UNIVERSITAT POLITÈCNICA DE VALÈNCIA

etsinf
Escola Tècnica Superior d'Enginyeria Informàtica

Escola Tècnica Superior d'Enginyeria Informàtica
Universitat Politècnica de València

EL PAPEL DEL INFORMÁTICO COMO AUDITOR EN LA "ISO 27001:2017 TECNOLOGÍA DE LA INFORMACIÓN. TÉCNICAS DE SEGURIDAD. SISTEMAS DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN. REQUISITOS."

Trabajo Fin de Grado

Grado en Ingeniería Informática

Autor: Jorge Asensi Shaw

Tutor: Mariluz Gordo Monzó

Curso 2018/2019

Resumen

La tecnología avanza a una velocidad vertiginosa y con ello el manejo de la información que es un valor primordial para las empresas. La información se encuentra sometida continuamente a amenazas, por tanto, garantizar su seguridad y protegerla es una necesidad de la sociedad. Para ello es necesario contar con profesionales en el sector que actualmente escasean con respecto a la enorme demanda existente. Según los datos de *"Global Information Cibersecurity Workforce Study"* se prevé que en el año 2022 habrán 1,5 millones de puestos vacantes de ciberseguridad en todo el mundo. Con el objetivo de ayudar a cubrir esta necesidad, se ha elaborado una guía de aproximación que recoge los conocimientos necesarios para ayudar a que nuevos titulados de informática o interesados en la materia, se orienten hacia el sector de la auditoría de sistemas de gestión de la seguridad de la información abarcando los conocimientos de la norma ISO/IEC 27001:2017, la auditoría, su proceso, la certificación y como formarse, entre otros. Para llevar a cabo este trabajo, se ha realizado una profunda lectura y síntesis de todos los conceptos necesarios, accediendo tanto a libros, artículos como trabajos realizados sobre esta temática.

Palabras clave: ISO 27001:2017, auditor, auditoría, certificación, sistemas de gestión de la seguridad de la información, informática.

Resum

La tecnologia avança a una velocitat vertiginosa i amb això el maneig de la informació que és un valor primordial per a les empreses. La informació es troba sotmesa contínuament a amenaces, per tant, garantir la seua seguretat i protegir-la és una necessitat de la societat. Per a això és necessari comptar amb professionals en el sector que actualment escassegen respecte a l'enorme demanda existent. Segons les dades de "Global Information Cibersecurity Workforce Study" es preveu que l'any 2022 hauran 1,5 milions de llocs vacants de ciberseguretat a tot el món. Amb l'objectiu d'ajudar a cobrir aquesta necessitat, s'ha elaborat una guia d'aproximació que recull els coneixements necessaris per a ajudar al fet que nous titulats d'informàtica o interessats s'orienten pel sector de l'auditoria de sistemes de gestió de la seguretat de la información, abastant els coneixements de la norma ISO/IEC 27001:2017, l'auditoria, el seu procés, la certificació i com formar-se, entre altres. Per a dur a terme aquest treball, s'ha realitzat una profunda lectura i síntesi de tots els conceptes necessaris, accedint tant a llibres, articles com a treballs realitzats sobre aquesta temàtica.

Paraules clau: ISO 27001:2017, auditor, auditoria, certificació, sistemes de gestió de la seguretat de la informació, informàtica.

Abstract

The technology advances at a dizzying speed and with it the handling of the information that is a primordial value for the companies. Information is constantly under threat, so ensuring its security and protecting it is a necessity for society. To do this, it is necessary to have professionals in the sector who are currently scarce in relation to the enormous demand that exists. According to the "Global Information Cybersecurity Workforce Study, 1.5 million cybersecurity positions are expected to be vacant worldwide by 2022. With the aim of helping to cover this need, an approximation guide has been realized that collects the necessary knowledge to help new computing graduates or interested parties be guided by the sector of the audit of information security management systems, covering knowledge of ISO/IEC 27001:2017, auditing, its process, certification and how to train, among others. In order to carry out this work, a deep reading and synthesis of all necessary concepts has been carried out, accesing books, articles as well as works carried out on this subject.

