como el objetivo de control anterior.

La organización deberá proteger los equipos ante cualquier tipo de amenaza bien sea medioambiental, acceso no autorizado, etc. Tendrá que considerar las consecuencias ante fallos de las empresas de servicios públicos (electricidad, gas, aire acondicionado, etc). Deberá proteger el cableado encargado de la transmisión de datos, mantener el equipo para asegurar la disponibilidad e integridad de la información. Gestionar aquellos equipos que están fuera de las instalaciones.

También deberá especificar la necesidad de aplicar la política de "Escritorio y pantallas limpios" y detallar procedimientos para la eliminación o reutilización de equipos. De igual forma se recomienda el uso de bloqueos de pantalla una vez el equipo esté sin utilizar pasado un tiempo.

Recomendaciones

- Los equipos informáticos tendrán que estar localizados y, en el caso especial de formar parte de instalaciones de almacenamiento, deben tener una protección de seguridad.
- Se tendría que controlar la temperatura y humedad en aquellas zonas donde estén determinados equipos. Por ejemplo, en la zona de servidores y bases dedatos se recomienda instalar equipos de aire acondicionado.
- Los servicios públicos contratados como la electricidad, gas, telecomunicaciones, etc. deberían ser monitorizados para asegurar el buen funcionamiento. En caso contrario, algunos activos podrían ser dañados. Por ejemplo si se producen sobrecargas de tensión, algunas máquinas podrían malfuncionar o directamente inutilizarse.
- Intentar poner el cableado en el suelo para evitar interferencias, daños o intercepción de las comunicaciones.
- Seguir las recomendaciones de los fabricantes en cuanto al mantenimiento. De hecho, algunas aseguradoras indican este punto de cara a reembolsar indemnizaciones posteriores a un daño.
- Los activos deberán ser identificados y registrados de forma que cuando se entrega y se devuelve el activo. Incluídos aquellos que están fuera de las instalaciones.
- En el caso tanto de reutilización como inutilización de equipos, se debe asegurar que la información sensible que antes albergaba, haya sido eliminada completamente.
- Utilizar salvapantallas automáticos si el equipo no es utilizado en un período de tiempo determinado.
- Disponer de un entorno de trabajo limpio y organizado ("Clean desk policy") para evitar dejar documentación sensible disponible en todo momento.
- Intentar utilizar impresoras o escaners que funcionen sólo si el usuario utiliza su clave y contraseña o bien tarjetas de acceso identificativos. De esta manera se evita el uso no autorizado.

## 12.1 Procedimientos operacionales y responsabilidades

Asegurar operaciones correctas y seguras de las instalaciones de procesado de la información.

| | GDPR | Docs / Regs ISO27001 |
|---|---|---|
| 12.1.1 Procedimientos operacionales documentados | Obligatorio | Sí |
| 12.1.2 Gestión de cambios | No obligatorio | No |
| 12.1.3 Gestión de capacidad | No obligatorio | No |
| 12.1.4 Separación de los ambientes de desarrollo, pruebas y operación | No obligatorio | No |

**Notas y recomendaciones**

Las organizaciones deben tener todos sus procesos operacionales documentados para poder conocer la manera de trabajar, como interactúan entre ellos, que tipo de herramientas pueden necesitar, los tiempos de ejecución, etc.

Por lo general, se suelen producir cambios en las operaciones por tanto, se deben identificar y registrar normalmente a través de procedimientos que requieren una aprobación expresa de un grupo responsable de la organización. Algunos implican cambios que afecta a la capacidad o rendimiento que deben tener los sistemas.

En caso de tratarse de empresas que se dedican a desarrollar productos y posteriormente a testearlos, se recomienda separar las áreas.

Recomendaciones

- Documentar los procedimientos operativos, las maquinas utilizadas, los sistemas de almacenamiento, comunicaciones entre procesos, la planificación de los recursos, la monitorización de los sistemas.
- Gestionar los cambios que se produzcan en los procesos de negocio, organizativos, desarrollo y testeo incluyendo la planificación y comunicación con las personas directamente afectada por los cambios.
- Estudiar con antelación los requisitos futuros para la compañía y así asegurar el buen desempeño de los objetivos de negocio. Por ejemplo, necesidad de recursos en un determinado período de tiempo como en vacaciones o excendencias, nuevos equipos informáticos para futuras aplicaciones, etc.
- En el caso de empresas dedicadas a desarrollos y testeo de productos, definir procedimientos de comunicación entre los entornos. Por ejemplo, para desarrollos software, definir entornos de TEST, PreProducción y Producción. Así pues, para pasar un producto de un entorno a otro, se requerirá un testeo y validación en el entorno previo, para posteriormente desplegar el producto en el nuevo.

## 12.2 Protección contra códigos maliciosos

Asegurar que la información y las instalaciones de procesado de la información están protegidas contra los códigos maliciosos.

| | GDPR | Docs / Regs ISO27001 |
|---|---|---|
| 12.2.1 Controles contra códigos maliciosos | No obligatorio | No |

**Notas y recomendaciones**

Se trata de un objetivo recomendable. Las organizaciones están sujetas a ataques informáticos a través de códigos maliciosos. Se deben aplicar controles que impidan su ejecución. De igual forma, los empleados deberán ser conscientes puesto que gran parte de los problemas vienen a través de instalación de programas no autorizados o la no actualización de los sistemas.

Recomendaciones

- Prohibición de instalación de programas sin la aprobación del responsable de la seguridad de la información.
- Instalación de antivirus.
- Bloqueo de acceso a determinadas páginas de descargas gratuitas.
- Instalar de forma automática y obligatoria todas las actualizaciones disponibles de los fabricantes.

## 12.3 Copias de respaldo

Proteger contra la pérdida de datos.

| | GDPR | Docs / Regs ISO27001 |
|---|---|---|
| 12.3.1 Respaldo de información | Obligatorio | No |

**Notas y recomendaciones**

Se tienen que realizar siempre copias de respaldo ante posibles pérdidas de información. Controles periódicos de dichas copias son igualmente necesarios para verificar que la información no ha podido deteriorarse.

Conviene que las copias no se encuentren en el mismo sitio donde están los datos originales para evitar la destrucción de datos en ambos lugares en caso de daño en el sitio principal.

Recomendaciones

- Crear un plan de respaldo que defina cuando realizar las copias de seguridad y su periodicidad, que información almacenar, tipo de la copia de seguridad (por ejemplo, completa, incremental o diferencial).
- Almacenar las copias de seguridad en algún lugar alejado y con seguridad del sitio principal.
- Aplicar medidas de seguridad física a las copias de seguridad para evitar que se inutilicen por ejemplo en caso de algún desastre natural como una inundación.
- Realizar verificaciones periódicas de los datos de respaldo.

## 12.4 Registro y monitorización

Registrar eventos y generar evidencias.

| | GDPR | Docs / Regs ISO27001 |
|---|---|---|
| 12.4.1 Registro de eventos | No obligatorio | Sí |
| 12.4.2 Protección de la información de registro | No obligatorio | No |
| 12.4.3 Registros del administrador y del operador | No obligatorio | Sí |
| 12.4.4 Sincronización de relojes | No obligatorio | No |

**Notas y recomendaciones**

Se tienen que monitorizar todos los eventos relacionados con la seguridad de la información que se produzcan bien sea a través de las operaciones diarias como por brechas de seguridad incluidas las actividades del administrador. La información puede ser utilizada como informe de seguimiento.

Los datos recogidos deberían ser protegidos para evitar un uso no autorizado y sobre todo para garantizar su integridad de información.

Si la organización dispone de muchos sistemas, los relojes de las máquinas deberán estar sincronizados.

Recomendaciones

- Recoger la identidad de los usuarios y sus actividades incluyendo fechas, horas, eventos específicos.
- Recoger las actividades del sistema así como la fecha y hora, comunicaciones automáticas con otros sistemas.
- Recoger los privilegios utilizados.
- Recoger los ficheros utlizados y el acceso a bases de datos.
- Recoger las direcciones de red accedidas.
- Recoger los intentos y denegaciones de acceso a los sistemas.
- Recoger los cambios de configuración.
- Evitar que los registros puedan ser alterados dando como máximo permiso de lectura a ciertos usuarios.
- Los administradores, al tener acceso a los registros de eventos, deben prestar cuidado especial de no adulterar información de los mismos. Se pueden utilizar herramientas automáticas para monitorizar el estado de los registros.
- Cuando se dispone de varios sistemas, se recomienda sincronizar los relojes de la máquina para evitar que mismos registros tengan distintas horas.

## 12.5 Control de software operacional

Asegurar la integridad de los sistemas operacionales.

| | GDPR | Docs / Regs ISO27001 |
|---|---|---|
| 12.5.1 Instalación de software en sistemas operativos | No obligatorio | No |

**Notas y recomendaciones**

Se deben desarrollar procedimientos a la hora de instalar software para asegurar que no se trata de código malicioso o simplemente aplicaciones que puedan afectar al rendimiento de aplicaciones corporativas.

Recomendaciones

- Las instalaciones sólo las debería llevar a cabo el administrador.
- Deberán ser aplicaciones aprobadas por la Dirección y en modo ejecutable. En ningún caso código interpretado por máquinas virtuales, macros, etc.
- Deberá existir un plan de respaldo en caso de que la instalación no ha sido satisfactoria. Para ello se puede mantener la versión anterior que será eliminada una vez verificado que la nueva funciona correctamente.
- Deberá haber un registro de todas las aplicaciones instaladas o eliminadas.

## 12.6 Gestión de la vulnerabilidad técnica

Prevenir la explotación de las vulnerabilidades técnicas.

| | GDPR | Docs / Regs ISO27001 |
|---|---|---|
| 12.6.1 Gestión de las vulnerabilidades técnicas | No obligatorio | No |
| 12.6.2 Restricciones sobre la instalación de software | No obligatorio | No |

**Notas y recomendaciones**

Las vulnerabilidades técnicas se tendrán que recoger de manera sistemática de forma que la organización tenga en cuenta de antemano como afrontar su potencial impacto. Convendrá definir los roles y responsabilidades de las personas encargadas de tratarlas, el tiempo de reacción y monitorizar si dicha gestión es correcta o necesita revisión. Si se identifica una vulnerabilidad, la organización deberá indicar el riesgo a la que se puede ver sometida.

Por otra parte, al igual que en objetivo de control anterior, se necesitan definir unas restricciones a la instalación de software.

Recomendaciones

- Definir roles y responsabilidades de las personas encargadas de la gestión de vulnerabilidades.
- Definir el tiempo de reacción ante el impacto de una vulnerabilidad con los objetivos de negocio.
- Revisar el proceso de la gestión de las vulnerabilidades técnicas de manera regular.
- Las instalaciones sólo las debería llevar a cabo el administrador.
- Deberán ser aplicaciones aprobadas por la Dirección y en modo ejecutable. En ningún caso código interpretado por máquinas virtuales, macros, etc.
- Deberá existir un plan de respaldo en caso de que la instalación no ha sido satisfactoria. Para ello se puede mantener la versión anterior que será eliminada una vez verificado que la nueva funciona correctamente.
- Deberá haber un registro de todas las aplicaciones instaladas o eliminadas.

## 12.7 Consideraciones sobre auditorias de sistemas de información

Minimizar el impacto de las actividades de auditoría en los sistemas operacionales.

| | GDPR | Docs / Regs ISO27001 |
|---|---|---|
| 12.7.1 Información controles de auditoría de sistemas | No obligatorio | Sí |

**Notas y recomendaciones**

Las compañías deben ser auditadas para verificar el correcto funcionamiento de sus sistemas operacionales. Un programa de auditoría debería incluir un plan para la ejecución de auditorías tanto internas como externas.

Recomendaciones

- Definir un programa de auditoría aprobado por la dirección y que contemple los tipos de auditoria a realizar. Esta actividad debería hacerse una vez al año.
- El alcance de la auditoría debería ser acordado teniendo en cuenta la disponibilidad de las personas que se verán implicadas.

## 13.1 Gestión de seguridad de las redes

Asegurar la protección de la información en redes y en las instalaciones de procesado de la información de soporte.

| | GDPR | Docs / Regs ISO27001 |
|---|---|---|
| 13.1.1 Controles de redes | No obligatorio | No |
| 13.1.2 Seguridad de los servicios de red | No obligatorio | No |
| 13.1.3 Separación en las redes | No obligatorio | No |

**Notas y recomendaciones**

Las redes tienen que controlarse para impedir que haya acceso no autorizado a los datos que por ellas circulan. Si la organización dispone de varias áreas, convendría que se dividiera en distintos dominios de red. De igual forma se podrían separar según las operaciones de negocio.

Convendrá establecer acuerdos de servicio con los proveedores (SLA) y por tanto se precisará una monitorización de los SLA incluso proceder a auditorías si se considera oportuno.

Recomendaciones

- Definir procedimientos para la gestión de los equipos de red.
- Si el tamaño de la organización es elevado y dispone de varias áreas, dividir la red en distintos dominios.
- La conexión a los sistemas de red debe ser restringido al administrador del sistema.
- Establecer SLAs con el proveedor de servicios de red y monitorizar el servicio ofrecido.
- Incluir al proveedor del servicio en posibles auditorías de la organización.

## 13.2 Transferencia de información

Mantener la seguridad de información transferida dentro de la organización y con cualquier entidad externa.

| | GDPR | Docs / Regs ISO27001 |
|---|---|---|
| 13.2.1 Políticas y procedimientos de transferencia de información | Obligatorio | No |
| 13.2.2 Acuerdos sobre transferencia de información | Obligatorio | No |
| 13.2.3 Mensajería electrónica | Obligatorio | No |
| 13.2.4 Acuerdos de confidencialidad o de no divulgación | Obligatorio | Sí |

**Notas y recomendaciones**

Las organizaciones suelen distribuir información con otras entidades externas. Esta transferencia debe estar sujeta a controles de seguridad para impedir que la información sea distribuida más allá del ámbito del acuerdo entre ambas partes. Se requiere la definición de una serie de políticas que incluirán los acuerdos y procedimientos a seguir como por ejemplo confidencialidad y no divulgación.

Recomendaciones

- Definir procedimientos para proteger la copia, modificación, distribución y destrucción de los datos.
- Utilizar en todo momento criptografía para proteger todo tipo de información enviada sea sensible o no.
- Concienciar a los empleados en la necesidad de no revelar datos confidenciales.
- Utilizar acuerdos para la transferencia de la información que indiquen las responsabilidades de cada parte, los estándares a utilizar, las responsabilidades en caso de incidente de seguridad, niveles de servicio acordado, uso de criptografía para el envío de información.
- Los acuerdos de confidencialidad y no divulgación deberían constatar el tipo de información que se envía previa clasificación (Por ejemplo, pública, interna, secreta, etc), detallar el período del acuerdo de confidencialidad entre ambas partes, responsabilidades en caso de divulgación de datos no autorizados, propiedad de la información para evitar litigios por incumplimiento de la ley de protección intelectual.

## 14.1 Requisitos de seguridad de los sistemas de información

Asegurar que la seguridad de la información es una parte integral de los sistemas de información en todo el ciclo de vida. Esto además incluye los requisitos para los sistemas de información los cuales proporcionan servicios sobre redes públicas.

| | GDPR | Docs / Regs ISO27001 |
|---|---|---|
| 14.1.1 Análisis y especificación de requisitos de seguridad de la información | Obligatorio | Sí |
| 14.1.2 Seguridad de servicios de las aplicaciones en redes publicas | No obligatorio | No |
| 14.1.3 Protección de transacciones de los servicios de las aplicaciones | No obligatorio | No |

**Notas y recomendaciones**

Los requisitos de la seguridad de la información se deben aplicar para los nuevos sistemas que se desarrollen o para mejoras en los ya existentes. Se deben considerar múltiples aspectos recogidos en varios objetivos de control como la especificación de obligaciones y reponsabilidades, gestión segura de los procesos de negocio, control de acceso, etc sobre todo teniendo en cuenta la disponibilidad, confidencialidad e integridad.

Así mismo, se tiene que gestionar la seguridad en los servicios que hacen uso de redes públicas para evitar las actividades fraudulentas y la divulgación o modificación de información no autorizada. Este punto está muy relacionado con la protección de las transacciones que se realizan en las operaciones diarias como podría ser las compras o tramitaciones administrativas en línea.

Recomendaciones

- Establecer controles de acceso que comtemplen autenticación y autorización de usuarios.
- Notificar las obligaciones y responsabilidades de los usuarios.
- Revisar los requisitos de seguridad que se requieren aplicar para los nuevos desarrollos incluyendo la relación con otros controles de seguridad ya implantados. Posiblemente no se prestan la suficiente atención por no considerarse parte del alcance del proyecto.
- Establecer como requisito principal que los sistemas preserven la confidencialidad, integridad y disponibilidad de los servicios en aquellos que impliquen transferencias de información en redes públicas.
- En caso de pagos a través de internet proporicional pasarelas seguras para evitar fraudes.
- Aplicar siempre encriptación en la transmisión de la información y en los protocolos utilizados para ello.
- Utilizar la firma electrónica siempre para ciertas operaciones como por ejemplo las transacciones financieras y administrativas.
- Almacenar la información de las transacciones en entornos propios a la organización y no en entornos externos a los que se puede tener acceso a través de internet.

## 14.2 Seguridad en los procesos de desarrollo y soporte

Asegurar que la seguridad de la información está diseñada e implementada dentro del ciclo de vida de desarrollo de los sistemas de información

| | GDPR | Docs / Regs ISO27001 |
|---|---|---|
| 14.2.1 Política de desarrollo seguro | No obligatorio | No |
| 14.2.2 Procedimientos de control de cambios en sistemas | No obligatorio | No |
| 14.2.3 Revisión técnica de las aplicaciones después de cambios en la plataforma de operación | No obligatorio | No |
| 14.2.4 Restricciones en los cambios a los paquetes de software | No obligatorio | No |
| 14.2.5 Principios de construcción de sistemas seguros | No obligatorio | Sí |
| 14.2.6 Entorno de desarrollo seguro | No obligatorio | No |
| 14.2.7 Desarrollo contratado externamente | No obligatorio | No |
| 14.2.8 Pruebas de seguridad de sistemas | No obligatorio | No |
| 14.2.9 Prueba de aceptación de sistemas | No obligatorio | No |

**Notas y recomendaciones**

Este objetivo de control está muy relacionado con el anterior. En caso de desarrollar sistemas informáticos, la seguridad de la información siempre debe estar presente. Se tiene que definir una política que gestione el entorno de desarrollo, los requisitos para las distintas fases del ciclo de vida, en la gestión del control de cambios y versiones, capacidad de los empleados en ser capaces de identificar, evitar y resolver vulnerabilidades.

Se tendrían que documentar todos aquellos procesos enfocados a aplicar la seguridad de la información en todo el ciclo de vida y en todos los entornos afectados, incluyendo las actividades de desarrollo subcontratadas en el exterior.