Key words : ISO 27001:2017, auditor, audit, certification, information security manaement systems, computing.

Tabla de contenidos

Contenido

1. Introducción

El mundo está globalmente conectado, se encuentra en la llamada era de la información o era digital. El mayor valor que tienen las empresas o su mayor poder es la información. Como dice Julien Mur senior manager del departamento "*Information Technology and Life Sciences"* de la consultora de recursos humanos *"Hays" "Los países ricos ya no van a producir bienes de consumo, sino que generarán riqueza a través de la información. Cualquier empresa tiene que gestionar sus datos, almacenarlos y sobre todo protegerlos"*. Actualmente, las empresas están constantemente analizando y gestionando información, debido a los grandes avances tecnológicos éste gran valor ya no se almacena en archivadores de papel, sino que se almacenan en dispositivos tales como: pendrives, discos duros o la propia *"nube"*.

Las distintas empresas gestionan una gran cantidad de información, ya sean datos sobre sus cuentas, sobre sus trabajadores, sus clientes, etc. Estos datos, están continuamente sometidos a amenazas, por tanto es de vital importancia que se garantice su seguridad y su correcta gestión. Para hacer frente a estas amenazas se deben establecer una serie de protocolos o políticas de seguridad, que son distintas dependiendo de las necesidades de la empresa.

Las normas ISO son un conjunto de normas de gestión para las empresas, establecidas por el Organismo Internacional de Estandarización (ISO), a diferencia de las leyes estas normas no son obligatorias.

Existen varias normas, la que rige cómo gestionar e implantar correctamente un sistema de gestión de la seguridad de la información **es la norma ISO 27001:2017**. Este sistema de gestión permite a las empresas manejar correctamente la información y mantenerla segura frente a las amenazas.

¿Cómo pueden saber las empresas si sus datos están seguros o si sus protocolos de seguridad son correctos? o ¿Cómo garantizar a los clientes que sus datos están seguros y pueden confiar en dicha empresa? La respuesta a estas preguntas se consigue una vez implantada la norma ISO 27001:2017 en la empresa a través de la "evaluación" de un equipo auditor durante el proceso denominado auditoría. Si el resultado es favorable, es decir, cumple los requisitos de la norma, la empresa auditada obtendrá el certificado que acredita el cumplimiento de la norma ISO 27001:2017 *"Tecnologías de la información Técnicas de Seguridad Sistemas de Gestión de la Seguridad de la Información"*.

1.1 Motivación

Una de las cuestiones más importantes que un estudiante se pregunta finalizando la carrera es: "¿Qué trabajo de fin de grado (TFG) se va a realizar?" Este tiene que venir motivado por las inquietudes durante todo el proceso de aprendizaje de la carrera así como por los intereses futuros hacia los que se quiere derivar los estudios realizados. La temática de la seguridad de la información es un aspecto de rigurosa actualidad que va evolucionando conforme avanza la tecnología, por ello es de vital importancia concienciar a la sociedad de la trascendencia que tiene hoy en día asegurar la información y su manejo, y que mejor que aplicando la norma ISO 27001:2017.

La realización de este proyecto va a permitir conocer en profundidad la norma ISO 27001:2017, en que consiste el trabajo del auditor de sistemas de gestión de la seguridad de la información, qué aptitudes ha de tener, las pautas a seguir para realizar una auditoría, en qué casos se concede la certificación… Por tanto, tras la consecución de este trabajo de fin de grado se obtendrán las aptitudes extra que a todo interesado en este campo puede resultarle de gran interés

La información con la que trabajan las empresas, tal y como se ha indicado, tiene una gran trascendencia en el mundo laboral y por lo tanto, es un requisito imprescindible afianzar su seguridad. Los informáticos tienen la oportunidad de concienciar a las empresas y ayudarles a implantar y conocer esta norma, para que vean la ISO 27001, no como una norma, si no como una "ley" , es decir, como una obligación que toda empresa tiene que cumplir hoy en día a la hora de asegurar los datos y la información.

En conclusión, tras la culminación de este trabajo, se espera incitar a muchos informáticos a entrar en este apasionante campo y ayudar a los interesados a tomar conciencia del valor de la información a tratar así como de la envergadura que tiene mantener su seguridad a corto y medio plazo en los tiempos actuales y futuros.

1.2 Objetivos

Se plantean dos objetivos fundamentales:

Conocer en profundidad esta norma, su metodología y su aplicación a las distintas empresas, además del papel del informático como auditor de sistemas de gestión de la seguridad de la información.

Elaborar una guía de aproximación para un informático que desee ejercer como auditor de sistemas de gestión de seguridad de la información que incluya la siguiente información:

- Norma ISO 27001
  Detallar la norma, sus componentes y su gran trascendencia actualmente,

- Profundizar en el concepto de auditoría
  Explicar qué es la auditoria y un auditor, especificando el perfil del auditor de sistemas de gestión de la seguridad de la información.

- La correcta metodología que se debe realizar durante el proceso de auditaría
  Principalmente explicar de una manera clara y concisa como se audita.

- Herramientas de auditoría
  Cuales son y su utilidad.

- La certificación
  Esclarecer qué es, en que consiste y las ventajas de obtener la certificación de la norma ISO 27001.

- Concienciar de la importancia de la seguridad de los datos
  Concienciando tanto al informático como a las empresas.

1.3 Impacto esperado

En la actualidad, el mundo de la informática y con ello la información avanza a una velocidad vertiginosa y en consecuencia, se deben establecer mecanismos para gestionar la información de una manera adecuada para así evitar las amenazas y pérdidas a las que puede ser sometida. Este trabajo, permitirá al lector obtener los conceptos necesarios que debe saber cualquier auditor de sistemas de gestión de seguridad de la información: la norma ISO 27001 *"Tecnologías de la información Técnicas de Seguridad Sistemas de Gestión de la Seguridad de la Información"*, la auditoría, la certificación, etc. Además, este trabajo mostrará la gran importancia que tiene para la empresa, la adquisición y establecimiento de la norma.

Por tanto, el impacto esperado desde el punto de vista del informático es el potenciamiento de este rol de auditor de sistemas de gestión de la seguridad de la información, incentivando a otros informáticos, explicando como funciona este sector y como formarse. Es fundamental que vean atractiva esta salida profesional, que va más allá del enfoque puramente técnico, dado que requiere una serie de habilidades sociales.

Sin olvidar, estimular a aquellas empresas que se encuentren dubitativas con respecto al establecimiento de dicha norma, mostrando de una manera concisa, el proceso y los beneficios de la misma.

1.4 Metodología

Todo buen trabajo se fundamenta en una buena planificación y metodología. Primordialmente se realizará un proceso de investigación y lectura de artículos, libros, trabajos de fin de grado, trabajos de fin de master, webs que traten sobre auditoría, la norma ISO 27001:2017 y sistemas de gestión de la seguridad de la información entre otros. Es decir, el primer paso consistirá en ampliar y adquirir los conocimientos necesarios con respecto a los aspectos del tema a tratar.

La investigación se llevará a cabo mediante buscadores tales como: google académico, riunet, polibuscador y los propios buscadores webs convencionales. No obstante, para obtener la norma ISO 27001:2017 y otras normas de gestión se accederá a la sección de la Universidad Politécnica de Valencia llamada *"AENORmas"* y de ahí se obtendrán las normas necesarias para el trabajo.

Una vez realizada la profunda lectura de todos los documentos relevantes, se realizará una síntesis de la información obtenida y se empezará a redactar la guía propuesta, abarcando todos los temas marcados como objetivos, al mismo tiempo que se va completando esta memoria así como un diccionario de términos.