Recomendaciones

- Gestionar todos los entornos como desarrollo, testing, preproduction, etc. para la aplicación de una política de seguridad en todas las aplicaciones. Por ejemplo definiendo distintos entornos de desarrollo o test según las aplicaciones, aplicando controles de acceso a dichos entornos, monitorización de todos los cambios, etc.
- Revisar la seguridad utilizada para el control de los repositorios y en la gestión de control de cambios y versiones. La CMDB debe estar siempre actualizada y gestionada por el administrador incluyendo versiones de todos los paquetes de softwarey otros activos, propietarios de los activos.
- En caso de cambios en las plataformas operativas, asegurar que no se ve impactado ningún proceso de negocio que afecte a su operativa y su seguridad. Los cambios deben realizarse con suficiente antelación para que se definan pruebas previas y planes de contingencia en caso de problemas.
- Evitar en la medida de lo posible los cambios en los paquetes. Si en cualquier caso se aconseja realizar, identificar si algún proceso operativo puede verse afectado y actuar en consecuencia.
- Documentar siempre todos los procesos enfocados a la aplicación de la seguridad en todo su ciclo de vida así como en todos los entornos afectados, desde desarrollo hasta test.
- En caso de subcontratar servicios de desarrollo externos, definir requisitos de seguridad específicos para este tipo de servicio, identificar códigos de conducta, acuerdos de confidencialidad y de propiedad intelectual, necesidad de realizar auditorias de seguridad sobre el servicio prestado, obtener la documentación creada para todo el ciclo de vida del proyecto desde desarrollo a test.

## 14.3 Datos de prueba

Asegurar la protección de los datos utilizados para las pruebas.

| | GDPR | Docs / Regs ISO27001 |
|---|---|---|
| 14.3.1 Protección de datos de prueba | Obligatorio | No |

**Notas y recomendaciones**

Todos los datos realizados en las pruebas deben ser protegidos para evitar divulgación de la información. No se deben utilizar datos sensibles que puedan identificar a la persona.

Recomendaciones

- Evitar utilizar datos que permitan identificar a la persona de cualquier forma.
- Si los datos de prueba son utilizados por personas no responsables de los mismos, solicitar siempre autorización de su uso.
- En lugar de ofrecer datos reales, intentar proporcionar datos simulados para evitar divulgación de la información. En caso de no ser posible, ofrecer algunas muestras representativas y más aún en caso de que la información real contenga una cantidad ingente de datos.
- Aplicar control de acceso a estos datos y a otros sistemas que los utilizan de la misma forma que a otros sistemas operacionales.
- Eliminar los datos de test una vez utilizados.
- Monitorizar la información que se utiliza para las puebas de test. Podrá ser utilizada para posteriores auditorias de seguridad.

## 15.1 Seguridad de la información en las relaciones con los proveedores

Asegurar la protección de los activos de la organización que son accesibles por los proveedores.

| | GDPR | Docs / Regs ISO27001 |
|---|---|---|
| 15.1.1 Política de seguridad de la información para las relaciones con proveedores | Obligatorio | Sí |
| 15.1.2 Tratamiento de la seguridad dentro de los acuerdos con proveedores | Obligatorio | No |
| 15.1.3 Cadena de suministro de tecnología de información y comunicación | No obligatorio | No |

**Notas y recomendaciones**

Las organizaciones que tienen relaciones con proveedores necesitan definir una política de cubra los aspectos relativos con la seguridad a través de acuerdos que recogerán entre otros, los tipo de servicios, la monitorización que se va a realizar, como gestionar las incidencias, la documentación que se necesitará producir, etc.

Recomendaciones

- Identificar el tipo de servicios como por ejemplo TIC, logísticos, servicios de infraestructura, servicios financieros.
- Identificar el tipo de información a la que tendrá acceso el proveedor. Evitar datos sensibles que identiquen a la persona.
- Especificar la monitorización que se realizará de las actividades con el proveedor y las auditorias que se realizarán sobre sus servicios.
- Especificar la forma de gestionar las incidencias y la resolución de defectos.
- Definir la documentación por los servicios prestados y los criterios de su aceptación.
- Identificar los requisitos legales en los que ambas partes están sujetos.
- Clasificar la información según la política de seguridad.
- Presentar a los empleados la forma de relacionarse con el proveedor e identificar el tipo de información que se puede compartir.
- Definir los requisitos para la gestión de las incidencias.

## 15.2 Gestión de la prestación de servicios con los proveedores

Mantener un nivel acordado de seguridad de la información y entrega de servicios de acuerdo con los acuerdos con los proveedores

| | GDPR | Docs / Regs ISO27001 |
|---|---|---|
| 15.2.1 Seguimiento y revisión de los servicios de los proveedores | No obligatorio | Sí |
| 15.2.2 Gestión de cambios en los servicios de proveedores | No obligatorio | No |

**Notas y recomendaciones**

Las organizaciones deben realizar un seguimiento de la gestión de los servicios que realizan los proveedores de forma regular y a las que se recomienda auditar cada cierto período de tiempo.

Se suelen llevar acuerdos de nivel de servicio donde se monitoriza el nivel de servicio y se da constancia del cumplimiento de los acuerdos firmados por ambas partes.

Recomendaciones

- Realizar reuniones de seguimiento de forma regular para monitorizar y el cumplimiento de los niveles de acuerdo con el proveedor. Así mismo para gestionar los desacuerdos y problemas entre ambas partes
- Realizar auditorías de seguridad de forma regular.
- En caso de que el proveedor contrate otros proveedores, asegurarse que no se divulga información sin previo acuerdo por ambas partes.
- Gestionar los posibles cambios de acuerdo que se puedan producir en un futuro. Por ejemplo uso de nuevas tecnologías, cambios de localizaciones físicas, adquisición de nuevos activos, etc.

## 16.1 Gestión de incidentes y mejoras de seguridad de la información

Asegurar un enfoque consistente y efectivo para la gestión de los incidentes de seguridad de la información, incluyendo la comunicación sobre eventos y debilidades de seguridad.

| | GDPR | Docs / Regs ISO27001 |
|---|---|---|
| 16.1.1 Responsabilidad y procedimientos | Obligatorio | No |
| 16.1.2 Reporte de eventos de seguridad de la información | No obligatorio | Sí |
| 16.1.3 Reporte de debilidades de seguridad de la información | No obligatorio | Sí |
| 16.1.4 Evaluación de eventos de seguridad de la información y decisiones sobre ellos | No obligatorio | Sí |
| 16.1.5 Respuesta a incidentes de seguridad de la información | No obligatorio | Sí |
| 16.1.6 Aprendizaje obtenido de los incidentes de seguridad de la información | No obligatorio | No |
| 16.1.7 Recolección de evidencia | No obligatorio | No |

**Notas y recomendaciones**

Las responsabilidades y procedimientos se deben definir para una respuesta rápida a los incidentes de seguridad. En caso de que se produzca alguno, deben ser notificados lo más rápido posible utilizando los canales de comunicación establecidos (por ejemplo autoridades de supervisión y las encargadas para el cumplimiento de las leyes o a ciertos grupos de interés como CERTs). Los empleados o contratistas deberían ser partícipes de la comunicación notificando en caso de sospecha de incidente de seguridad.

Los eventos que se produzcan deberán ser clasificados y recogidos y, en función de su consideración, se podrán definir como incidentes. Se requerirá aplicar las acciones establecidas en la política de seguridad de la organización. Esta información servirá como lección aprendida para posibles futuros eventos.

Recomendaciones

- Definir las responsabilidades y sus procedimientos para la gestión de los incidentes de seguridad. Algunos procedimientos serían monitorización, análisis forense, reporte, evaluación de los eventos, etc. Los procedimientos los llevarán a cabo personas relacionadas con la seguridad de la información.
- Los empleados y contratistas deben notificar cualquier evento que sospechen que se trata de un incidente. Posteriormente esos eventos deberán ser clasificados para determinar si son incidentes de seguridad o no.
- Se recogerá la información y se procederá a un análisis forense para determinar las causas y su tratamiento. Deberá ser almacenada para poder tener un registro y así mismo podrá ser utilizada como lección aprendida.

## 17.1 Continuidad de seguridad de la información

La continuidad de la seguridad de la información debe integrarse en los sistemas de la gestión de la continuidad del negocio de la organización.

| | GDPR | Docs / Regs ISO27001 |
|---|---|---|
| 17.1.1 Planificación de la continuidad de la seguridad de la información | No obligatorio | No |
| 17.1.2 Implementación de la continuidad de la seguridad de la información | Obligatorio | Sí |
| 17.1.3 Verificación, revisión y evaluación de la continuidad de la seguridad de la información | No obligatorio | No |

**Notas y recomendaciones**

La continuidad de la seguridad de la información debe formar parte de la continuidad del negocio de la organización. Para ello es precisa una planificación documentada, una definición de una estructura organizativa con la responsabilidad y competencia para la gestión de los incidentes y una revisión regular de la continuidad en la seguridad de la información para asegurar que la organización está preparada para eventos adversos.

Recomendaciones

- Cuando se planifique la continuidad del negocio se debe considerar al mismo tiempo los requisitos de continuidad para la seguridad de la información. Se debe planificar como proceder en caso de que se produzca un incidente.
- La estructura organizativa tiene que estar preparada de antemano. Los responsables de forma parte de las acciones de contingencia debe ser lo suficientemente compententes para llevarlo a cabo y tener soporte en todo momento de la dirección para la toma de decisiones que se basarán en la planificación previa.
- Se deberán realizar simulacros para verificar la continuidad de los sistemas de información comprobando los procedimientos y controles puestos en funcionamiento. Estos simulacros están enfocados en los posibles eventos adversos que pueden afectar a los objetivos de negocio y no a cambios por ejemplo en el uso de nuevas aplicaciones o infraestructuras con nuevos requisitos de seguridad.

## 17.2 Redundancias

Asegurar la disponibilidad de las instalaciones de procesado de la información.

| | GDPR | Docs / Regs ISO27001 |
|---|---|---|
| 17.2.1 Disponibilidad de instalaciones de procesamiento de información | No obligatorio | No |

**Notas y recomendaciones**

Este objetivo de control es una extensión del anterior. La organización debe asegurar que existe disponibilidad en las instalaciones de procesado de la información.

Recomendaciones

- Aplicar sistemas redundantes de forma que, en caso de no disponibilidad de uno de ellos, el resto pueda asumir la continuidad del servicio.
- Realizar copias de seguridad de la información accesible por los sistemas.
- Realizar simulacros para verificar la disponibilidad de los sistemas ante una posible caída del servicio principal.

## 18.1 Cumplimiento con los requisitos legales y contractuales

Evitar incumplimientos de obligaciones legales, estatutarias, reglamentarias o contractuales relacionadas con la seguridad de la información y con cualquier requisito de seguridad.

| | GDPR | Docs / Regs ISO27001 |
|---|---|---|
| 18.1.1 Identificación de la legislación aplicable y de los requisitos contractuales | Obligatorio | Sí |
| 18.1.2 Derechos de propiedad intelectual | Obligatorio | No |
| 18.1.3 Protección de registros | Obligatorio | No |
| 18.1.4 Privacidad y protección de datos personales | Obligatorio | No |
| 18.1.5 Reglamentación de controles criptográficos | Obligatorio | No |

**Notas y recomendaciones**

Las organizaciones están sujetas a distintas obligaciones legales, estatutarias, reglamentarias o contractuales. De forma particular con la GDPR y la LOPDP. Es decir, deben cumplir con los requisitos para el cumplimiento de la seguridad de la información identificándolos y documentándolos.

Los derechos de propiedad intelectual deben ser protegidos y necesitan cumplir las regulaciones vigentes. Se require definir una política de gestión que detalle el uso legal de los activos de información, como generar concienciación para su uso, como registrar la evidencia de propiedad mediante licencias o documentación oficial de los productos, mantenimiento de las licencias ya adquiridas, traspaso de productos a otras partes,etc.

La información personal identificable debe ser en todo momento protegida y considerada como privada. En caso de utilización de encriptación, se requiere que cumpla con las normativas vigentes.

Recomendaciones

- Considerar las normativas vigentes a las que está sujeta la organización. En el caso español, la LOPDP y la GDPR a partir de mayo de 2018. La máxima prioridad por tanto, es implementar aquellos controles que ayuden a la gestión de la seguridad de la información.
- Establecer una política de gestión de los derechos de propiedad intelectual. Deberá ser transmitida a toda la organización.
- Utilizar software adquirido en fuentes reconocidas para evitar que los derechos de propiedad no han sido violados. La licencia de compra debe ser registrada como prueba de evidencia. Se deben seguir los términos y condiciones aceptados a la hora de adquirir el software.
- La información personal identificable debe ser en todo momento protegida y considerada como privada.
- La encriptación utilizada siempre deberá cumplir con las normativas vigentes.

## 18.2 Revisiones de seguridad de la información

Asegurar que la seguridad de la información se implementa y opera de acuerdo con las políticas y procedimientos de la organización.

| | GDPR | Docs / Regs ISO27001 |
|---|---|---|
| 18.2.1 Revisión independiente de la seguridad de la información | No obligatorio | Sí |
| 18.2.2 Cumplimiento con las políticas y normas de seguridad | No obligatorio | Sí |
| 18.2.3 Revisión del cumplimiento técnico | No obligatorio | Sí |

**Notas y recomendaciones**

La política de seguridad debe ser revisada para confirmar que se utiliza. Se precisa que se realice de manera independiente para evitar que se vea condicionada por las personas que la han definido. A ser posible de distintas áreas operativas o a través auditorias externas. Debe cumplir con las políticas y estándares de seguridad.

El cumplimiento técnico debe revisarse en función de la política de seguridad de la organización.

Recomendaciones

- Revisar la política de seguridad por personas que no han sido involucradas en su desarrollo pero que, no obstante, conozcan los objetivos de negocio.
- La información obtenida debe ser documentada y mantenida.
- Los responsables deben encargarse del cumplimiento de las políticas de aquellas áreas que son de su responsabilidad. En caso de encontrar incumplimientos, deberán identificar las razones y las acciones para su cumplimiento.
- Aquellas revisiones de cumplimiento técnico conviene hacerlas con herramientas automatizadas. En caso contrario, una persona con las competencias.
- Las revisiones deberán ser planificadas con antelación y de forma periódica.

# 8. Aplicación de la guía (supuesto ficticio)

*¿Puedo disponer de un ejemplo aplicado de la guía propuesta?*

La aplicación de la guía se basará en el supuesto ficticio de una pequeña empresa de menos de 30 empleados dedicada a la venta de productos de montaña a través de internet. A pesar de tener mucha competencia, se está abriendo camino gracias a los contactos y experiencia que tiene el fundador, un apasionado de la alta montaña, después de estar involucrado en este sector deportivo tan especializado desde hace muchos años.

La empresa se llama *Ibones de Aragón S.L.*. Se fundó en febrero de 2015 con un presupuesto muy reducido que contaba con una pequeña oficina donde había varios equipos informáticos para el desarrollo de una página web, y un almacén alquilado cercano a la oficina. Posteriormente, la compañía se ha ido desarrollando y ha crecido hasta el punto que se ha tenido que desplazar a una zona industrial cercana. El almacén adquirido está en un local anexo.

Actualmente su mercado es íntegramente nacional. No obstante se prevé una apertura internacional del negocio, principalmente en Europa y Sudamérica. Implicará delegaciones en varios países y por tanto contratación de nuevos empleados para dar soporte.

Su misión, visión y valores definen su identidad corporativa:

- Misión – objetivo de *Ibones de Aragón S.L.*
  - Ofrecer productos especializados en alta montaña
  - Proporcionar los mejores precios en equipación
  - Promover el turismo sostenible en montaña
- Visión – sus aspiraciones a largo plazo
  - Ser líderes en venta online de productos de montaña
  - Ser referentes en deportes de montaña
- Valores – sus acciones y comportamiento
  - Integridad y transparencia con el cliente
  - Responsabilidad con el cliente
  - Pasión por la montaña

Las siguientes secciones muestran la organización actual de la compañía. Es decir, apenas ha aplicado controles de seguridad y por tanto convendrá utilizar la guía propuesta para, cuando menos, cumplir con la GDPR y a ser posible, tener una base para la implantación de un SGSI en un futuro próximo. La dirección está comprometida completamente con este fin.

Así pues, teniendo en cuenta que esta guía de controles de fácil implantación no debe ser muy técnica, se presenta la situación actual y lo que convendría realizar siguiendo los controles ISO/IEC 27002:2013. Nótese que está fuera del alcance de este TFM la identificación de los riesgos aunque se presenta la Declararación de Aplicabilidad brevemente explicado en el capítulo anterior. De esta forma, el lector tendrá una visión no técnica y muy sencilla de lo que una guía de estas características debería ofrecer. Es más, no se entra en detalle en la información técnica para poner todo el énfasis en la aplicación de esta guía de fácil implementación.

## 8.1. Organigrama de la empresa

A pesar de tratarse de una empresa pequeña, *Ibones de Aragón S.L.* se compone de cuatro áreas bien diferenciadas:

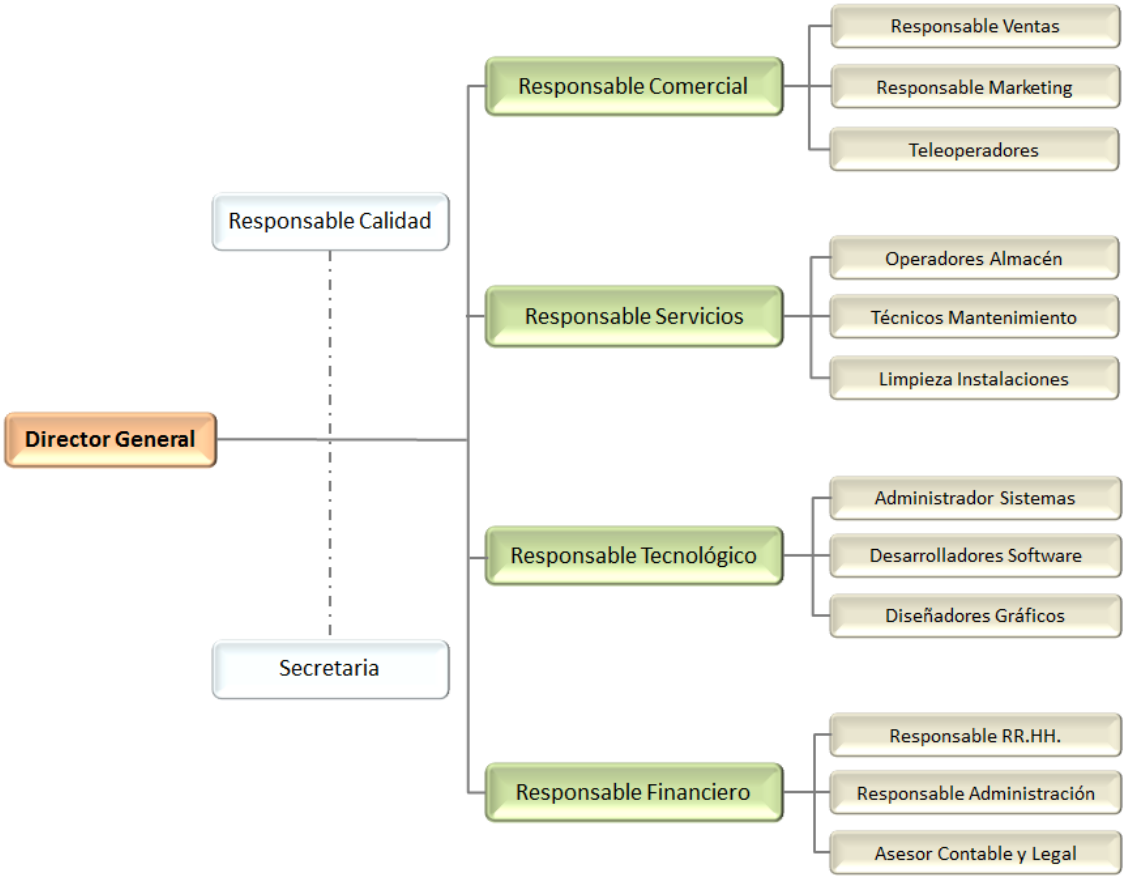



*Imagen 10 – Organigrama de Ibones de Aragón S.L.*

El equipo humano es el siguiente[3]:

- Director general (1) – Fundador de *Ibones de Aragón S.L.*. Responsable máximo de la compañía.
- Responsable de calidad (1) – Encargado de las normativas de calidad de la organización. Principal impulsor de la aplicación de la ISO27000 como referencia para la seguridad de la información. Colabora de manera transversal con los distintas áreas.
- Secretaria (1) – Realiza funciones de secretaría, recepción y da soporte a la gerencia y a los responsables.