1.5 Estructura

A partir de este punto. En el **capítulo dos**, se encuentra una breve introducción a la norma ISO 27001 y tras ello un análisis crítico del estado del arte, de algunos de los distintos artículos, trabajos y libros relacionados con el tema a tratar, además de introducir la propuesta del proyecto. A continuación, en el **capítulo tres** se analiza la problemática que se pretende abordar, además del marco tanto ético como legal y los riesgos principales. Posteriormente se identifican las soluciones posibles para hacer frente al problema y se presenta la solución propuesta, incluyendo el plan de trabajo realizado para llevar a cabo la misma. Seguidamente en el **capítulo cuatro**, se indica el diseño de la solución explicando las razones de porqué se han tomado algunas decisiones. En el **capítulo cinco**, se explica de manera clara y extendida, paso a paso como se ha desarrollado la solución. En el tramo final de la memoria, se encuentran en el **capítulo seis** las conclusiones obtenidas tras la realización del trabajo y la relación que tiene el mismo con los estudios cursados. En el **capítulo siete**, se presentan las mejoras que se podrían haber llevado a cabo y las nuevas líneas de desarrollo, consecutivamente en el **capítulo ocho** se encuentras las referencias de la memoria. Tras ello en el **capítulo nueve** se encuentra un glosario de términos relacionados con la temática. Finalmente en el **anexo** se presenta la guía de aproximación realizada.

2. Estado del arte

2.1 ¿Qué es la norma ISO 27001?

La ISO 27001:2017 "Tecnología de la información Técnicas de seguridad Sistemas de Gestión de la Seguridad de la Información" es una norma de gestión internacional creada por la Organización internacional de Normalización (ISO). Ésta es una organización independiente y no gubernamental, que cuenta con un total de 164 organismos nacionales de normalización que participan en el desarrollo de normas internacionales, entre ellas está la norma ISO 27001:2017, su publicación tuvo lugar en el año 2005 y se desarrolló en base a la norma británica BS 7799-2.

Esta norma tiene como función mantener la confidencialidad e integridad de los datos y de la información, así como de los sistemas que la procesan. Es una norma que debería tenerse más en cuenta en el mundo laboral, debido a la gran cantidad de información que se maneja, no obstante, cada vez más empresas solicitan los servicios de auditoría para la correcta implementación de sistemas de gestión de seguridad de la información, con el objetivo de que, tras la verificación de que se cumple la norma, obtener la certificación.

2.2 Búsqueda de documentos relacionados

Se ha realizado una búsqueda sobre artículos o trabajos relacionados con la norma ISO 27001 y la auditoría de sistemas de gestión de la seguridad de la información. Para ello se han empleado distintos buscadores web tales como: google académico, riunet, polibuscador y buscador de google convencional. Los resultados obtenidos han sido algunos artículos y trabajos relacionados con estos aspectos.

En la siguiente tabla, se muestran de manera organizada algunos de los resultados obtenidos tras el proceso, éstos vienen organizados en los siguientes parámetros: título, autor, año de edición y editorial, además de incluir un breve resumen y palabras clave de los respectivos documentos.

Tabla 1 Estado del arte

TÍTULO	AUTOR	AÑO DE EDICIÓN	EDITORIAL	RESUMEN	PALABRAS CLAVES
Fundamentos de ISO 27001 y su aplicación en las empresas	Martha Isabel Ladino Paula Andrea Villa S. Ana María López E.	2011	Universidad tecnológica de Pereira (Colombia)	Trata de concienciar la importancia de implantar un SGSI bajo la norma ISO 27001 en las empresas, explicando el proceso y ofreciendo una alternativa para aquellas empresas que no pueden permitirse la certificación de la norma.	ISO ISO27001 Sistema de gestión de seguridad de la información Plan-Do-Check-Act (PDCA)
Metodología de análisis y evaluación de riesgos aplicados a la seguridad informática y de información bajo la norma ISO/IEC 27001	Francisco Nicolás Javier Solarte Solarte Edgar Rodrigo Enriquez Rosero Mirian del Carmen Benavides Ruano	2015	*Revista Tecnológica ESPOL.*	Explicación de conceptos básicos dentro de la seguridad informática y de la información, que están relacionados con el análisis de riesgos de la norma ISO 27001. Se incluye un ejemplo de auditoría de seguridad de la información con posterior obtención de resultados tras analizar y evaluar los riesgos.	Análisis y evaluación de riesgos Estándar ISO 2700 Seguridad informática, seguridad de la información Plan-Do-Check-Act (PDCA)
Implantación de un sistema de gestión de seguridad de información bajo la ISO 27001: análisis del riesgo de la información	José Gregorio Arévalo Ascanio Ramón Armando Bayona Trillos Dewar Willmer Rico Bautista	2015	Revista Tecnura	Realiza un análisis preciso sobre la situación empresarial del municipio de Ocaña (Colombia) para encontrar debilidades con respecto al sector tecnológico. Se propone implantar un SGSI bajo la norma ISO 27001.	Tecnologías de Información ISO 27001