[3] *Se muestran entre paréntesis el número de personas.*

- Responsable comercial (1) – Realiza las funciones comerciales de la compañía. Se encarga del cumplimiento de los objetivos de venta, establece las directrices de marketing y coordina el trabajo de los teleoperadores.
- Responsable de servicios (1) – Se encarga de la coordinación de las actividades de los operadores que trabajan en el almacén donde se tiene el material de montaña para distribuir, de las personas que trabajan en el mantenimiento de las instalaciones (p.ej. electricidad, agua, etc.) así como las personas encargadas de la limpieza.
- Responsable tecnológico (1) – Se encarga de la coordinación de las actividades TIC de la compañía. Como responsable está a cargo del administrador del sistema, de los desarrolladores del software y de los diseñadores gráficos. Esta persona desempeña labores de Jefe de Proyecto para, entre otras cosas, los nuevos desarrollos informáticos. Se encarga de la gestión de los datos TIC.
- Responsable financiero (1) – Se encarga de la coordinación de las tareas relacionadas con Recursos Humanos, formación y concienciación a los empleados, la administración de la compañía y de la asesoría contable y legal.
- Responsable de ventas (1) – Se encarga de las ventas de la compañía. Establece contactos con proveedores de material.
- Responsable de marketing (1) – Se encarga del marketing: realiza estudios de mercado, propone modificaciones en la página Web de la compañía al ser el punto principal de contacto de los clientes, realiza campañas en medios de comunicación como radios y TV locales, etc.
- Teleoperadores (2) – Son el punto de contacto de la compañía. Reciben llamadas de clientes tanto para consultas como reclamaciones o quejas.
- Operadores de almacén (3) – Se encargan de la manipulación del material a la venta disponible en el almacén. No tienen acceso a los servicios informáticos de la compañía.
- Técnicos de mantenimiento (2) – Se encargan del mantenimiento de las instalaciones como sería el correcto funcionamiento eléctrico o suministro de agua (p.ej. cambio de fluorescentes, arreglo de sanitarios, etc.).
- Limpieza de instalaciones (2) - Se encargan de la limpieza de las instalaciones. Lo realizan de lunes a viernes fuera de horario de atención al público (20:00 a 21:00).
- Administración de sistemas (1) – Se encarga de la administración TIC de *Ibones de Aragón S.L.* Es el responsable de los sistemas y la persona encargada de la instalación de nuevos productos software, gestión de cuentas de usuario en caso de nuevo empleado, asignación de roles, etc.
- Desarrolladores de software (3) – Son los encargados de la actualización de la página web de la compañía, desarrollo de nuevas funcionalidades software, etc.
- Diseñadores gráficos (2) – Se encargan de adaptar la página web de la compañía introduciendo nuevos elementos gráfico que la hagan más atractiva para el cliente. Trabajan en estrecha colaboración con los desarrolladores de software puesto que serán ellos los que adapten la página.
- Responsable de recursos humanos (1) – Se encarga de los recursos humanos de la compañía incluyendo la formación y concienciación.
- Responsable de administración (1) – Se encarga de la administración de los datos contables de la compañía pero no de los datos TIC ya que de ellos se encarga el Responsable Tecnológico.
- Asesor contable y legal (1) – Realiza funciones de soporte contable y legal para todas las actividades de la organización. Uno de los impulsores del cumplimiento de la GDPR.

## 8.2. Instalaciones

Las nuevas instalaciones de *Ibones de Aragón S.L.* se encuentran en 2 edificios anexos. El primero tiene 2 plantas donde se encuentra la oficina y el segundo es el almacen. No están unidos físicamente.

Ambos edificios disponen de detectores de presencia, alarma conectada a servicios de seguridad y CCTV (Circuito Cerrado de Televisión para Vigilancia). El registro del vídeo se almacena durante 72 horas cubriendo fines de semana.

Se adjuntan los planos aproximados de la estructura de ambos edificios:

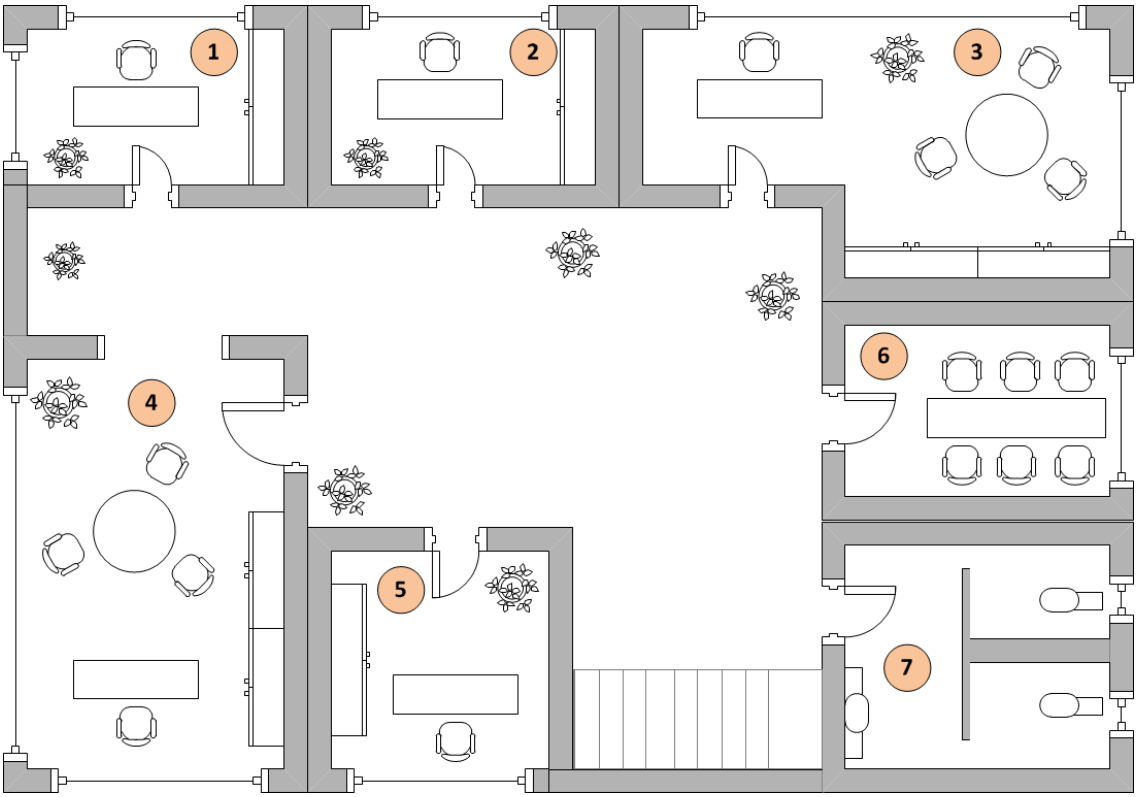



*Imagen 11 – Planta superior del edificio de oficinas*

***Leyenda***

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 1 | Responsable comercial | 2 | Responsable servicios | 3 | Responsable financiero<br>Responsable RR.HH.<br>Responsable administración<br>Asesor contable y legal | 4 | Director general |
| 5 | Responsable calidad | 6 | Sala de reuniones | 7 | Aseos | | |

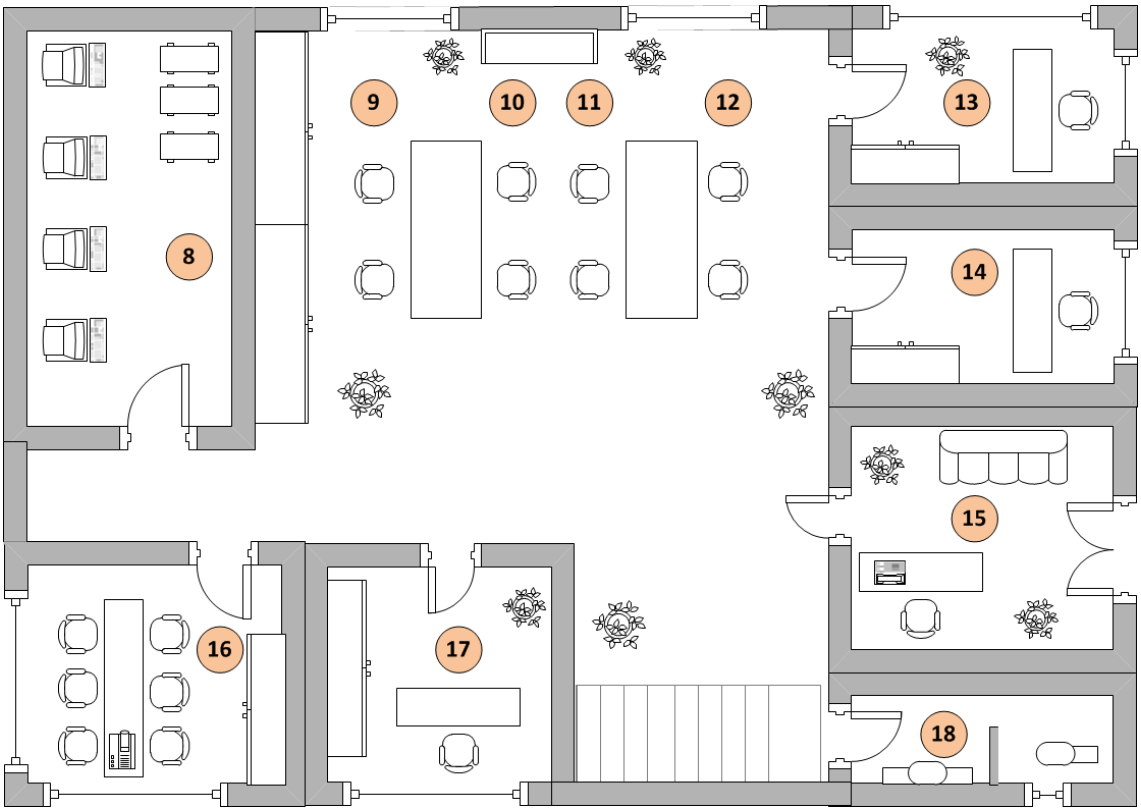



*Imagen 12 – Planta inferior del edificio de oficinas*

***Leyenda***

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 8 | Sala de servidores | 9 | Diseñadores gráficos | 10 | Desarrolladores software | 11 | Administrador Desarrollador software |
| 12 | Teleoperadores | 13 | Responsable ventas | 14 | Responsable marketing | 15 | Secretaria (entrada principal) |
| 16 | Sala de reuniones | 17 | Responsable tecnológico | 18 | Aseos | | |

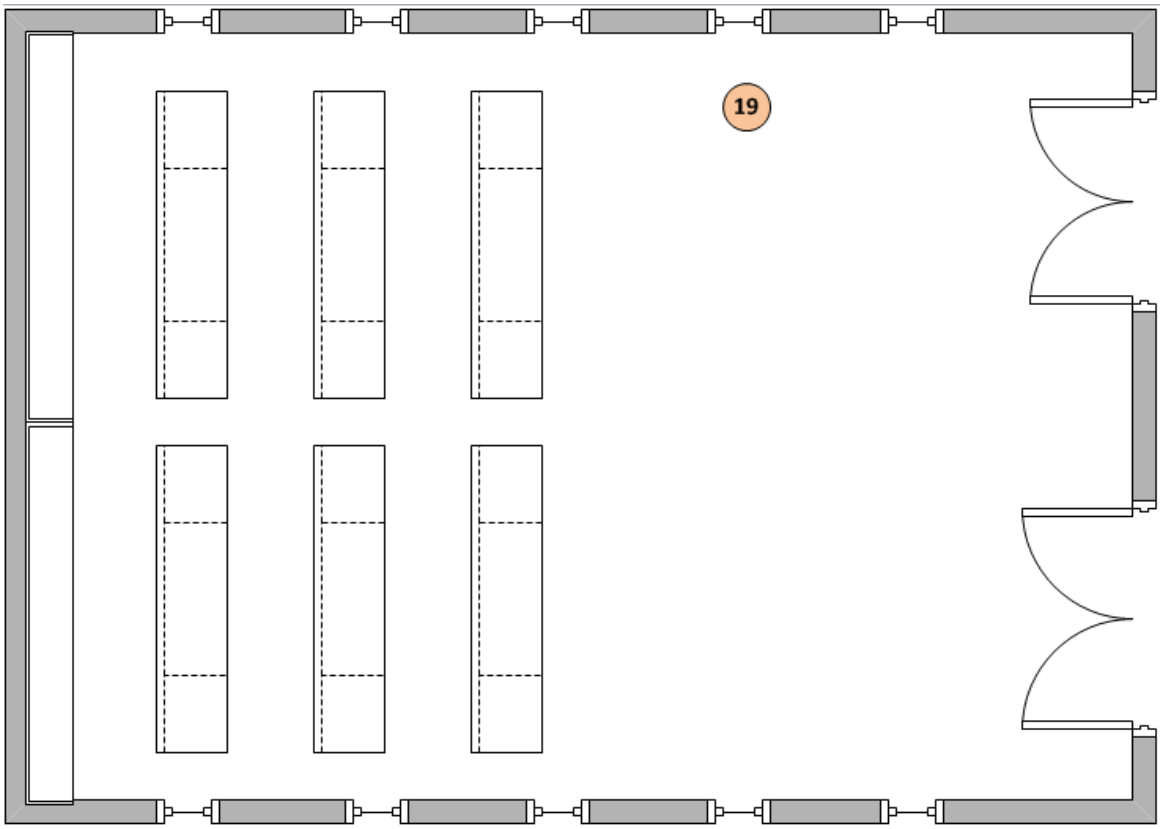



*Imagen 13 – Almacén situado en el edificio anexo*

***Leyenda***

19 Almacen

## 8.3. Equipamiento informático (hardware / software)

*Ibones de Aragón S.L.* cuenta con los siguientes medios:

- Hardware
  - 23 PCs de sobremesa
  - 8 Portátiles
  - 1 Servidor de correo
  - 2 Servidores Web / Aplicaciones
  - 2 Impresoras / Fotocopiadoras / Escáner
  - 2 PCs entorno de pruebas
  - 1 Servidor de desarrollo y backup
  - 2 Servidores de base de datos (desarrollo y producción)
  - 2 Firewalls

- Red
  - 1 Router
  - 2 Puntos de acceso WiFi
- Software
  - 1 proxy
  - 40 Licencias sistemas operativos
  - 40 Licencias antivirus
  - 40 Licencias varias aplicaciones ofimáticas (**nota**: no se considera relevante indicar su nombre)

## 8.4. Aplicación de los controles para *Ibones de Aragón S.L.*

La aplicación de los controles siguiendo la guía propuesta en el capítulo anterior seguirá un esquema básico para cada objetivo de control según la ISO/IEC 27002:2013:

1) Estado de la empresa antes de implementar los controles de cada objetivo (AS-IS).
2) Estado futuro una vez se implementen algunos o todos los controles del objetivo (TO-BE)[4].
3) Sección del DdA referido al Objetivo de Control una vez implementados algunos o todos sus controles.

| **5.1 Dirección de gestión para la seguridad de la información** |
|---|
| Proporciona dirección de gestión y soporte para la seguridad de la información de acuerdo con los requisitos de negocio, leyes y regulaciones relevantes. |
| **Estado Actual (AS-IS)** |
| • La compañía no dispone de una política de seguridad. Se limita únicamente a dar instrucciones a los empleados *ad-hoc* según se van conociendo incidentes de seguridad que aparecen en los medios de comunicación.<br>• No se tienen en cuenta las implicaciones legales vigentes. En particular la GDPR. |
| **Estado Futuro (TO-BE)** |
| • La compañía ha definido una política de seguridad de la información que será de obligado cumplimiento para todos los empleados y aquellas terceras partes que tendrán acceso a la información sensible que trate la compañía.<br>• La política de seguridad de información, aunque en una versión preliminar, contiene aquellos puntos más relevantes que la Dirección ha considerado deben tenerse en cuenta. Los responsables de área han participado en su definición. Se han evitado referencias a otras políticas de seguridad para poder definir una propia.<br>• Se realiza una revisión de la misma a finales de cada año. Lo cual puede significar en modificación de algunas cláusulas o la adición de nuevas.<br>• Como punto de partida se ha tenido en consideración el cumplimiento de la GDPR puesto que entrará en vigor en los próximos meses. La compañía puede estar sujeta a duras sanciones si no se cumple. |

[4] *En algunos controles se presentan ejemplos como anexos a este documento*

| Documento de Aplicabilidad (sección) | | | | | |
|---|---|---|---|---|---|
| **Control** | **Selec.** | **Justificación selección** | **Impl.** | **Justificación exclusión** | **Referencia** |
| 5.1.1 | ✔ | Es fundamental recoger en un documento la política de seguridad de obligatorio cumplimiento por todos los empleados | ✔ | | • REF-05-01.1 Política de seguridad |
| 5.1.2 | ✔ | La política de seguridad debe ser revisada de forma periódica | ✔ | | • REF-05-01.1 Política de seguridad |

## 6.1 Organización interna

Establecer un marco de trabajo de gestión para iniciar y controlar la implementación y la operación de la seguridad de la información dentro de la organización.