Guía de aplicación de la Norma UNE-ISO/IEC 27001 sobre seguridad en sistemas de información para pymes	Luis Gómez Fernández Ana Andrés Álvarez	2012	AENOR ediciones	Guía que explica los conocimientos básicos y avanzados necesarios sobre la aplicación de la Norma ISO 27001 . No obstante ,esta guía va enfocada a las pequeñas empresas	ISO 27001 Gestión información Pymes Plan-Do-Check-Act (PDCA)
Análisis del Riesgo y el Sistema de Gestión de Seguridad de Información El Enfoque ISO 27001:2005	Alberto G. Alexander, Ph.D	2005	Eficiencia Gerencial y Productividad	Explicación extendida de las fases del proceso de evaluación del riesgo, que permiten a una organización cumplir los requerimientos de la norma ISO 27001	Gestión Riesgos ISO 27001 Proceso de evaluación de riesgos Amenaza
Sistema de Gestión de Seguridad de la información: Análisis de ISO-27001:2005	Alejandro Corletti Estrada	2006	Servicio de Belt en seguridad de la información y protección de datos	Explicación de la norma ISO 27001 incidiendo en el ISMS en castellano SGSI sistema de gestión de seguridad de la información.	ISO 27001 IEC ISMS
ISO 27001: Funcionalidades y ventajas en la empresa	www.pmg-ssi.com	2016	-	Introduce que es la norma ISO 27001, dónde puede ser implantada y cómo funciona. Argumenta mediante cuatro ventajas esenciales la importancia de la norma ISO 27001 en la organización o empresa.	ISO 27001 Ventajas

Implantación de la norma UNE-ISO/IEC 27001 en una empresa de sector servicios	Jorge Anduix Fuentes	2015	Universitat Politécnica de Valencia	Implantación de la norma UNE-ISO/IEC 27001 en una empresa, mediante la realización de una auditoría de sistemas. Incluye un informe ejemplo de una auditoría de la ISO 27001.	ISO 27001 Implantación Certificación
Plan de auditoría del desarrollo de aplicaciones en una empresa informática	Mª Amparo Aguilar Escobí	2012	Universitat Politécnica de Valencia	Explica los conceptos de auditoría de sistemas de información desde el origen de la primera auditoría (finalidad, objetivos, etc), además de los distintos organismos, certificaciones y normativas. Finalmente, explica el plan de auditoría del desarrollo de aplicaciones informáticas.	Auditoría Sistemas de Información Certificación

2.3 Crítica al estado del arte

La búsqueda de artículos o trabajos relacionados con algunos de estos aspectos individualmente, no ha sido costosa, sin embargo, escasean los artículos o trabajos que engloban todos estos conceptos o explican cómo se forma un auditor de sistemas de gestión de la seguridad de la información o que perfil ha de tener.

La mayoría de los resultados obtenidos no explican la ISO 27001 desde el punto de vista del auditor, si no que están orientados desde el punto de vista de la empresa. Se centran únicamente en aspectos concretos de la norma, pero no en la auditoria, ni en cómo se audita esta norma. Tampoco dan una información muy detallada del perfil que tiene que tener un auditor de sistemas de gestión de la seguridad de la información, que es uno de los papeles fundamentales en los que se va a enfocar este trabajo.

Algunos de estos documentos están desactualizados debido al momento de su realización y no explican la norma ISO 27001:2017 actual, en su lugar emplean la de

versiones anteriores, como es el caso del documento *"Análisis del Riesgo y el Sistema de Gestión de Seguridad de Información El Enfoque ISO 27001:2005",* que trata la versión del año 2005.

En conclusión, la mayoría de documentos encontrados centran gran parte del contenido en la Norma ISO 27001 así como su implantación en las empresas. Sin embargo, el papel del auditor es uno de los temas ausentes. Por ello el resultado de este TFG puede ser innovador y útil, ya que debido a los avances tecnológicos surgen nuevas amenazas.

2.4 Propuesta

Este trabajo tiene como función principal explicar cuál es el papel del informático como auditor de sistemas de gestión de seguridad de la información bajo la norma ISO 27001:2017, incluyendo su importancia y beneficios mediante la elaboración de un documento que guie a un profesional informático recién titulado a orientarse hacia este sector, mostrando los conceptos necesarios de la norma ISO 27001:2017, de la auditoría, y la certificación, además de cómo obtenerlos.

3. Análisis del problema

El gran problema que generalmente se observa es la falta de profesionales en el sector de la ciberseguridad, según una encuesta realizada por el *"Centro para la Ciberseguridad y Educación (ISC)"* en el año 2022 habrá 1,8 millones de puestos vacantes de expertos en ciberseguridad, de ellos 350.000 en Europa. Hecho que requiere un cambio drástico debido a la velocidad vertiginosa a la que avanza la tecnología, el manejo de información y por consiguiente las amenazas a las que está sometida, lo que conlleva a la necesidad de una gran cantidad de profesionales en este sector.

Una de las principales razones por las que se produce esta falta de profesionales, es debido a la inmediatez con la que se han producido estos cambios, la sociedad se ha dado cuenta de la importancia de esta información, su vulnerabilidad y la facilidad con la que pueden ser dañada. Hoy en día y debido a estos avances (por ejemplo el 5G), la preocupación por los ataques externos a este activo hace que sea necesario expertos de su seguridad, es una necesidad social y empresarial.

Actualmente, la información que se encuentra en la web es ambigua y difícil de localizar.

Empresas de todo tipo de sectores y en mayor medida en el sector de las TIC (Tecnologías de la información y la comunicación) tal y como indican los datos mostrados en el encuesta oficial de ISO de 2017, solicitan auditorías para la verificación de la correcta implantación de la norma ISO/IEC 27001:2017 y la consiguiente obtención, en caso favorable, de la certificación, dado que con el avance de los años las empresas son más conscientes de la necesidad de implantar correctamente un sistema de gestión de la seguridad de la información. De 2016 a 2017 se incrementó un 19% las certificaciones de la norma ISO/IEC 27001:2017

3.1 Análisis del marco legal y ético

3.1.1 Legal

En el manejo correcto de la información hay que cumplir con la legislación.

Existen tres leyes fundamentales que rigen este manejo, que son:

- "*Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales*"

  Esta ley española, también conocida como LOPDGDD es la "nueva" LOPD (Ley de Protección de Datos) aprobada en diciembre de 2018. Tiene como objetivo principal, garantizar y salvaguardar los datos de carácter personal de toda

persona física registrada sobre cualquier tipo de información, hecho que como indica el artículo 18.4 de la constitución española es un derecho: *"La protección de las persona físicas en relación al tratamiento de datos personales es un derecho fundamental"*. (fuente*: BOE núm. 294, de 6 de diciembre de 2018, referencia: BOE-A-2018-16673)*

- *"Real Decreto Legislativo 1/1996, de 12 de abril, por el que se aprueba el texto refundido de la Ley de Propiedad Intelectual, regularizando, aclarando y armonizando las disposiciones legales vigentes sobre la materia"*. Esta ley española, también conocida como LPI fue aprobada el 12 de abril de 1996. Tiene como finalidad proteger la "creatividad" de las personas, según la propia ley, su función es proteger: "la propiedad intelectual de una obra literaria, artística o científica…" (fuente*: BOE núm. 97, ref BOE-A-1996-8930)*.

- *"Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, del 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)"* RGPD, es semejante a la LOPDGDD española, pero a nivel europeo. De hecho, la LOPDGDD tenía como objetivo cumplir las directrices de esta ley europea. (fuente: *BOE, "DOUE núm. 119, de 4 de mayo de 2016")*

Estas tres leyes van ligadas a la seguridad de la información, ya que el objetivo principal de estas, es proteger distintos aspectos de la misma. Una base importante de las normas ISO es su cumplimiento legal, que a su vez es uno de sus requisitos.