**Estado Actual (AS-IS)**

- La organización tiene establecidas algunas responsabilidades y roles. El responsable del tratamiento de los datos es el Responsable Tecnológico. No obstante, los procesos no han sido claramente identificados y por lo tanto no existe responsable para todos y cada uno de ellos. De forma implícita es el Responsable Tecnológico.
- No existe una separación de deberes de forma que una misma persona puede iniciar, procesar, finalizar y eliminar las acciones sin que nadie las valide.
- No se dispone de una lista de contactos con las autoridades.

**Estado Futuro (TO-BE)**

- Los procesos han sido clasificados y se ha asignado un responsable y rol para cada uno de ellos.
- La estructura organizativa permite la separación de deberes de forma que los responsables de área son validadores de funciones de los subordinados para evitar la modificación no autorizada o no intencionada de los activos de la organización. Estos a su vez son validados por el Director General.
- Existe una lista de contactos con las autoridades para el cumplimiento de las leyes y regulaciones así como autoridades de supervisión. En caso de incidente serían notificados de manera oportuna.
- Teniendo en consideración los desarrollos software realizados en la compañía (p.ej. adaptaciones en la página web), instalación de sistemas, etc. la compañía tiene en cuenta la gestión de proyectos en el ámbito de la seguridad de la información para evitar o mitigar riesgos.

| Documento de Aplicabilidad (sección) | | | | | |
|---|---|---|---|---|---|
| **Control** | **Selec.** | **Justificación selección** | **Impl.** | **Justificación exclusión** | **Referencia** |
| 6.1.1 | ✔ | Cada responsable de los procesos debe verificar que se cumplen sus actividades y obligaciones a realizar. | ✔ | | • REF-06-01.1 – Roles y responsabilidades |
| 6.1.2 | ✔ | La estructura organizativa permite la separación de deberes. | ✔ | | N/A |
| 6.1.3 | ✔ | Es preciso establecer contacto con las autoridades en caso de algún incidente informático | ✔ | | • REF-06-01.3 – Lista de contactos |
| 6.1.4 | ✘ | | | Aunque el contacto con grupos | N/A |

## 6.1 Organización interna

Establecer un marco de trabajo de gestión para iniciar y controlar la implementación y la operación de la seguridad de la información dentro de la organización.

| | | | | | |
|---|---|---|---|---|---|
| | | | | de interés es importante, la compañía no se considera lo suficientemente madura.<br>En un futuro se prevé participar en algún fórum de seguridad al menos por parte del responsable tecnológico y el administrador. | |
| 6.1.5 | ✔ | La compañía realiza desarrollos software. Por tanto, conviene aplicar la seguridad en el código fuente para evitar posibles amenazas | ✔ | | N/A |

## 6.2 Dispositivos móviles y teletrabajo

Asegurar la seguridad del teletrabajo y el uso de los aparatos móviles.

**Estado Actual (AS-IS)**

- La compañía tiene un listado de los equipos disponibles (p.ej. 23 PCs de sobremesa, 8 portátiles, etc) pero se desconoce cuales tienen acceso a ciertas aplicaciones corporativas.
- Algunos portátiles son utilizados a título personal sin control alguno.
- No suelen actualizarse a no ser por recomendación de compañeros de trabajo en lugar de forma automática.

**Estado Futuro (TO-BE)**

- La compañía ha realizado el inventariado de los equipos y conoce las aplicaciones a las que pueden acceder.
- La política de seguridad define los procedimientos a seguir en cuanto al uso de los equipos.

**Documento de Aplicabilidad** (sección)

| Control | Selec. | Justificación selección | Impl. | Justificación exclusión | Referencia |
|---|---|---|---|---|---|
| 6.2.1 | ✔ | La compañía dispone de varios equipos portátiles. Los empleados deben seguir los preceptos recogidos en la política de seguridad de la compañía. | ✔ | | • REF-05-01.1 Política de seguridad |
| 6.2.2 | ✘ | | | Aunque algunas personas disponen de portátiles, no se permite actualmente realizar teletrabajo aunque se está considerando en caso de que la empresa se extienda a distintas localizaciones en Europa y Sudamérica. | N/A |

## 7.1 Previo al empleo

Asegurar que los empleados y los contratistas comprenden sus responsabilidades y que sean adecuadas para los roles para los que son considerados.

**Estado Actual (AS-IS)**

- La compañía no realiza un estudio previo del candidato. Se limita a recibir el CV y según la respuesta de la entrevista es contratado o rechazado.
- No se exige la firma de un acuerdo de confidencialidad a la hora de firmar el contrato. Por ello, se ha dado un caso de divulgación de información cuando un empleado descontento ha dejado la empresa.

**Estado Futuro (TO-BE)**

- La compañía solicita en referencias del candidato. En la medida de lo posible se pide que se ofrezcan una vez se ha realizado la primera entrevista de trabajo.
- Se revisa la información disponible en LinkedIn y la participación del candidato en foros profesionales.
- Se solicita un registro de antecedentes penales al candidato.
- Se solicita una copia de los títulos profesionales o educativos y de los certificados que disponga en caso de ser relevantes para el puesto al que opta.
- La compañía exige la firma de un acuerdo de confidencialidad y no divulgación de información cuando se firma el contrato.

**Documento de Aplicabilidad** (sección)

| Control | Selec. | Justificación selección | Impl. | Justificación exclusión | Referencia |
|---|---|---|---|---|---|
| 7.1.1 | ✔ | Se deben estudiar los antecedentes de los candidatos para considerar que son exactamente lo que la organización requiere. | ✔ | | N/A |
| 7.1.2 | ✔ | El candidato debe asumir la política de seguridad de la compañía y firmar un acuerdo de confidencialidad y no divulgación de la información. | ✔ | | • REF-07-01.2 – Acuerdo de confidencialidad |

## 7.2 Durante el empleo

Asegurar que los empleados y contratistas conozcen y cumplen con sus responsabilidades de seguridad de la información.

**Estado Actual (AS-IS)**

- No existe política de seguridad, por tanto los empleados realizan sus tareas sin prestar mucha atención a la seguridad de la información. Se basan más en opiniones que en instrucciones dadas por la organización.
- Los roles y responsabilidades no están definidos y por lo tanto los empleados pueden estar involucrados en procesos que no les corresponde.
- No existe un plan de formación y concienciación con la seguridad de la información. La dirección se remite a cursos online gratuitos sin verificar si son adecuados para la organización.

**Estado Futuro (TO-BE)**

- La compañía ha definido una política de seguridad de la información.
- Se dispone de los roles y responsabilidades de los empleados.
- Se ha definido un calendario de cursos de formación y concienciación para cada empleado. Se deberán realizar una vez al año.

**Documento de Aplicabilidad** (sección)

| Control | Selec. | Justificación selección | Impl. | Justificación exclusión | Referencia |
|---|---|---|---|---|---|
| 7.2.1 | ✔ | La dirección debe ser el pilar fundamental para la aplicación de las medidas de seguridad. Tiene que dar soporte en este ámbito. | ✔ | | • REF-05-01.1 Política de seguridad<br>• REF-06-01.1 – Roles y responsabilidades |
| 7.2.2 | ✔ | Es necesario que los empleados sean conscientes y conozcan la relevancia de la seguridad de la información puesto que la compañía trata datos sensibles de clientes. | ✔ | | • REF-07-02.2 – Calendario de cursos de seguridad |
| 7.2.3 | ✔ | En caso de brecha de seguridad se precisa de un proceso disciplinario para evitar que se produzcan efectos similares en un futuro. | ✘ | | • NOTA: este documento podría estar desarrollado por el departamento de RR. HH. de la organización . |

## 7.3 Terminación o cambio de empleo

Proteger los intereses de la organización como parte del proceso de cambio o terminación del empleo.

**Estado Actual (AS-IS)**

- No se exige la firma de un acuerdo de confidencialidad a la hora de firmar el contrato. Por ello, se ha dado un caso de divulgación de información cuando un empleado descontento ha dejado la empresa.

**Estado Futuro (TO-BE)**

- La compañía exige la firma de un acuerdo de confidencialidad y no divulgación de información cuando se firma el contrato.

**Documento de Aplicabilidad** (sección)

| Control | Selec. | Justificación selección | Impl. | Justificación exclusión | Referencia |
|---|---|---|---|---|---|
| 7.3.1 | ✔ | El candidato debe asumir la política de seguridad de la compañía y firmar un acuerdo de confidencialidad y no divulgación de la información | ✔ | | • REF-07-01.2 – Acuerdo de confidencialidad |

## 8.1 Responsabilidad por los activos

Identificar activos organizativos y definir responsabilidades de protección apropiadas.

**Estado Actual (AS-IS)**

- La compañía tiene identificados sus activos de una forma vaga. No obstante no tiene definidos los roles y responsabilidades ni tampoco un propietario.
- No existe ningún documento que mencione la propiedad intelectual sobre los productos desarrollados en el ejercicio de sus funciones por parte de los empleados.

**Estado Futuro (TO-BE)**

- Los activos han sido claramente identificados y se han definido responsabilidades y roles de los responsables.
- Los propietarios son los responsables de la gestión de los activos.
- En caso de rescisión de contrato los empleados u otras partes que disponen de activos de la compañía los devuelven tal y como está definido en su contrato.

**Documento de Aplicabilidad** (sección)

| Control | Selec. | Justificación selección | Impl. | Justificación exclusión | Referencia |
|---|---|---|---|---|---|
| 8.1.1 | ✔ | Los activos que tiene la compañía deben ser identificados para conocer su importancia | ✔ | | • REF-06-01.1 – Roles y responsabilidades |
| 8.1.2 | ✔ | Los propietarios son los responsables de los activos que tienen asignados | ✔ | | • REF-06-01.1 – Roles y responsabilidades |
| 8.1.3 | ✔ | Los activos deben ser utilizados de acorde a las actividades de negocio tal y como está estipulado en el contrato entre la compañía y la persona física o jurídica y en la política de seguridad | ✔ | | • REF-05-01.1 Política de seguridad |
| 8.1.4 | ✔ | Los activos deben ser devueltos a la compañía una vez terminado el contrato que les unía a la compañía | ✔ | | • Contrato entre la compañía y la persona física o jurídica que estará disponible en el departamento de administración. |

## 8.2 Clasificación de la información

Asegurar que la información recibe un nivel apropiado de protección de acuerdo con su importancia para la organización.

**Estado Actual (AS-IS)**

- La información no está clasificada. La información se considera interna, publica o confidencial según lo considere la persona que la manipula.
- No se realiza un seguimiento de la información a modo de registro.

**Estado Futuro (TO-BE)**

- La compañía ha establecido unos criterios de clasificación de la información.
- Los activos son tratados en función de los criterios de clasificación.

**Documento de Aplicabilidad** (sección)

| Control | Selec. | Justificación selección | Impl. | Justificación exclusión | Referencia |
|---|---|---|---|---|---|
| 8.2.1 | ✅ | Se necesita identificar la criticidad y valor de la información por posible modificación o divulgación de la misma | ✅ | | • REF-08-02.1 – Clasificación de la información |
| 8.2.2 | ❌ | | | A día de hoy no se ha necesitado etiquetar los activos. La dirección considera que no dispone de muchos activos. Sin embargo, con la ampliación de la compañía en un futuro cercano se considera que será necesario implentará este control. | N/A |
| 8.2.3 | ✅ | Se necesitan definir procedimientos de tratamiento de los activos según la clasificación de la información desarrollada | ✅ | | • REF-08-02.1 – Clasificación de la información |

## 8.3 Manipulación de media

Prevenir la divulgación, modificación, eliminación o destrucción no autorizada de la información almacenada en los medios.

**Estado Actual (AS-IS)**

- Los documentos relevantes así como los equipos removibles (p.ej. pendrives) se almacenan en cajones de los armarios sin seguridad.
- No se realizan copias de seguridad de los datos de los clientes. Se han producido pérdidas de datos por problemas de almacenamiento en algunos dispositivos.
- Se desconoce lo que había en ciertos dispositivos que apenas se han utilizado en meses anteriores. La información es relevante y se ha perdido por no tener un registro de la información.

**Estado Futuro (TO-BE)**

- Aquellos dispositivos que han dejado de ser útiles para la organización son completamente destruidos.
- Todos los dispositivos móviles (p.ej. pendrives) son almacenados en cajones con candados de seguridad.
- Se realiza un registro de todos los datos que se almacenan en los dispositivos móviles de forma que se conoce lo que en ellos había antes de ser destruidos.
- Se realizan copias de seguridad de todo tipo de información sensible.
- Se utiliza criptografía en aquellos dispositivos móviles que contienen información sensible.

| Documento de Aplicabilidad (sección) | | | | | |
|---|---|---|---|---|---|
| **Control** | **Selec.** | **Justificación selección** | **Impl.** | **Justificación exclusión** | **Referencia** |
| 8.3.1 | ✅ | Según la clasificación de la información que contienen, los disposibtivos debe seguir los preceptos disponibles en la política de seguridad | ✅ | | • REF-05-01.1 Política de seguridad |
| 8.3.2 | ✅ | Los dispositivos no útiles que almacenen información sensible deben ser destruidos completamente para no permitir el acceso a su información | ✅ | | • REF-05-01.1 Política de seguridad |
| 8.3.3 | ❌ | | | No se requiere transporte de información física de medios. | N/A |

## 9.1 Requisitos de negocio para el control de acceso

Limitar el acceso a la información y a las instalaciones de procesamiento de la información.

**Estado Actual (AS-IS)**

- La compañía no dispone de una política de seguridad.
- No se han definido claramente los roles y responsabilidades de los empleados ni hay separación de deberes.

**Estado Futuro (TO-BE)**

- La organización ha creado una política de seguridad que contempla el control de acceso.
- Los usuarios y sus roles se revisan de manera periódica. Se realizan actividades de reconciliación que se ejecutan cada 3 meses para comprobar que los usuarios y roles son los que corresponden o si hay que eliminar algunos usuarios (p.ej. en caso de terminar el contrato).
- El administrador de sistema realiza un seguimiento de los servicios de red de manera periódica y mantiene un registro de accesos.

| Documento de Aplicabilidad (sección) | | | | | |
|---|---|---|---|---|---|
| **Control** | **Selec.** | **Justificación selección** | **Impl.** | **Justificación exclusión** | **Referencia** |
| 9.1.1 | ✅ | Se requiere establecer una política de control de acceso a las aplicaciones corporativas que identifique las restricciones, derechos o roles de los usuarios. | ✅ | | • REF-05-01.1 Política de seguridad<br>• REF-06-01.1 – Roles y responsabilidades |
| 9.1.2 | ✅ | Sólo se deben dar permiso a las redes a aquellos usuariosque han sido específicamente autorizados para ello. | ✅ | | • REF-05-01.1 Política de seguridad<br>• REF-06-01.1 – Roles y responsabilidades |

## 9.2 Gestión de acceso de usuarios

Asegurar el acceso de usuario autorizado y prevenir el acceso no autorizado a los sistemas y servicios.

**Estado Actual (AS-IS)**

- No existe control de usuarios bien definido. Se ha dado el caso de crear un mismo usuario dos veces para dos personas con distinta responsabilidad.
- No existe un control de permisos privilegiados. Se ha dado el caso en el que el asesor legal disponía de los mismos accesos a todo tipo de información como el Director General. Esto fue debido a que necesitaba una información puntual únicamente accesible por el Director y por tanto se le permitió acceder a todo tipo de datos.

**Estado Futuro (TO-BE)**

- Se ha definido un proceso de control de acceso para ofrecer derechos a los usuarios de una manera formal y rigurosa.
- Los usuarios deben tener en cuenta la política de seguridad para el control de acceso. Entre otras cosas, deben modificar su contraseña de forma periódica las cuales deben ser difíciles de adivinar.
- Los usuarios y sus roles se revisan de manera periódica. Se pretende realizar actividades de reconciliación que se ejecutarán cada 3 meses para comprobar que los usuarios y roles son los que corresponden o si hay que eliminar algunos usuarios (p.ej. en caso de terminar el contrato).

**Documento de Aplicabilidad** (sección)

| Control | Selec. | Justificación selección | Impl. | Justificación exclusión | Referencia |
|---|---|---|---|---|---|
| 9.2.1 | ✔ | Se requiere de un proceso formal para el control de acceso teniendo en cuenta los roles y responsabilidades. | ✔ | | • REF-06-01.1 – Roles y responsabilidades |
| 9.2.2 | ✔ | Se requiere de un proceso formal para el control de acceso teniendo en cuenta los roles y responsabilidades. | ✔ | | • REF-06-01.1 – Roles y responsabilidades |
| 9.2.3 | ✔ | Es necesario que el acceso a ciertos datos se ofrezca a usuarios autorizados. | ✔ | | • REF-06-01.1 – Roles y responsabilidades |
| 9.2.4 | ✔ | Los usuarios deben mantener secreta la información de acceso a sus cuentas. | ✔ | | • REF-05-01.1 Política de seguridad<br>• REF-06-01.1 – Roles y responsabilidades |
| 9.2.5 | ✔ | Se requiere realizar actividades de reconciliación de forma regular | ✘ | | • REF-06-01.1 – Roles y responsabilidades |
| 9.2.5 | ✔ | Se requiere realizar una revisión de los derechos de acceso de los usuarios en caso de finalización del contrato con la compañía. | ✔ | | • REF-06-01.1 – Roles y responsabilidades |

## 9.3 Responsabilidades de los usuarios

Asegurar que los usuarios sean responsables para la salvaguarda de la información de autenticación.

**Estado Actual (AS-IS)**

- Los usuarios son conscientes de la responsabilidad para mantener sus datos de autenticación. No obstante, no suelen tenerlo muy en cuenta. Tienen a escribir sus contraseñas en papeles fácilmente accesibles o simplemente sus contraseñas son muy fáciles de adivinar.

**Estado Futuro (TO-BE)**

- La política de seguridad define el control de acceso que se realiza en la compañía. Los empleados siguen los preceptos que allí se incluyen.

**Documento de Aplicabilidad** (sección)

| Control | Selec. | Justificación selección | Impl. | Justificación exclusión | Referencia |
|---|---|---|---|---|---|
| 9.3.1 | ✔ | Los usuarios deben mantener secreta la información de acceso a sus cuentas. | ✔ | | • REF-05-01.1 Política de seguridad<br>• REF-06-01.1 – Roles y responsabilidades |

## 9.4 Control de acceso a sistemas y aplicaciones

Prevenir el acceso no autorizado a los sistemas y aplicaciones.

**Estado Actual (AS-IS)**

- No existe control de acceso a las aplicaciones. Por ejemplo, se pueden realizar múltiples intentos sin que el sistema se bloquee, los campos de las contraseñas no se ocultan, etc.
- No existe control de gestión de contraseñas de forma que el sistema permite que se utilicen contraseñas con poca seguridad

**Estado Futuro (TO-BE)**

- El sistema controla el número de intentos de acceso. Utiliza sistemas CAPTCHA. No permite que se visualice el contenido de las contraseñas.
- Se exige que las contraseñas se cambien de forma regular.
- El sistema exige el uso de contraseñas robustas.
- El control de acceso al código fuente del software sólo está disponible para los empleados directamente relacionados con el desarrollo.

**Documento de Aplicabilidad** (sección)

| Control | Selec. | Justificación selección | Impl. | Justificación exclusión | Referencia |
|---|---|---|---|---|---|
| 9.4.1 | ✔ | Se necesita que haya restricciones de acceso según lo definido en la política de seguridad de la compañía. | ✔ | | • REF-05-01.1 Política de seguridad |

## 9.4 Control de acceso a sistemas y aplicaciones

Prevenir el acceso no autorizado a los sistemas y aplicaciones.

| | | | | | |
|---|---|---|---|---|---|
| 9.4.2 | ✔ | Se requiere utilizar un procedimiento para un acceso controlado | ✔ | | • REF-05-01.1 Política de seguridad |
| 9.4.3 | ✔ | Se precisa de un soporte para la creación de contraseñas robustas | ✘ | | • REF-05-01.1 Política de seguridad |
| 9.4.4 | ✘ | | | No se utilizan programas utilitarios privilegiados | N/A |
| 9.4.5 | ✔ | La compañía realiza desarrollos software. Sólo las personas dedicadas a estas actividades deben tener acceso al código fuente | ✔ | | • REF-05-01.1 Política de seguridad |

## 10.1 Controles criptográficos

Asegurar el uso apropiado y efectivo de la criptografía para proteger la confidencialidad, autenticación y/o la integridad de la información.

**Estado Actual (AS-IS)**

- No se utiliza ningún tipo de encriptación para proteger la información sensible.

**Estado Futuro (TO-BE)**

- No se ha definido una política sobre el uso de controles criptográficos. No obstante se utiliza encriptación para el envío de mensajes.

**Documento de Aplicabilidad** (sección)

| Control | Selec. | Justificación selección | Impl. | Justificación exclusión | Referencia |
|---|---|---|---|---|---|
| 10.1.1 | ✘ | | | No se ha definido una política de encriptación. La compañía no está preparada para llevarlo a cabo. Está estudiando la contratación de un servicio externo que ayude a su implementación en un futuro | N/A |
| 10.1.2 | ✘ | | | Ver exclusión del control 10.1.1 | N/A |

## 11.1 Áreas seguras

Prevenir el acceso físico no autorizado, daños e interferencias a las instalaciones de procesamiento de información e información de la organización.

**Estado Actual (AS-IS)**

- La compañía tiene en cuenta la seguridad física a sus instalaciones aplicando ciertos controles: existe una zona de servidores, el almacen está separado de las oficinas, tiene bolardos en la entrada principal de las oficinas, etc. No obstante, el control no es muy exhaustivo.

**Estado Futuro (TO-BE)**

- La compañía tiene zonas claramente separadas donde se encuentra la información sensible (ver plano de las instalaciones disponible en este mismo capítulo).
- Dispone de barreras físicas de acceso al edificio mediante bolardos.
- Se lleva un registro de acceso a las instalaciones. La secretaria apunta el nombre de la persona que accede, fecha y hora de entrada y salida, persona a la que visita, etc.
- La compañía ha creado tarjetas identificativas que permiten el acceso a ciertas zonas de las instalaciones. Por ejemplo, el administrador y responsable tecnológico pueden acceder a la sala de servidores gracias a los derechos de acceso que tienen en sus tarjetas identificativas. Sin embargo, los operadores de almacén o los teleoperadores no pueden.
- Se dispone de 2 extintores en la planta alta y 2 en la planta baja de las oficinas. El almacen dispone de 3 extintores.
- Los edificios disponen de detectores de presencia, alarma conectada a servicios de seguridad y CCTV (Circuito Cerrado de Televisión para Vigilancia). El registro del vídeo se almacena durante 72 horas cubriendo fines de semana.

**Documento de Aplicabilidad** (sección)

| Control | Selec. | Justificación selección | Impl. | Justificación exclusión | Referencia |
|---|---|---|---|---|---|
| 11.1.1 | ✔ | Existen distintas zonas que separan los datos con información sensible (p.ej. la sala de servidores, o los despachos de los responsables de área y del director general están en distintas plantas) | ✔ | | • Plano de las instalaciones |
| 11.1.2 | ✔ | Se precisa que ciertas personas tengan acceso a ciertas zonas de las instalaciones | ✔ | | • REF-11-01.2 – Acceso a las instalaciones |
| 11.1.3 | ✘ | | | Las instalaciones son muy pequeñas. Resulta muy difícil evitar que se tenga conocimiento de las zonas donde se encuentra la información sensible. De todas maneras, con la ampliación de la compañía en un futuro, se procederá a aplicar este control para evitar esta situación. | N/A |
| 11.1.4 | ✘ | | | La compañía no se encuentra en una zona de riesgo medioambiental (p.ej. aludes, terremotos, fuego, etc.) | N/A |
| 11.1.5 | ✘ | | | Las instalaciones son muy pequeñas. Con la ampliación de la | N/A |

## 11.1 Áreas seguras

Prevenir el acceso físico no autorizado, daños e interferencias a las instalaciones de procesamiento de información e información de la organización.

| | | | | | |
|---|---|---|---|---|---|
| | | | | compañía en un futuro, se procederá a aplicar este control. | |
| 11.1.6 | ✔ | Es preciso que el área de carga y descarga esté separada de las oficinas. Sólo se permite acceder a las oficinas en caso de que la tarjeta identificativa de la persona les permita. | ✔ | | • Plano de las instalaciones |

## 11.2 Equipos

Prevenir la pérdida, el daño, el robo o el compromiso de los activos y la interrupción de las operaciones de la organización.

**Estado Actual (AS-IS)**

- La zona de máquinas no dispone de control de temperaturas. La zona de servidores siempre tiene una temperatura elevada.
- No se revisa el mantenimiento de las máquinas.
- La documentación se suele dejar encima de las mesas independientemente de tratarse o no de información sensible.
- No se utilizan salvapantallas para bloquear el ordenador después de no utilizarse en un tiempo.
- Algunos equipos se mueven en las instalaciones (p.ej. se dejan en una sala de reuniones en lugar de llevarlo consigo en todo momento).
- No se utilizan cables de seguridad para los ordenadores portátiles.

**Estado Futuro (TO-BE)**

- La compañía ha aplicado la política de "Escritorio y pantallas limpios".
- Se utilizan cables de seguridad para todos los ordenadores portátiles.
- Los equipos están siempre localizados.
- La compañía tiene control de temperatura y humedad para la zona de servidores y dispone así mismo sistemas de refrigeración y calefacción en las oficinas.
- Se siguen siempre las recomendaciones de mantenimiento por parte de los fabricantes para evitar posibles daños.
- Se utilizan siempre salvapantallas de bloqueo en caso de no utilización de la máquina

**Documento de Aplicabilidad** (sección)

| Control | Selec. | Justificación selección | Impl. | Justificación exclusión | Referencia |
|---|---|---|---|---|---|
| 11.2.1 | ✔ | Los equipos tienen que estar localizados y protegidos. | ✔ | | N/A |
| 11.2.2 | ✔ | Se requiere revisar el estado en el que se encuentran los servicios públicos (p.ej. agua, electricidad, etc). | ✔ | | N/A |
| 11.2.3 | ✘ | | | El cableado de las instalaciones fue creado antes de que la | N/A |

## 11.2 Equipos

Prevenir la pérdida, el daño, el robo o el compromiso de los activos y la interrupción de las operaciones de la organización.

| | | | | | |
|---|---|---|---|---|---|
| | | | | compañía se desplazase a esta nueva localización. | |
| 11.2.4 | ✔ | Se requiere seguir las recomendaciones de los fabricantes de los equipos. | ✔ | | N/A |
| 11.2.5 | ✔ | Se requiere un control de aquellos activos que se han retirado de las instalaciones. | ✘ | | N/A |
| 11.2.6 | ✘ | | | Aunque algunas personas disponen de portátiles, no se permite actualmente realizar teletrabajo. Se está considerando en caso de que la empresa se extienda a distintas localizaciones en Europa y Sudamérica. No se permite utilizar los portátiles si el empleado no está en las instalaciones. | • REF-05-01.1 Política de seguridad |
| 11.2.7 | ✔ | Se debe asegurar que posibles datos sensibles hayan sido eliminados en caso de reutilización o eliminación de los equipos. | ✘ | | N/A |
| 11.2.8 | ✔ | Todos los equipos si no se utilizan deben tener algún tipo de protección. | ✔ | | • REF-05-01.1 Política de seguridad |
| 11.2.9 | ✔ | Se requiere que la información sensible no esté disponible en los escritorios a no ser necesario para las actividades del trabajo. | ✔ | | • REF-05-01.1 Política de seguridad |

## 12.1 Procedimientos operacionales y responsabilidades

Asegurar operaciones correctas y seguras de las instalaciones de procesado de la información.

**Estado Actual (AS-IS)**

- Los procedimientos operacionales no se han documentado. La compañía es todavía inmadura.
- La compañía tiene distintas zonas para la el desarrollo, pruebas y operación.
- No se gestionan los cambios de los procesos de negocio. Todo se realiza ad-hoc y sobre la marcha.

**Estado Futuro (TO-BE)**

- La compañía ha documentado sus procedimientos operacionales para poder conocer la manera de trabajar, como se interactúa en las actividades de negocio, el tipo de herramientas que se necesitan, los tiempos de ejecución, etc.
- La compañía gestiona los cambios que se realizan en los procesos de negocio.
- Se estudian futuros requisitos de la compañía para el desarrollo de los objetivos de negocio.
- La compañía tiene distintas zonas para la el desarrollo, pruebas y operación.

| Documento de Aplicabilidad (sección) | | | | | |
|---|---|---|---|---|---|
| **Control** | **Selec.** | **Justificación selección** | **Impl.** | **Justificación exclusión** | **Referencia** |
| 12.1.1 | ✔ | Se precisan documentar todos los procesos operativos para hacerlos disponibles a todas las personas que lo necesiten | ✔ | | N/A |
| 12.1.2 | ✔ | Es necesario gestionar los cambios en la organización que puedan afectar a la seguridad de la información. | ✔ | | N/A |
| 12.1.3 | ✔ | Se preciso realizar una gestión de la capacidad para futuros cambios organizativos. Más si cabe sabiendo los planes de expansión estratégicos que tiene la compañía. | ✔ | | N/A |
| 12.1.4 | ✔ | La compañía desarrolla software y por tanto se recomienda separar las zonas de desarrollo, pruebas y operación. | ✔ | | • Plano de las instalaciones |

## 12.2 Protección contra códigos maliciosos

Asegurar que la información y las instalaciones de procesado de la información están protegidas contra los códigos maliciosos.

**Estado Actual (AS-IS)**

- La organización utiliza antivirus aunque no lo suele actualizar.
- Se permite el acceso a páginas de descarga gratuitas. Por esa razón se suele introducir código malicioso.
- Los empleados realizan instalación de aplicaciones a su libre albedrío.
- No existe actualización automática de aplicaciones.

**Estado Futuro (TO-BE)**

- El antivirus se actualiza de forma automática.
- Las aplicaciones se actualizan de forma automática
- Se bloquea el acceso a páginas de descargas gratuitas.
- Las instalaciones sólo las puede realizar el administrador con la aprobación del Responsable Tecnológico.

| Documento de Aplicabilidad (sección) | | | | | |
|---|---|---|---|---|---|
| **Control** | **Selec.** | **Justificación selección** | **Impl.** | **Justificación exclusión** | **Referencia** |
| 12.2.1 | ✔ | Se requiere la protección contra código malicioso para que impida que se vea afectada la confidencialidad, integridad y disponibilidad de la información. | ✔ | | • REF-05-01.1 Política de seguridad |

## 12.3 Copias de respaldo

Proteger contra la pérdida de datos.

**Estado Actual (AS-IS)**

- No se suelen realizar copias de seguridad de la información.
- En el caso de realizarse no se verifican dichos datos pasado un tiempo.

**Estado Futuro (TO-BE)**

- Se realizan copias de seguridad de los datos. Se suelen hacer de manera incremental cada semana.
- Se realizan verificaciones periódicas de las copias de seguridad.

**Documento de Aplicabilidad** (sección)

| Control | Selec. | Justificación selección | Impl. | Justificación exclusión | Referencia |
|---|---|---|---|---|---|
| 12.3.1 | ✔ | Se tienen que realizar copias de seguridad ante posibles pérdidas de información y verificar de forma periódica que la información no se haya deteriorado. | ✔ | | N/A |

## 12.4 Registro y monitorización

Registrar eventos y generar evidencias.

**Estado Actual (AS-IS)**

- No se registran los eventos que se producen en los sistemas.

**Estado Futuro (TO-BE)**

- Se registran los eventos que se producen en los sistemas. Entre otros las actividades realizadas por el administrador del sistema.

**Documento de Aplicabilidad** (sección)

| Control | Selec. | Justificación selección | Impl. | Justificación exclusión | Referencia |
|---|---|---|---|---|---|
| 12.4.1 | ✔ | Se tienen que registrar todos los eventos de seguridad que se producen en los sistemas de la organización. | ✔ | | N/A |
| 12.4.2 | ✔ | Es necesario proteger la información de los registros para evitar que sea modificada. | ✘ | | N/A |
| 12.4.3 | ✔ | Las actividades del administrador deben registrarse puesto que están capacitados para modificar logs. | ✘ | | N/A |
| 12.4.4 | ✘ | | | No se disponen de varios sistemas por lo que no se requiere la sincronización de relojes | N/A |

## 12.5 Control de software operacional

Asegurar la integridad de los sistemas operacionales.

**Estado Actual (AS-IS)**

- Los usuarios instalan operaciones por su propia cuenta. Se han dado caso de aplicaciones maliciosas.

**Estado Futuro (TO-BE)**

- Sólo el administrador puede instalar aplicaciones en los equipos previa autorización del responsable.

**Documento de Aplicabilidad** (sección)

| Control | Selec. | Justificación selección | Impl. | Justificación exclusión | Referencia |
|---|---|---|---|---|---|
| 12.5.1 | ✔ | Se requiere un control en las instalaciones de software para los equipos de los empleados. | ✔ | | • REF-05-01.1 Política de seguridad |

## 12.6 Gestión de la vulnerabilidad técnica

Prevenir la explotación de las vulnerabilidades técnicas.

**Estado Actual (AS-IS)**

- No existe una definición de roles y responsabilidades bien definido. Las vulnerabilidades no son bien gestionadas.
- Los usuarios instalan operaciones por su propia cuenta. Se han dado caso de aplicaciones maliciosas.

**Estado Futuro (TO-BE)**

- Los roles y responsabilidades están definidos. Las vulnerabilidades están gestionadas por la persona identificada como responsable de las mismas. Suele ser el administrador de sistemas.
- Sólo el administrador puede instalar aplicaciones en los equipos previa autorización del responsable.
- Se registran todas las aplicaciones que han sido instaladas o eliminadas por equipo.
- No se permite la utilización de máquinas virtuales a excepción de los equipos de desarrollo y siempre y cuando sean necesarios para aplicaciones propias del negocio.

**Documento de Aplicabilidad** (sección)

| Control | Selec. | Justificación Selección | Impl. | Justificación exclusión | Referencia |
|---|---|---|---|---|---|
| 12.6.1 | ✔ | Se precisa gestionar la forma de tratar las vulnerabilidades de los sistemas e identificar claramente los roles y responsabilidades de los empleados. | ✔ | | • REF-06-01.1 – Roles y responsabilidades |
| 12.6.2 | ✔ | Se requiere un control en las instalaciones de software para los equipos de los empleados | ✔ | | • REF-05-01.1 Política de seguridad |

## 12.7 Consideraciones sobre auditorias de sistemas de información

Minimizar el impacto de las actividades de auditoría en los sistemas operacionales.

**Estado Actual (AS-IS)**

- No se realizaba auditoría alguna.

**Estado Futuro (TO-BE)**

- La compañía realiza auditorías de calidad y de seguridad de la información.

**Documento de Aplicabilidad** (sección)

| Control | Selec. | Justificación selección | Impl. | Justificación exclusión | Referencia |
|---|---|---|---|---|---|
| 12.7.1 | ✔ | Se precisa realizar controles de auditoría de los sistemas para verificar que se tiene en consideración la seguridad de la información al realizarse tratamiento de datos sensibles. | ✔ | | N/A |

## 13.1 Gestión de seguridad de las redes

Asegurar la protección de la información en redes y en las instalaciones de procesado de la información de soporte.

**Estado Actual (AS-IS)**

- La organización no tiene segmentada la red.

**Estado Futuro (TO-BE)**

- La organización tiene segmentadas las áreas en 2, una para el desarrollo del software y otra para el resto de actividades de la compañía.
- La administración de las redes la lleva a cabo exclusivamente el administrador de sistemas.

**Documento de Aplicabilidad** (sección)

| Control | Selec. | Justificación selección | Impl. | Justificación exclusión | Referencia |
|---|---|---|---|---|---|
| 13.1.1 | ✔ | Se precisa controlar la información que circula en la red de la organización para evitar el acceso no autorizado a información sensible. | ✔ | | N/A |
| 13.1.2 | ✔ | Se necesita definir acuerdos de servicio con el proveedor de servicios de la red y monitorizarlo a través de SLAs y proceder con auditorias si se considera oportuno. | ✘ | | N/A |
| 13.1.3 | ✔ | La compañía ha segregado la red en 2 dominios. Se requiere un control a tal efecto. | ✔ | | N/A |

## 13.2 Transferencia de información

Mantener la seguridad de información transferida dentro de la organización y con cualquier entidad externa.

**Estado Actual (AS-IS)**

- No existe política de seguridad de la información.
- La compañía distribuye información de forma interna sin control. Algunos empleados disponen de datos con información sensible.

**Estado Futuro (TO-BE)**

- Existe un control para transferir la información según la clasificación de la información.
- Se utiliza encriptación en el envío de los emails.
- Se han definido acuerdos de confidencialidad y no divulgación de información para los empleados y terceras partes.
- El plan de formación para la concienciación de los empleados presenta la necesidad de realizar un control para la transferencia de la información dentro de la compañía y hacia el exterior.

**Documento de Aplicabilidad** (sección)

| Control | Selec. | Justificación selección | Impl. | Justificación exclusión | Referencia |
|---|---|---|---|---|---|
| 13.2.1 | ✔ | Se requiere una política de transferencia de la información para evitar la distribución fuera del ámbito contractual entre las partes. | ✔ | | • REF-05-01.1 Política de seguridad<br>• REF-07-02.2 – Calendario de cursos de seguridad<br>• REF-08-02.1 – Clasificación de la información |
| 13.2.2 | ✔ | Se precisa la definición de acuerdos de confidencialidad y no divulgación tanto para empleados como para terceras partes para evitar divulgación de datos sensibles e inclumplimiento de la ley de protección intelectual. | ✔ | | • REF-07-01.2 – Acuerdo de confidencialidad y no divulgación<br>• REF-08-02.1 – Clasificación de la información |
| 13.2.3 | ✔ | Se requiere de una encriptación de la información para el envío de emails. | ✔ | | • REF-05-01.1 Política de seguridad |
| 13.2.4 | ✔ | Se precisa la definición de acuerdos de confidencialidad y no divulgación tanto para empleados como para terceras partes para evitar divulgación de datos sensibles e inclumplimiento de la ley de protección intelectual | ✔ | | • REF-07-01.2 – Acuerdo de confidencialidad y no divulgación<br>• REF-08-02.1 – Clasificación de la información |

## 14.1 Requisitos de seguridad de los sistemas de información

Asegurar que la seguridad de la información es una parte integral de los sistemas de información en todo el ciclo de vida. Esto además incluye los requisitos para los sistemas de información los cuales proporcionan servicios sobre redes públicas.