En la norma ISO 27001:2017 uno de los objetivos de control y controles de referencia es: *"Cumplimiento de los requisitos legales y contractuales"* que tiene como finalidad: *"evitar incumplimientos de las obligaciones legales, estatuarias, reglamentarias o contractuales relativas a la seguridad de la información o los requisitos de la seguridad"*. Por tanto la norma ISO 27001:2017 igual que el resto de normas ISO, ayudan a cumplir con la legislación.

A continuación, se muestran dos ilustraciones de los apartados de la norma ISO 27001:2017, que buscan cumplir con estas leyes comentadas anteriormente (las mismas han sido extraídas de la propia norma ISO 27001:2017 a través del servicio "*AENORmas"*):

A.18.1.2	Derechos de Propiedad Intelectual (DPI)	*Control* Deben implementarse procedimientos adecuados para garantizar el cumplimiento de los requisitos legales, regulatorios y contractuales sobre el uso de materiales, con respecto a los cuales puedan existir derechos de propiedad intelectual y sobre el uso de productos de software patentados.

Ilustración 1 A.18.1.2 Derechos de Propiedad Intelectual, Objetivos de control y controles de referencia de la norma ISO 27001:2017

A.18.1.4	Protección y privacidad de la información de carácter personal	*Control* Debe garantizarse la protección y la privacidad de los datos, según se requiera en la legislación y la reglamentación aplicables.

Ilustración 2 A.18.1.4 Protección de privacidad de la información de carácter personal. Objetivos de control y controles de referencia de la norma ISO 27001:2017

3.1.2 Ético

Todo informático igual que todo profesional debe actuar de manera ética, la ética tal y como define la Real Academia Española de la Lengua (RAE) es un: *"Conjunto de normas que rigen la conducta de la persona en cualquier ámbito de la vida"*.

La ética hay que tenerla presente en todos los ámbitos de la vida, los profesionales tienen un criterio avalado por unos conocimientos adquiridos que otras personas no tienen y deben actuar de manera ética y profesional, sin aprovecharse del desconocimiento de otros como por ejemplo no realizar ingeniería social.

La ingeniería social consiste en utilizar a las personas para, sin su conocimiento o consentimiento, realizar tareas que afecten a la seguridad o bien obtener información privada como contraseñas o datos bancarios.

Un ejemplo de falta de ética fue el incidente ocurrido en el año 2014 en el Hospital de Fuenlabrada cuando se filtraron datos de sus pacientes a la clínica privada de Los Madroños, lo que dio lugar a ceses de altos cargos del hospital, y a una gran desconfianza por parte de los clientes en el tratamiento de sus datos.

Cuando se trabaja con información hay que mantenerse firme y cumplir con la ética y la legislación, dado que hay una enorme responsabilidad en el momento que se manejan datos de personas físicas.

Los auditores de gestión de la información deben actuar de manera ética desde el punto de vista profesional, dado que el informe resultante de su auditoría debe ser completamente veraz y objetivo.

3.2 Análisis de riesgos

Existen una enorme cantidad de riesgos pero principalmente se pueden identificar dos tipos de ellos, uno en cuanto a la gestión de la información en las empresas y otro en cuanto a la propuesta realizada.

3.2.1 Gestión de la información

Tal y como se ha indicado en varias ocasiones, toda empresa hoy en día, maneja información, debido al creciente uso de las nuevas tecnologías. Esta información está continuamente sometida a amenazas a causa de la aparición de: ciberdelincuentes, descuidos, falta de organización, desconocimiento del personal, mala praxis, etc. Por tanto, es de vital importancia garantizar su correcta gestión y su seguridad, corrigiendo las debilidades o fallos de los activos de información (vulnerabilidades) y protegiéndola de los ciberataques, que se encuentran a la orden del día.

Fundamentalmente, se pueden encontrar dos riesgos en las empresas con respecto al manejo de información, que son los siguientes:

Una empresa sin gestión de la información supone un alto riesgo para la misma, dado que se encontrará expuesta a grandes amenazas, como son los ciberataques, además, la empresa puede llegar a incumplir partes de la legislación tales como las leyes previamente comentadas. Esto supondría pérdidas para las empresas incluso sanciones, según el informe realizado por "*radware*" (empresa mundial de ciberseguridad) llamado *"Radware´s 2018-2019 Global Application & Network Security Report"* el coste medio de un solo ciberataque exitoso fue de 1,1 millones de dólares.