**Estado Actual (AS-IS)**

- La compañía tiene una página web desde la cual se pueden comprar sus productos de montaña. No obstante no existe control alguno para la transacción de los servicios.

**Estado Futuro (TO-BE)**

- Se utiliza firma electrónica para las facturas electrónicas. Se ha establecido que se utilizará el estándar FacturaE.
- Todo desarrollo software tiene en cuenta requisitos de seguridad.
- Se dispone de controles de autenticación y autorización para el acceso de los clientes a la cesta de la compra.
- Los clientes puede realizar compras seleccionando el tipo de pago seguro.
- Se utiliza encriptación en la transmisión de la información y en los protocolos utilizados.
- Todos los datos se gestionan en sistemas de la compañía y no se hace uso de terceros (p.ej. "en la nube").

**Documento de Aplicabilidad** (sección)

| Control | Selec. | Justificación selección | Impl. | Justificación exclusión | Referencia |
|---|---|---|---|---|---|
| 14.1.1 | ✔ | Se requiere que a la hora de definir requisitos para los desarrollos se tengan en cuenta también aquellos que son no funcionales, en concreto, requisitos de seguridad de la información. | ✔ | | • REF-05-01.1 Política de seguridad |
| 14.1.2 | ✔ | Se precisa controlar la información que circula por las redes públicas para evitar una posible modificación o divulgación. | ✔ | | N/A |
| 14.1.3 | ✔ | Se necesita proteger las aplicaciones de transacciones de servicio para evitar una posible modificación o divulgación de la información incluída en las comunicaciones. | ✔ | | • REF-05-01.1 Política de seguridad |

## 14.2 Seguridad en los procesos de desarrollo y soporte

Asegurar que la seguridad de la información está diseñada e implementada dentro del ciclo de vida de desarrollo de los sistemas de información.

**Estado Actual (AS-IS)**

- Los nuevos desarrollos no consideran la seguridad de información a la hora de definir los requisitos. Se han producido multitud de ataques por esta razón (i.e. SQLInjection).
- Los procesos relacionados con la seguridad de la información no se suelen documentar.

**Estado Futuro (TO-BE)**

- Se documentan los procesos relacionados con la seguridad de la información.
- Los requisitos de seguridad son considerados desde el inicio de cualquier proyecto de desarrollo software.
- Los desarrollos utilizan siempre control de versiones y cambios.
- La CMDB está siempre actualizada. El administrador es el encargado de su gestión.

| Documento de Aplicabilidad (sección) | | | | | |
|---|---|---|---|---|---|
| **Control** | **Selec.** | **Justificación selección** | **Impl.** | **Justificación exclusión** | **Referencia** |
| 14.2.1 | ✔ | Se requiere de una política de desarrollo que se aplicará para todos los desarrollos software. | ✔ | | • REF-05-01.1 Política de seguridad<br>• Política de desarrollo de software (**NOTA**: no disponible en este TFM pues está fuera de su alcance) |
| 14.2.2 | ✔ | Los cambios de los sistemas necesarios en el desarrollo del software deben estar controlados a través de una gestión de cambios | ✔ | | N/A |
| 14.2.3 | ✘ | | | No se considera a día de hoy ningún cambio en la plataforma de operación | N/A |
| 14.2.4 | ✘ | | | No se requiere a día de hoy ningún cambio en los paquetes de software que se utilizan para los desarrollos de software | N/A |
| 14.2.5 | ✔ | Se requiere de una política de desarrollo que se aplicará para todos los desarrollos software. Está totalmente relacionado con el 14.2.1 | ✔ | | • REF-05-01.1 Política de seguridad<br>• Política de desarrollo de software (**NOTA**: no disponible en este TFM pues está fuera de su alcance) |
| 14.2.6 | ✔ | Se necesita definir un entorno seguro de desarrollo que cubrirá todo el ciclo de vida de los proyectos. | ✔ | | • Política de desarrollo de software (**NOTA**: no disponible en este TFM pues está fuera de su alcance) |
| 14.2.7 | ✘ | | | No existe desarrollo externo subcontratado | N/A |
| 14.2.8 | ✔ | Se requiere que se realicen pruebas de seguridad de los sistemas durante el desarrollo. | ✔ | | N/A |
| 14.2.9 | ✔ | Se requiere que se realicen pruebas de aceptación de los sistemas durante el desarrollo. | ✔ | | N/A |

## 14.3 Datos de prueba

Asegurar la protección de los datos utilizados para las pruebas.

**Estado Actual (AS-IS)**

- Los datos que se utilizan en las pruebas no se protegen. Se utilizan datos reales que identifican a la persona. No son datos ficticios.
- No se registran los datos que han sido utilizados y que pueden ser útiles para posibles auditorías.

**Estado Futuro (TO-BE)**

- Los datos que se utilizan para realizar pruebas son siempre simulados para evitar utilizar datos sensibles que identifiquen a la persona.
- Se aplican controles de seguridad para el acceso a este tipo de datos de la misma forma que si se utilizaran datos reales.
- Los datos de prueba no reales se eliminan una vez utilizados.

**Documento de Aplicabilidad** (sección)

| Control | Selec. | Justificación selección | Impl. | Justificación exclusión | Referencia |
|---|---|---|---|---|---|
| 14.3.1 | ✔ | Los datos de prueba deben ser protegidos y controlados para evitar que se disponga de información sensible que pueda identificar a la persona. | ✔ | | • REF-05-01.1 Política de seguridad<br>• Política de desarrollo de software (**NOTA**: no disponible en este TFM pues está fuera de su alcance) |

## 15.1 Seguridad de la información en las relaciones con los proveedores

Asegurar la protección de los activos de la organización que son accesibles por los proveedores.

**Estado Actual (AS-IS)**

- No se realiza un control exhaustivo de la información a la que pueden acceder los proveedores como por ejemplo la información de clientes.
- No existe clasificación de la información.

**Estado Futuro (TO-BE)**

- Se controla la información que se proporciona a los proveedores.
- Se ha definido una clasificación de la información.
- Se exige la firma de un acuerdo de confidencialidad y no divulgación por parte de los proveedores.
- Existe una gestión de incidentes y resolución de defectos.
- Como parte de la concienciación del empleado, se han preparado cursos que explican como relacionarse con los proveedores.

| Documento de Aplicabilidad (sección) | | | | | |
|---|---|---|---|---|---|
| **Control** | **Selec.** | **Justificación selección** | **Impl.** | **Justificación exclusión** | **Referencia** |
| 15.1.1 | ✔ | Se requiere controlar los requisitos de seguridad de la información para mitigar los riesgos del acceso que pueda tener el proveedor con los activos de la organización. | ✔ | | • REF-05-01.1 Política de seguridad<br>• REF-07-02.2 – Calendario de cursos de seguridad<br>• REF-08-02.1 – Clasificación de la información |
| 15.1.2 | ✔ | Se deben definir acuerdos de no divulgación y confidencialidad con los proveedores que puedan tener acceso a información sensible. Esta información debe indicar los requisitos que traten con posibles riesgos de seguridad. | ✔ | | • REF-07-01.2 – Acuerdo de confidencialidad y no divulgación<br>• REF-08-02.1 – Clasificación de la información |
| 15.1.3 | ✔ | Se deben definir acuerdos de no divulgación y confidencialidad con los proveedores que puedan tener acceso a información sensible. Esta información debe indicar los requisitos que traten con posibles riesgos de seguridad. | ✔ | | • REF-07-01.2 – Acuerdo de confidencialidad y no divulgación |

## 15.2 Gestión de la prestación de servicios con los proveedores

Mantener un nivel acordado de seguridad de la información y entrega de servicios de acuerdo con los acuerdos con los proveedores.

**Estado Actual (AS-IS)**

- No existe un control exhaustivo de los servicios que ofrecen los proveedores.

**Estado Futuro (TO-BE)**

- La organización monitoriza el servicio ofrecido por los proveedores a través de SLAs.
- Se ha definido un acuerdo de servicio y de confidencialidad y no divulgación con los proveedores.

| Documento de Aplicabilidad (sección) | | | | | |
|---|---|---|---|---|---|
| **Control** | **Selec.** | **Justificación selección** | **Impl.** | **Justificación exclusión** | **Referencia** |
| 15.2.1 | ✔ | Se requiere monitorizar los servicios que ofrece el proveedor | ✔ | | • REF-07-01.2 – Acuerdo de confidencialidad y no divulgación.<br>• Contrato entre la compañía y el proveedor (**NOTA**: no disponible en este TFM pues está fuera de su alcance) |
| 15.2.2 | ✘ | | | No se preveen cambios por el momento con los proveedores. Tal vez con la futura expansión de la compañía. Entonces se revisarán los acuerdos de servicio y se implementará este control | N/A |

## 16.1 Gestión de incidentes y mejoras de seguridad de la información

Asegurar un enfoque consistente y efectivo para la gestión de los incidentes de seguridad de la información, incluyendo la comunicación sobre eventos y debilidades de seguridad.

**Estado Actual (AS-IS)**

- Cuando se produce un incidente, no siempre se notifica ni se recoge la evidencia.
- Los empleados no son consciente de la relevancia de un incidente y como puede afectar a la seguridad.

**Estado Futuro (TO-BE)**

- Cuando se produce cualquier tipo de incidencia, se notifica al responsable tecnológico y al administrador de sistemas.
- Los incidentes son clasificados y registrados como evidencia.
- Los incidentes son tratados como lecciones aprendidas.

| Documento de Aplicabilidad (sección) | | | | | |
|---|---|---|---|---|---|
| **Control** | **Selec.** | **Justificación selección** | **Impl.** | **Justificación exclusión** | **Referencia** |
| 16.1.1 | ✔ | Los procedimientos y responsabilidades se deben establecer para tener una rápida respuesta ante un incidente | ✔ | | • REF-05-01.1 Política de seguridad<br>• REF-06-01.1 – Roles y responsabilidades |
| 16.1.2 | ✔ | Los indidentes que se produzcan deben ser siempre comunicados. | ✔ | | • REF-05-01.1 Política de seguridad |
| 16.1.3 | ✔ | Se deben notificar aquellas debilidades encontradas en el sistema | ✔ | | • REF-05-01.1 Política de |

## 16.1 Gestión de incidentes y mejoras de seguridad de la información

Asegurar un enfoque consistente y efectivo para la gestión de los incidentes de seguridad de la información, incluyendo la comunicación sobre eventos y debilidades de seguridad.

| | | | | | |
|---|---|---|---|---|---|
| | | como medida de prevención de posibles incidentes | | | seguridad |
| 16.1.4 | ✔ | Se deben evaluar los incidentes producidos y clasificarlos como incidentes de seguridad si procede | ✔ | | N/A |
| 16.1.5 | ✔ | Se deben responder los incidentes de acuerdo a los procedimientos documentados | ✔ | | N/A |
| 16.1.6 | ✔ | Se recolección de lecciones aprendidas sirve para la reducción de la probabilidad o impacto de incidentes potenciales en el futuro | ✔ | | N/A |
| 16.1.7 | ✔ | Se deben recoger todas las evidencias relacionadas con los incidentes de seguridad | ✔ | | • REF-05-01.1 Política de seguridad |

## 17.1 Continuidad de seguridad de la información

La continuidad de la seguridad de la información debe integrarse en los sistemas de la gestión de la continuidad del negocio de la organización.

**Estado Actual (AS-IS)**

- No existe un plan de continuidad relativo a la seguridad de la información.

**Estado Futuro (TO-BE)**

- A la hora de planificar la continuidad del negocio se tiene en cuenta la continuidad de la seguridad de la información.
- Se han programado simulacros para la verificación de la continuidad de los sistemas de información comprobando los procedimientos y controles puestos en funcionamiento aunque no se han implementado todavía.

**Documento de Aplicabilidad** (sección)

| Control | Selec. | Justificación selección | Impl. | Justificación exclusión | Referencia |
|---|---|---|---|---|---|
| 17.1.1 | ✔ | Se precisa una planificación documentada con la estructura organizativa según la responsabilidad y competencia para la gestión de los incidentes. | ✔ | | • REF-06-01.1 – Roles y responsabilidades |
| 17.1.2 | ✔ | Se tiene que implementar la continuidad del negocio teniendo en cuenta la continuidad de la seguridad de la información | ✔ | | N/A |
| 17.1.3 | ✔ | Se debe verificar la la continuidad de los sistemas de información comprobando los controles puestos en funcionamiento. | ✘ | | N/A |

## 17.2 Redundancias

Asegurar la disponibilidad de las instalaciones de procesado de la información.

**Estado Actual (AS-IS)**

- La compañía no dispone de sistemas redundantes para asumir la continuidad del servicio.

**Estado Futuro (TO-BE)**

- La compañía no dispone de sistemas redundantes para asumir la continuidad del servicio. No obstante, con la futura expansión de la compañía se prevé dotar a la organización de unas instalaciones redundantes.

**Documento de Aplicabilidad** (sección)

| Control | Selec. | Justificación selección | Impl. | Justificación exclusión | Referencia |
|---|---|---|---|---|---|
| 17.2.1 | ✗ | | | La compañía no dispone de sistemas redundantes para asumir la continuidad del servicio. | N/A |

## 18.1 Cumplimiento con los requisitos legales y contractuales

Evitar incumplimientos de obligaciones legales, estatutarias, reglamentarias o contractuales relacionadas con la seguridad de la información y con cualquier requisito de seguridad.

**Estado Actual (AS-IS)**

- La organización es consciente de que existen regulaciones a cumplir pero no prestan la suficiente atención.
- La información personal es tratada sin mucho control.
- Se utiliza software descargado de forma ilegal incumpliendo las leyes de protección intelectual.

**Estado Futuro (TO-BE)**

- La organización aplica los procedimientos necesarios para el cumplimiento de la GDPR y la LOPDP. Entre otros, la aplicación de esta guía de fácil implementación para las PYME.
- No se utiliza software ilegal y se respetan los derechos de propiedad intelectual.
- Se utiliza encriptación para el envío de mensajería según las regulaciones vigentes.

**Documento de Aplicabilidad** (sección)

| Control | Selec. | Justificación selección | Impl. | Justificación exclusión | Referencia |
|---|---|---|---|---|---|
| 18.1.1 | ✓ | Se exige la aplicación de la GDPR y LOPDP para España | ✓ | | N/A |
| 18.1.2 | ✓ | Los derechos de propiedad deben ser siempre cumplidos | ✓ | | N/A |
| 18.1.3 | ✓ | Todos los registros tomados deben ser protegidos para evitar posibles modificaciones, destrucciones o pérdidas. | ✓ | | N/A |

## 18.1 Cumplimiento con los requisitos legales y contractuales

Evitar incumplimientos de obligaciones legales, estatutarias, reglamentarias o contractuales relacionadas con la seguridad de la información y con cualquier requisito de seguridad.

| | | | | | |
|---|---|---|---|---|---|
| 18.1.4 | ✓ | La información personal identificable debe ser protegida y considerada como privada | ✓ | | N/A |
| 18.1.5 | ✓ | Se necesitan aplicar controles criptográficos según las regulaciones vigentes. | ✓ | | N/A |

## 18.2 Revisiones de seguridad de la información

Asegurar que la seguridad de la información se implementa y opera de acuerdo con las políticas y procedimientos de la organización.

**Estado Actual (AS-IS)**

- No existe política de seguridad de la información.

**Estado Futuro (TO-BE)**

- La política de seguridad de la información es revisada una vez al año por personas que no han participado directamente en su creación.
- Los responsables de área revisan de forma periódica que se aplican los procedimientos que están dentro de su ámbito de responsabilidad.
- Todos los cambios están documentados.

**Documento de Aplicabilidad** (sección)

| Control | Selec. | Justificación selección | Impl. | Justificación exclusión | Referencia |
|---|---|---|---|---|---|
| 18.2.1 | ✓ | Se precisa una revisión de la política de seguridad de forma independiente en intervalos regulares. | ✓ | | N/A |
| 18.2.2 | ✓ | La dirección y los responsables de área deben verificar de manera periódica que se aplican aquellos procedimientos o políticas dentro de su área de responsabilidad. | ✓ | | N/A |
| 18.2.3 | ✓ | Se debe revisar el cumplimiento técnico de los sistemas de acuerdo a la política de seguridad y los estándares. | ✓ | | N/A |

# 9. Conclusiones

*Las PYME podrán tener una guía de referencia. Y ahora, ¿qué convendría hacer?*

El desarrollo de este Trabajo Fin de Master ha permitido presentar las dificultades que afronta una PYME a la hora de seleccionar una lista de controles. Existen normas, estándares o guías de buenas prácticas que proporcionan muchos controles para la protección integral de las organizaciones. No obstante, son demasiados. Las PYME con dependencia tecnológica media, no tienen ni el presupuesto ni el conocimiento para aplicarlos y como consecuencia no los implementan a pesar del impacto al que se pueden ver sometidas por comprometer la seguridad de la información que tratan.

Otro factor importante son las regulaciones que son de obligado cumplimiento. En el caso europeo y más concreto el español, está la GDPR y la LOPDP. El trabajo ha permitido establecer una relación entre la lista de controles ISO/IEC 27002:2013 y la GDPR. De esta forma, a la vez que se proporciona una guía para una fácil implantación de controles, se puede cumplir con los objetivos de la regulación.

A lo largo del trabajo se han introducido conceptos fundamentales para la seguridad de la información. En concreto la gestión de riesgos. No se ha entrado en detalle a la hora de realizar el análisis de riesgos puesto que está fuera del alcance de este trabajo pero sí se han definido las estrategias de respuesta ante los riesgos.

Una breve sección ha presentado algunas cifras sobre los ataques informáticos que dejan claro la poca importancia que las PYME suelen dar a la seguridad de la información. Por desgracia, únicamente cuando son atacadas y su negocio se ve directamente afectado. Los ciberseguros para las PYME podrían ser parte de la solución. En cualquier caso no es suficiente. Las organizaciones no se deben limitar a transferir los riesgos sino a intentar mitigar los riesgos desde dentro.

Esta guía proporciona una base para una PYME de cara a aplicar algunos controles de seguridad. El supuesto ficticio podría servir como ejemplo de cara a la implementación de los controles. De todas formas, es importante tener en cuenta que cada organización es distinta y por consiguiente, el supuesto podría utilizarse como referencia.

## 9.1. Trabajo futuro

Este trabajo ha tenido en cuenta la aplicación de los controles ISO/IEC 27002:2013. Ahora bien, es necesario recordar que los estándares se van modificando con el tiempo. Eso implica que este trabajo deberá ser revisado conforme aparezcan nuevas versiones. Es decir, es muy posible que parte de los objetivos de control presentados en la guía y en el supuesto ficticio tengan distinta estructura.

Por otra parte, la guía se ha enfocado en la obligatoriedad de cumplir con la GDPR a partir de mayo de 2018. Esta regulación esta enfocada en Europa. Como trabajo futuro se propone realizar el mismo ejercicio pero teniendo en cuenta aquellas regulaciones que son de obligado cumplimiento más allá de los países que forman parte de la Unión Europea.

# 10. Referencias

## ESTÁNDARES, METODOLOGÍAS, GUÍAS DE BUENAS PRÁCTICAS

[1] **International Organization for Standardization (ISO/IEC 27000 family)**
Familia de estándares que ayudan a las organizaciónes a mantener sus activos de información seguros. La ISO/IEC 27001 es el estándar más conocido en la familia el cual proporciona los requisitos para el diseño de un SGSI.
https://www.iso.org/isoiec-27001-information-security.html

[2] **Control Objectives for Information and related Technology (COBIT)**
Marco de trabajo de negocio para la gobernanza y la gestión empresarial de las TIC. Es el producto de un grupo de trabajo global y de desarrollo de ISACA, asociación sin fines de lucro e independiente.
https://cobitonline.isaca.org/about

[3] **National Institute of Standards and Technology (NIST)**
Agencia de la Administración de Tecnología del Departamento de Comercio de Estados Unidos. Promueve la innovación y la competencia industrial en Estados Unidos.
https://www.nist.gov/

[4] **Project Management Body of Knowledge (PMBoK®)**
PMBoK es la publicación insignia del Project Management Institute (PMI). Es una guía fundamental para la gestión de proyectos. Contiene estándares y normas.
https://www.pmi.org/pmbok-guide-standards/foundational/pmbok/sixth-edition

[5] **MAGERIT**
MAGERIT es la metodología de análisis y gestión de riesgos elaborada por el Consejo Superior de Administración Electrónica que estima que la gestión de los riesgos es una piedra angular en las guías de buen gobierno.
https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html

## REGULACIÓN

[6] **General Data Protection Regulation (GDPR)**
Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos) (Texto pertinente a efectos del EEE).
http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32016R0679

[7] **Directive 95/46/EC**
Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos.
http://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX%3A31995L0046

[8] **Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (LOPDP)**
Ley Orgánica española que tiene por objeto garantizary proteger, en lo que concierne al tratamiento de losdatos personales, las libertades públicas y los derechosfundamentales de las personas físicas, y especialmentede su honor e intimidad personal y familiar.
https://www.boe.es/buscar/doc.php?id=BOE-A-1999-23750

[9] **Real Decreto 1720/2007, de 21 de diciembre**
Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal.
https://www.boe.es/buscar/act.php?id=BOE-A-2008-979

## INSTITUCIONES, ORGANISMOS

[10] **Instituto Nacional de Ciberseguridad (INCIBE)**
Entidad de referencia española para el desarrollo de la ciberseguridad y de la confianza digital de los ciudadanos, la red académica y de investigación española (RedIRIS) y las empresas, especialmente para sectores estratégicos.
https://www.incibe.es/

[11] **Capacidad Respuesta Incidentes de Seguridad de la Información del Centro Criptológico Nacional (CCN-CERT)**
Entidad que gestiona los ciberincidentes que afectan a sistemas del sector público, empresas y organizaciones de interés estratégico en España y a cualquier sistema clasificado.
http://www.ccn-cert.cni.es/

## REFERENCIAS ACADÉMICAS

[12] **Auditoría de certificación ISO 27001**
© FUOC • PID_00239306. Rafael Estevan de Quesada
Universidad Oberta de Catalunya (UOC).

[13] **Análisis de riesgos**
© FUOC • PID_00177810. Daniel Cruz Allende
Universidad Oberta de Catalunya (UOC).

[14] **Desarrollo de algunos objetivos de control deL SGSI**
© FUOC • PID_00177812. Silvia Garre Gui
Universidad Oberta de Catalunya (UOC).

## OTRAS REFERENCIAS

[15] **Beneficios de implantar un SGSI**
Beneficios de implantar un SGSI de acuerdo a la ISO/IEC 27001.ISO Tools Chile, marzo 2016.
http://www.isotools.cl/12-beneficios-de-implantar-un-sgsi-de-acuerdo-a-iso-27001/

[16] **Las PYME y la ciberseguridad**
Cifras sobre ciberseguridad en las PYME. Gestión Pyme, diciembre 2016.
http://gestionpyme.com/pyme-ciberseguridad/

[17] **Aumento del mercado de la ciberseguridad**
Fuerte aumento de la demanda de los ciberseguros tras ataques recientes. La Información, mayo 2017.
https://www.lainformacion.com/economia/aumenta-mercado-ciberseguros-ciberseguridad-ransomware_0_1027098909.html

[18] **El mercado de los ciberseguros por construir**
El mercado de ciberseguros crece de manera exponencial.Community of Insurance, octubre 2016.
http://communityofinsurance.es/blog/2016/10/16/ciberseguros-un-mercado-inmenso-por-construir/

[19] **Ejemplo de contrato de confidencialidad**
Ejemplo de contrato de confidencialidad para empleados, 2016.
https://www.milejemplos.com/contratos/ejemplo-de-contrato-de-confidencialidad-para-empleados.html

# 11. Anexos

## 11.1. Acrónimos

| Acrónimo | Descripción |
|---|---|
| BYOD | Bring Your Own Device (siglas en inglés de "Trae tu propio dispositivo") |
| CAPTCHA | Completely Automated Public Turing test to tell Computers and Humans Apart |
| CCTA | Central Computer and Telecommunications Agency (Reino Unido) |
| CCTV | Circuito Cerrado de Televisión para Vigilancia |
| CE | Comisión Europea |
| CERT | Computer Emergency Response Team |
| CMDB | Configuration Management Database |
| COBIT | Control Objectives for Information and Related Technologies |
| CRAMM | CCTARisk Analysis and Management Method |
| DdA | Declaración de Aplicabilidad |
| ENISA | European Union Agency for Network and Information Security |
| GDPR | General Data Protection Regulation (***nota***:*definición inglesa de RGPD*) |
| IEC | InternationalElectrotechnical Comisión |
| IIP | Información de Identificación Personal |
| ISMS | Information Security Management System (***nota***:*definición inglesa de SGSI*) |
| ISO | International Standards Organization |
| IT | Information Tecnology (***nota***:*definición inglesa de TIC*) |
| LOPDP | Ley Orgánica de Protección de Datos de Carácter Personal |
| MAGERIT | Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información |
| MAP | Ministerio de Administraciones Públicas |
| MVPN | Mobile Virtual Private Network |
| N / A | No aplica |
| NIST | National Institute of Standards & Technology (Estados Unidos) |
| OCTAVE | Operationally Critical Threat, Asset, and Vulnerability Evaluation |
| P2P | Peer to Peer (siglas en inglés de "Punto a Punto") |
| PE | Parlamento Europeo |
| PEC | Prácticas de Evaluación Continua |
| PII | Personally Identifiable Information (***nota***:*definición inglesa de IIP*) |
| PMBoK | Project Management Body of Knowledge |
| PMI | Project Management Institute |

| Acrónimo | Descripción |
|---|---|
| PYME | Pequeña Y Mediana Empresa |
| RGPD | Reglamento General de Protección de Datos |
| SGSI | Sistemas de Gestión de Sistemas de la Información |
| SLA | Service Level Agreement (Acuerdo de Nivel de Servicio) |
| SOA | Statement of Aplicability (***nota****:definición inglesa de DdA*) |
| TFM | Trabajo Fin de Máster |
| TIC | Tecnologías de la Información y las Comunicaciones |
| UE | Unión Europea |
| UOC | Universidad Oberta de Catalunya |
| VPN | Virtual Private Network |

## 11.2. REF-05-01.1 – Política de seguridad

**NOTA**: se muestra una versión preliminar de la política de seguridad de *Ibones de Aragón S.L.* a modo de ejemplo. Según lo expuesto, será revisada una vez al año.

| **POLÍTICA DE SEGURIDAD DE *IBONES DE ARAGÓN S.L.*** |
|---|
| **Introducción** |
| La compañía ha experimentado un crecimiento notable desde su fundación en 2015. Hemos conseguido ser una referencia de mercado en productos de montaña. Los clientes confían en nosotros. Por lo tanto, nosotros tenemos el deber de proporcionar la seguridad con la que gestionamos su información.<br>Este documento presenta la política de seguridad de la información que debe ser implantada en toda la organización. Dispone del total soporte de la dirección y toda la compañía está obligada a seguir los preceptos que aquí se presentan incluyendo terceras partes con las que se tenga relación en el ejercicio de las actividades de *Ibones de Aragón S.L.*<br>La política será revisada una vez al año para confirmar que la confidencialidad, integridad y disponibilidad de la información no se vea afectada. Esta política permitirá el cumplimiento con las regulaciones actuales a las que se ve sujeta la compañía. En concreto la General Data Protection Regulation (GDPR). |
| **Del derecho del cliente** |
| • Se debe garantizar la confidencialidad de la información en todo momento.<br>• La información personal almacenada tendrá un carácter temporal. En todo momento, la persona a la cual se realice un tratamiento de los datos, tendrá el derecho de rectificación, supresión o limitación de tratamiento de los datos. |
| **Del uso de las aplicaciones** |
| • No se permite el uso de aplicaciones que no dispongan de licencia.<br>• El borrado de aplicaciones software sólo lo podrá realizar el administrador de sistemas o en su defecto el responsable tecnológico.<br>• No se permite la instalación de programas software sin la previa autorización del responsable. El administrador de los sistemas es el encargado de la instalación.<br>• En caso de instalación de software con licencia pública, siempre se tendrán en cuenta los derechos de propiedad intelectual.<br>• Se restringe el acceso a redes sociales, aplicaciones de almacenamiento en la "nube" y aplicaciones de intercambio de ficheros "Punto a Punto".<br>• La Dirección exigirá el uso de software propietario o, en su defecto, utilización de software de licencia pública adquirido en lugares seguros cuyas páginas web sean oficiales.<br>• Es obligatorio realizar las actualizaciones de software que se reciban de forma automática.<br>• Todos los datos informáticos deberán tener una copia de seguridad que se realizará de forma diaria incremental. |
| **Del desarrollo software** |
| • Todos los desarrollos software deben considerar requisitos de seguridad desde el inicio de los proyectos.<br>• Los datos que se utilicen para realizar pruebas deben ser son siempre simulados para evitar utilizar datos sensibles que identifiquen a la persona. |
| **Del uso de los equipos** |
| • No se permite inactivar los sistemas de seguridad de los equipos corporativos que se utilizan en la |

**POLÍTICA DE SEGURIDAD DE *IBONES DE ARAGÓN S.L.***

organización (p.ej. antivirus).

- Es obligatorio que todos los equipos informáticos dispongan de antivirus actualizados.
- No se permite sacar aquellos recursos informáticos de la compañía sin previa autorización del responsable tecnológico o director general.
- Todos los recursos informaticos a disposición del personal deberán ser utilizados exclusivamente para las actividades inherentes al negocio de la compañía.
- Se deberán utilizar candados de seguridad en aquellos equipos portátiles que la compañía ha puesto a disposición del empleado.
- No se permite la utilización de equipos personales en la compañía para el desempeño de las actividades de negocio.
- No se permite utilizar los equipos portátiles de la compañía fuera de las instalaciones.
- Se deberán bloquear los ordernadores de sobremesa o portátiles cuando no se utilicen o bien pasada 1 hora de inactividad. Se desbloquearán mediante el usuario y contraseña del empleado.

**Del acceso**

- El administrador de sistemas es el encargado de proporcionar los accesos a los recursos informáticos.
- Se realizará un control de las personas que accedan a las instalaciones sin excepción.
- Todas las personas dispondrán de una tarjeta identificativa que permitirá el acceso a determinadas áreas de las instalaciones.
- Los empleados tendrán acceso a aquellas aplicaciones corporativas a las que hayan sido específicamente autorizados por los responsables de área o el director general.
- Las contraseñas deberán tener un mínimo de 8 caracteres incluyendo letras, números, mayúsculas, minúsculas y signos especiales.
- Las contraseñas deben ser difíciles de adivinar. Se pueden utilizar reglas nemotécnicas para evitar que se olviden.
- Se ofrecerá una contraseña inicial al crear el usuario. Una vez se acceda por primera vez a los sistemas corporativos, el usuario deberá cambiar esta contraseña.
- Las contraseñas se deberán cambiar una vez cada 3 meses.
- Las contraseñas no deben guardarse en papeles fácilmente accesibles como post-it, no almacenarse en ficheros no encriptados, etc.
- Los usuarios no deben distribuir la información de su autenticación ni siquiera a sus responsables. Debe considerarse como información personal.
- El administrador de sistemas puede crear listas de distribución siempre que haya recibido la aprobación del responsable tecnológico o del director general.
- El control de acceso al código fuente del software sólo está disponible para los empleados directamente relacionados con el desarrollo.

**De la comunicación y conexión al exterior**

- Toda comunicación deberá realizarse de forma encriptada para evitar su manipulación.
- Cada empleado dispondrá de un correo corporativo que unicamente podrá ser utilizado para aquellos fines profesionales relacionados con las actividades de la compañía y no para uso privado.
- La conexión a Internet se realizará siempre a través de la red corporativa. Se dispone de WiFi para invitados con limitado acceso a ciertas aplicaciones.
- Siempre se debe realizar una conexión exterior a través del proxy.

## POLÍTICA DE SEGURIDAD DE *IBONES DE ARAGÓN S.L.*

**De los incidentes**

- En caso de producirse cualquier tipo de incidencia, es obligatorio notificar al responsable tecnológico y al administrador de los sistemas.
- Los incidentes deben ser siempre clasificados y registrados como evidencia.
- Los incidentes deben ser tratados como lecciones aprendidas.
- Se deben notificar aquellas debilidades encontradas en el sistema como medida de prevención de posibles incidentes.

**De la clasificación de la información**

- Cada uno de los activos de la compañía dispondrá de un responsable. Por lo tanto, será el encargado de realizar un buen uso de los mismos.
- Aquellos documentos que la compañía emita o reciba deberán ser clasificados como *uso interno* (sólo accesibles al personal), *públicos* (podrán ser accesibles por todo el mundo) y *confidenciales* (únicamente accesibles por la Dirección.

**De la gestión de los dispositivos móviles**

- Todos los dispositivos móviles que contienen información sensible (p.ej. pendrives o HDD externos), deben ser almacenados en armarios con llave si no se utilizan en ese momento.
- Aquellos dispositivos móviles que contengan información sensible y dejen de ser útiles para la organización deberán ser completamente destruidos. Previamente se deberá realizar un registro de la información que contienen.
- Todos los dispositivos móviles deberán utilizar criptografía para almacenar información sensible.

**De la propiedad intelectual**

- Todos los desarrollos informáticos creados en la compañía formarán parte de los activos de la misma la cual dispondrá de los derechos de propiedad intelectual.

**De la formación**

- El personal deberá participar en aquellos cursos de seguridad de la información que se realizaran de forma periódica.

**De las auditorias**

- La Dirección establecerá un programa de auditoria con el fin de, como mínimo, llevar a cabo una auditoria al año sea interna o externa.

**De la política de "escritorio y pantallas limpios"**

- Los escritorios deben estar limpios de forma que no haya documentos con información sensible encima de la mesa a no ser que sean estrictamente necesarios para el desarrollo de las actividades de negocio.

**De las sanciones por incumplimiento**

- En caso de incumplimiento de esta política de seguridad, el personal se verá sujeto a sanciones según lo dispuesto en la normativa del departamento de RR.HH.

## 11.3. REF-06-01.1 – Roles y responsabilidades

**NOTA**: se muestra a modo de ejemplo la lista de roles y responsabilidades del Responsable Tecnológico. Se debería realizar el mismo ejercicio para el resto de personal de la compañía.

| **Responsable Tecnológico** | |
|---|---|
| Jefe Inmediato | Director General |
| Roles | • Administración TIC<br>• Desarrollo<br>• Diseño |
| Responsabilidades | • Verificar el uso adecuado de los recursos informáticos de Ibones de Aragón S.L.<br>• Realizar inventariado de los activos corporativos.<br>• Asegurar la Confidencialidad, Integridad y Disponibilidad de la información.<br>• Implementar mejoras de los procesos TIC y colaborar en la mejora continua de otros procesos de la compañía.<br>• Gestionar las acciones correctivas y preventivas.<br>• Gestionar el equipo de desarrollo de software.<br>• Participar en el programa de capacitación y de seguridad TIC de la compañía.<br>• Dirigir las actividades de Seguridad de la Información.<br>• Validar la adquisición de software de la compañía. |

## 11.4. REF-06-01.3 – Lista de contactos

**NOTA**: se muestra a modo de ejemplo parte de la lista de contactos con las autoridades que tendría la compañía.

| **Agencia Española de Protección de Datos** | |
|---|---|
| Descripción | Autoridad pública independiente española encargada de velar por la privacidad y la protección de datos de los ciudadanos. |
| URL | https://www.agpd.es/portalwebAGPD/index-ides-idphp.php |
| **CCN-CERT** | |
| Descripción | El CCN-CERT es la Capacidad de Respuesta a incidentes de Seguridad de la Información del Centro Criptológico Nacional español, CCN, adscrito al Centro Nacional de Inteligencia, CNI. |
| URL | https://www.ccn-cert.cni.es/ |
| **Cuerpo Nacional de Policía** | |
| Descripción | Instituto armado de naturaleza civil español, con estructura jerarquizada que tiene como misión proteger el libre ejercicio de los derechos y libertades y garantizar la seguridad ciudadana, con ámbito de actuación en todo el territorio nacional. |
| URL | https://www.policia.es/ |
| **ENISA** | |
| Descripción | La European Union Agency for Network and Information Security (ENISA) es un centro de conocimiento para la ciberseguridad en Europa. |
| URL | https://www.enisa.europa.eu/ |
| **Protección Civil** | |
| Descripción | Dirección General de Protección Civil y Emergencias de España. |
| URL | http://www.proteccioncivil.es/ |

## 11.5. REF-07-01.2 – Acuerdo de confidencialidad y no divulgación

**NOTA**: se muestra a modo de ejemplo una plantilla de acuerdo de confidencialidad y no divulgación para el trabajador [19]. Un acuerdo de naturaleza similar se debería crear para terceras partes (p.ej. proveedores).

**ACUERDO DE CONFIDENCIALIDAD Y NO DIVULGACIÓN DE *IBONES DE ARAGÓN S.L.***

**Primero.– OBJETO**

En virtud de la prestación de servicios de carácter laboral que <EL TRABAJADOR> efectuará para *Ibones de Aragón S.L.*, <EL TRABAJADOR> puede tener acceso a instalaciones, dependencias, recursos, sistemas, documentos en soporte papel, documentos electrónicos, soportes informáticos, electrónicos y telemáticos susceptibles de contener información considerada confidencial titularidad tanto de *Ibones de Aragón S.L.* como de otros terceros vinculados a ella a través de distintas relaciones jurídicas.

Es por ello que de acuerdo con el artículo 5 del Real Decreto Legislativo 1/1995, de 24 de marzo, por el que se aprueba el texto refundido de la Ley del Estatuto de los Trabajadores <EL TRABAJADOR> viene obligado expresamente a cumplir con las obligaciones concretas de su puesto de trabajo, de conformidad a las reglas de la buena fe y diligencia. En virtud de lo anterior, <EL TRABAJADOR> declara mediante el presente documento que asume su compromiso de cumplir y respetar el deber de secreto y sigilo profesional respecto de cualquier información confidencial que pueda conocer con motivo de la prestación de servicios y ejecución de su contrato laboral.

A efectos de lo anterior *Ibones de Aragón S.L.* pone en conocimiento de <EL TRABAJADOR> que por "información confidencial" se entenderá toda aquella información, incluyendo datos de carácter personal relativos a personas físicas, que en cualquier momento (pasado, presente y/o futuro) y con ocasión de los servicios prestados por <EL TRABAJADOR>, *Ibones de Aragón S.L.* facilite, entregue o, de cualquier forma (verbal, escrita, visual u otras), y bajo cualquier tipo de soporte o canal (papel, electrónico, telemático, soportes informáticos, mensajes de correo electrónico u otros documentos o soportes), ponga a disposición de <EL TRABAJADOR> y que, en general, y en los más amplios términos, concierna, afecte o se refiera directa, indirecta, mediata o inmediatamente, ya a *Ibones de Aragón S.L.*, ya a los terceros (personas físicas o jurídicas) con quienes se mantenga cualquier tipo de vinculación, o, sin mantenerla actualmente, pueda existir ésta en un futuro.

**Segundo.– OBLIGACIONES**

En cumplimiento del objeto del presente documento, <EL TRABAJADOR> se compromete a mantener bajo el más estricto secreto profesional toda la información confidencial que pueda llegar a su conocimiento como consecuencia del desempeño de sus funciones, comprometiéndose el trabajador a no divulgarla, publicarla, cederla, revelarla ni de otra forma, directa o indirecta, ponerla a disposición de terceros, ni total ni parcialmente, y a cumplir esta obligación incluso con sus propios familiares u otros miembros de *Ibones de Aragón S.L.* que no estén autorizados a acceder a la citada información, en su encargo profesional o por razón del puesto que ocupan.

Asimismo, declara conocer y se compromete a respetar y cumplir la normativa y medidas de seguridad implementadas por *Ibones de Aragón S.L.* a fin de garantizar la seguridad y protección de la información confidencial.

**Tercero.– VIGENCIA DEL DEBER DE SIGILO PROFESIONAL**

<EL TRABAJADOR> garantiza que, tras la terminación de la relación laboral cualquiera que sea su causa,

## ACUERDO DE CONFIDENCIALIDAD Y NO DIVULGACIÓN DE *IBONES DE ARAGÓN S.L.*

mantendrá vigente su deber de sigilo y secreto profesional respecto de la información confidencial a que haya tenido acceso durante el desempeño de sus funciones durante la vigencia de la relación laboral y devolverá inmediatamente a Ibones de Aragón S.L. cualquier soporte o documento en el que conste información confidencial que por cualquier causa obrare en su poder, o la destruirá siguiendo los procedimientos de seguridad para el borrado de información establecidos por Ibones de Aragón S.L.

### Cuarto.– SANCIONES

<EL TRABAJADOR> declara conocer que las faltas por los trabajadores al servicio de Ibones de Aragón S.L. reguladas en este compromiso de confidencialidad, se clasificarán atendiendo a su importancia, reincidencia e intención, en leves, graves y muy graves, de conformidad con lo dispuesto en el Convenio Colectivo de aplicación y en las normas vigentes del ordenamiento jurídico laboral. En consecuencia, las sanciones que Ibones de Aragón S.L. podrá aplicar, según la gravedad y circunstancias de las faltas cometidas, serán las establecidas en la Legislación citada.

### Quinto.– PROTECCIÓN DE DATOS

De conformidad con la Ley 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (en adelante LOPD), Ibones de Aragón S.L. con domicilio social en _____ (indicar) informa a <EL TRABAJADOR> de que los datos de carácter personal derivados de la suscripción de este documento así como los generados en virtud del objeto del mismo serán tratados con la finalidad de llevar a cabo un control de cumplimiento de su compromiso de confidencialidad respecto de toda la información reservada y confidencial que reciba durante la ejecución de la relación laboral. Dicho tratamiento tiene carácter obligatorio y resulta imprescindible a los fines indicados. Asimismo Ibones de Aragón S.L. informa al TRABAJADOR de que en cualquier momento puede ejercitar los derechos de acceso, rectificación, cancelación y oposición dirigiéndose por escrito a la siguiente dirección _____ (o indicar otros medios establecidos por la organización de acuerdo con las posibilidades determinadas en la LOPD y su Reglamento de desarrollo).

Declaro el entendimiento del presente documento, manifiesto mi conformidad con su contenido y acepto el cumplimiento de todas las normas que en el mismo se proponen y/o adjuntan, en _____a _____ de _____de _____.

Firmado por <EL TRABAJADOR>

Don/Dña _____

## 11.6. REF-07-02.2 – Calendario de cursos de seguridad

**NOTA**: se muestra a modo de ejemplo un calendario de cursos de seguridad obligatorios a realizar por todos los empleados.

| Fecha | Tipo | Lugar | Descripción | Duración |
|---|---|---|---|---|
| (dd) Marzo (aaaa) | Presencial | xxxx , Zaragoza | Concienciación sobre la seguridad | 1 hora |
| (dd) Marzo (aaaa) | Webinar | Online | Protección de Datos | 1 hora |
| (dd) Marzo (aaaa) | Webinar | Online | Código ético | 30 minutos |
| (dd) Marzo (aaaa) | Presencial | xxxx , Zaragoza | Relación con el cliente y proveedor | 2 horas |
| (dd) Junio (aaaa) | Webinar | Online | Protección de Datos | 1 hora |
| (dd) Junio (aaaa) | Webinar | Online | Código ético | 30 minutos |
| (dd) Junio (aaaa) | Presencial | xxxx , Zaragoza | Relación con el cliente y proveedor | 2 horas |
| (dd) Junio (aaaa) | Presencial | xxxx , Zaragoza | Concienciación sobre la seguridad | 1 hora |
| (dd) Octubre (aaaa) | Webinar | Online | Protección de Datos | 1 hora |
| (dd) Octubre (aaaa) | Webinar | Online | Código ético | 30 minutos |
| (dd) Octubre (aaaa) | Presencial | xxxx , Zaragoza | Concienciación sobre la seguridad | 1 hora |
| (dd) Diciembre (aaaa) | Presencial | xxxx , Zaragoza | Relación con el cliente y proveedor | 2 horas |

## 11.7. REF-08-02.1 – Clasificación de la información

**NOTA**: se muestra a modo de ejemplo una clasificación de la información para la documentación.

| Nivel | Descripción |
|---|---|
| Confidencial | Sólo disponible para la Dirección y los Responsables de Área |
| Uso Interno | Información de uso interno. Sólo disponible para empleados |
| Público | Accesible a todo el público |

## 11.8. REF-11-01.2 – Acceso a las instalaciones

**NOTA**: se muestra a modo de ejemplo una tarjeta de acceso a las instalaciones y un registro de acceso que será mantenido por la secretaria.

La tarjeta permite acceder a ciertas áreas de las instalaciones. Por ejemplo, para poder entrar en las oficinas o en la zona de servidores. Existen dispositivos de lectura de tarjetas justo en la entrada de las oficinas o al lado de la puerta de la zona de servidores. Dependiendo de los roles de las personas, se permitirá o no el acceso.

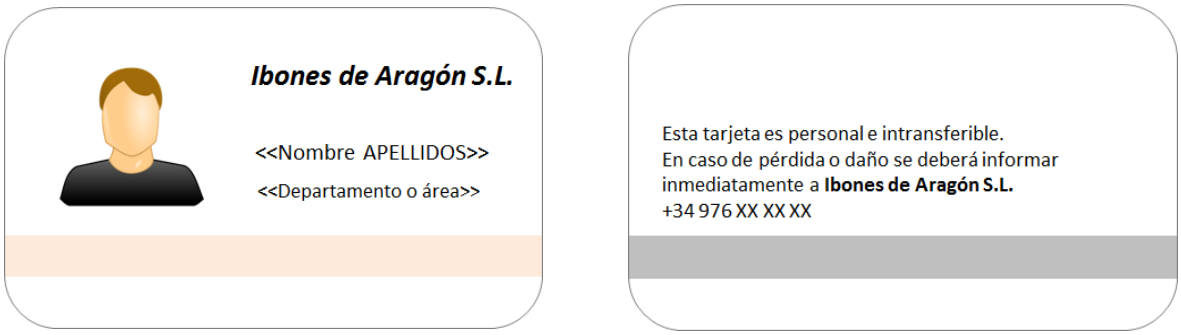



*Imagen 14 – Ejemplo de tarjeta de acceso*

El registro de acceso será gestionado por la secretaria en la entrada a las oficinas. Recogerá cierta información de aquellos visitantes que no sean empleados de la compañía y, por lo tanto, no disponen de tarjetas identificativas de acceso.

| Fecha | Entrada | Salida | Nombre | Contacto | Motivo visita | Firma |
|---|---|---|---|---|---|---|
| dd/mm/aaaa | hh:mm | hh:mm | | | | |
| dd/mm/aaaa | hh:mm | hh:mm | | | | |
| dd/mm/aaaa | hh:mm | hh:mm | | | | |
| dd/mm/aaaa | hh:mm | hh:mm | | | | |

## 11.9. Lista de controles ISO/IEC 27002:2013

| ISO IEC 27002:2013 |
|---|
| **5 Políticas de seguridad de la información** |
| **5.1 Dirección de gestión para la seguridad de la información** |
| 5.1.1 Políticas para la seguridad de la información |
| 5.1.2 Revisión de las políticas para seguridad de la información |
| **6 Organización de la seguridad de la información** |
| **6.1 Organización interna** |
| 6.1.1 Roles y responsabilidades para la seguridad de información |
| 6.1.2 Separación de deberes |
| 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 móviles y teletrabajo** |
| 6.2.1 Política para dispositivos móviles |
| 6.2.2 Teletrabajo |
| **7 Seguridad de los recursos humanos** |
| **7.1 Previo al empleo** |
| 7.1.1 Selección |
| 7.1.2 Términos y condiciones del empleo |
| **7.2 Durante el empleo** |
| 7.2.1 Responsabilidades de la dirección |
| 7.2.2 Toma de conciencia, educación y formación en la seguridad de la información |
| 7.2.3 Proceso disciplinario |
| **7.3 Terminación o cambio de empleo** |
| 7.3.1 Terminación o cambio de responsabilidades de empleo |
| **8 Gestión de activos** |
| **8.1 Responsabilidad por 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 Clasificación de la información |
| 8.2.2 Etiquetado de la información |
| 8.2.3 Manejo de activos |
| **8.3 Manipulación de media** |
| 8.3.1 Gestión de medios removibles |
| 8.3.2 Eliminación de los medios |
| 8.3.3 Transferencia de medios físicos |
| **9 Control de acceso** |
| **9.1 Requisitos de negocio para el control de acceso** |
| 9.1.1 Política de control de acceso |
| 9.1.2 Política sobre el uso de los servicios de red |
| **9.2 Gestión de acceso de usuarios** |
| 9.2.1 Registro y cancelación del registro de usuarios |

| ISO IEC 27002:2013 |
|---|
| 9.2.2 Suministro de acceso de usuarios |
| 9.2.3 Gestión de derechos de acceso privilegiado |
| 9.2.4 Gestión de información de autenticación secreta de usuarios |
| 9.2.5 Revisión de los derechos de acceso de usuarios |
| 9.2.6 Retiro o ajuste de los derechos de acceso |
| **9.3 Responsabilidades de los usuarios** |
| 9.3.1 Uso de la información de autenticación secreta |
| **9.4 Control de acceso a sistemas y aplicaciones** |
| 9.4.1 Restricción de acceso Información |
| 9.4.2 Procedimiento de ingreso seguro |
| 9.4.3 Sistema de gestión de contraseñas |
| 9.4.4 Uso de programas utilitarios privilegiados |
| 9.4.5 Control de acceso a códigos fuente de programas |
| **10 Criptografía** |
| **10.1 Controles criptográficos** |
| 10.1.1 Política sobre el uso de controles criptográficos |
| 10.1.2 Gestión de claves |
| **11 Seguridad física y del entorno** |
| **11.1 Áreas seguras** |
| 11.1.1 Perímetro de seguridad física |
| 11.1.2 Controles físicos de entrada |
| 11.1.3 Seguridad de oficinas, recintos e instalaciones |
| 11.1.4 Protección contra amenazas externas y ambientales |
| 11.1.5 Trabajo en áreas seguras |
| 11.1.6 Áreas de carga y descarga |
| **11.2 Equipos** |
| 11.2.1 Ubicación y protección de los equipos |
| 11.2.2 Servicios de suministro |
| 11.2.3 Seguridad del cableado |
| 11.2.4 Mantenimiento de equipos |
| 11.2.5 Retirada de activos |
| 11.2.6 Seguridad de equipos y activos fuera de las instalaciones |
| 11.2.7 Eliminación segura o reutilización de equipos |
| 11.2.8 Equipos de usuario desatendidos |
| 11.2.9 Política de escritorio limpio y pantalla limpia |
| **12 Seguridad de las operaciones** |
| **12.1 Procedimientos operacionales y responsabilidades** |
| 12.1.1 Procedimientos operacionales documentados |
| 12.1.2 Gestión de cambios |
| 12.1.3 Gestión de capacidad |
| 12.1.4 Separación de los ambientes de desarrollo, pruebas y operación |
| **12.2 Protección contra códigos maliciosos** |
| 12.2.1 Controles contra códigos maliciosos |
| **12.3 Copias de respaldo** |
| 12.3.1 Respaldo de información |
| **12.4 Registro y monitorización** |
| 12.4.1 Registro de eventos |
| 12.4.2 Protección de la información de registro |

| ISO IEC 27002:2013 |
|---|
| 12.4.3 Registros del administrador y del operador |
| 12.4.4 Sincronización de relojes |
| **12.5 Control de software operacional** |
| 12.5.1 Instalación de software en sistemas operativos |
| **12.6 Gestión de la vulnerabilidad técnica** |
| 12.6.1 Gestión de las vulnerabilidades técnicas |
| 12.6.2 Restricciones sobre la instalación de software |
| **12.7 Consideraciones sobre auditorias de sistemas de información** |
| 12.7.1 Información controles de auditoría de sistemas |
| **13 Seguridad de las comunicaciones** |
| **13.1 Gestión de seguridad de las redes** |
| 13.1.1 Controles de redes |
| 13.1.2 Seguridad de los servicios de red |
| 13.1.3 Separación en las redes |
| **13.2 Transferencia de información** |
| 13.2.1 Políticas y procedimientos de transferencia de información |
| 13.2.2 Acuerdos sobre transferencia de información |
| 13.2.3 Mensajería electrónica |
| 13.2.4 Acuerdos de confidencialidad o de no divulgación |
| **14 Adquisición, desarrollo y mantenimientos de sistemas** |
| **14.1 Requisitos de seguridad de los sistemas de información** |
| 14.1.1 Análisis y especificación de requisitos de seguridad de la información |
| 14.1.2 Seguridad de servicios de las aplicaciones en redes publicas |
| 14.1.3 Protección de transacciones de los servicios de las aplicaciones |
| **14.2 Seguridad en los procesos de desarrollo y soporte** |
| 14.2.1 Política de desarrollo seguro |
| 14.2.2 Procedimientos de control de cambios en sistemas |
| 14.2.3 Revisión técnica de las aplicaciones después de cambios en la plataforma de operación |
| 14.2.4 Restricciones en los cambios a los paquetes de software |
| 14.2.5 Principios de construcción de sistemas seguros |
| 14.2.6 Entorno de desarrollo seguro |
| 14.2.7 Desarrollo contratado externamente |
| 14.2.8 Pruebas de seguridad de sistemas |
| 14.2.9 Prueba de aceptación de sistemas |
| **14.3 Datos de prueba** |
| 14.3.1 Protección de datos de prueba |
| **15 Relación con los proveedores** |
| **15.1 Seguridad de la información en las relaciones con los proveedores** |
| 15.1.1 Política de seguridad de la información para las relaciones con proveedores |
| 15.1.2 Tratamiento de la seguridad dentro de los acuerdos con proveedores |
| 15.1.3 Cadena de suministro de tecnología de información y comunicación |
| **15.2 Gestión de la prestación de servicios con los proveedores** |
| 15.2.1 Seguimiento y revisión de los servicios de los proveedores |
| 15.2.2 Gestión de cambios en los servicios de proveedores |
| **16 Gestión de incidentes de seguridad de la información** |
| **16.1 Gestión de incidentes y mejoras de seguridad de la información** |
| 16.1.1 Responsabilidad y procedimientos |
| 16.1.2 Reporte de eventos de seguridad de la información |

| ISO IEC 27002:2013 |
|---|
| 16.1.3 Reporte de debilidades de seguridad de la información |
| 16.1.4 Evaluación de eventos de seguridad de la información y decisiones sobre ellos |
| 16.1.5 Respuesta a incidentes de seguridad de la información |
| 16.1.6 Aprendizaje obtenido de los incidentes de seguridad de la información |
| 16.1.7 Recolección de evidencia |
| **17 Aspectos de seguridad de la información de la gestión de continuidad de negocio** |
| **17.1 Continuidad de seguridad de la información** |
| 17.1.1 Planificación de la continuidad de la seguridad de la información |
| 17.1.2 Implementación 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 de procesamiento de información |
| **18 Cumplimiento** |
| **18.1 Cumplimiento con los requisitos legales y contractuales** |
| 18.1.1 Identificación de la legislación aplicable y de los requisitos contractuales |
| 18.1.2 Derechos de propiedad intelectual |
| 18.1.3 Protección de registros |
| 18.1.4 Privacidad y protección de datos personales |
| 18.1.5 Reglamentación de controles criptográficos |
| **18.2 Revisiones de seguridad de la información** |
| 18.2.1 Revisión independiente de la seguridad de la información |
| 18.2.2 Cumplimiento con las políticas y normas de seguridad |
| 18.2.3 Revisión del cumplimiento técnico |

*Tabla 5 – Lista de controles ISO/IEC 27002:2013*