Una empresa que no aplique normas de gestión tales como la norma ISO 27001:2017 está sometida al riesgo de quedarse muy por detrás de sus competidores, dado que las normas ISO suponen una mejora notable para las empresas y por consiguiente más fiabilidad y seguridad para los clientes.

Estos dos riesgos se pueden solucionar concienciando a las empresas de la importancia del correcto y seguro manejo de la información, mediante la implantación de un sistema de gestión de la seguridad de la información tal y como indica la norma ISO 27001:2017.

3.2.2 Propuesta

El mayor riesgo al que puede estar sometido este proyecto es, la falta de aceptación del mismo por parte de los interesados y por tanto que no resulte provechoso.

Riesgo que puede ser solventado si es realizado de manera atractiva, didáctica y amena para el lector. Conteniendo los recursos y la información necesaria que debe tener este proyecto.

3.3 Identificación y análisis de soluciones posibles

El objetivo principal consiste en recoger toda la información necesaria para que un informático pueda formarse y conozca como ejercer como auditor de sistemas de gestión de la seguridad de la información.

Se plantean tres soluciones para alcanzarlo y solventar la problemática:

- Elaboración de una guía de aproximación

Este guía orientará a los recién titulados en informática o cualquier interesado en el mundo de la auditoría de sistemas de gestión. En él se tendrá fácil acceso a la información necesaria para entender en que consiste esta salida profesional, que requisitos son necesarios cumplir, que norma es la que lo rige y como formarse, así como la importancia de este sector y sus ventajas, de forma amena y didáctica.

- Recolección de dudas de profesionales del sector

La segunda solución consiste en elaborar un documento donde se recopilen todas las dudas que se les plantearon en su momento a los distintos profesionales del sector así como su solución, contactando con distintos profesionales del sector.

- Realización de un blog

La última solución planteada consiste en realizar un blog o web que recoja toda la información necesaria que debe conocer un informático que quiera ejercer como auditor o que esté interesado en este sector.

Una vez expuestas las tres soluciones se mostrará una tabla comparativa con sus respectivas ventajas y desventajas.

Tabla 2 Soluciones posibles

SOLUCIÓN	VENTAJAS	DESVENTAJAS
Elaboración de una guía que recoja los conceptos básicos para ejercer como auditor de sistemas de gestión de seguridad de la información	- Elemento tanto tangible como digital - Libertad de añadir todos los contenidos - Su acceso no requiere de conexión a internet	- Una mala estructura y explicación puede confundir.
Recolección de dudas de profesionales del sector	- Resolución de dudas concretas - Muy directo	- Puede resultar escueto y falto de información - Puede no dar soluciones a dudas actuales
Realización de un blog	- Es autodidáctico - La información es más actualizada	- Se puede distorsionar el objetivo. - Un mal diseño puede suponer dificultad de encontrar la información

Finalmente, la elección fue la elaboración de una guía puesto que es donde mejor se puede recoger toda esta información, además de que es un documento tanto tangible como digital y de fácil acceso para cualquier usuario, que no requiere de conexión a internet.

3.4 Solución propuesta

La solución evidente a esta problemática de falta de profesionales en el sector de la ciberseguridad, es que cada vez más informáticos se decidan por ella, derivándose, en este caso, al sector de la auditoría de sistemas de gestión de la seguridad de la información, por tanto sería conveniente facilitar el acceso al conocimiento de este campo y esta norma.

La elaboración de guía de aproximación que contenga toda la información necesaria, facilitaría este acceso y conocimiento al informático, mostrando cuales son los conceptos necesarios y como obtenerlos, tanto de la norma como del auditor y la certificación. Es necesario incidir en la trascendencia de esta salida profesional y en las ventajas que tiene este sector de la auditoria.

Para desarrollar esta solución, el proceso de elaboración se realizará en distintas fases, empezando con una fase de profunda lectura y asimilación de conceptos. Posteriormente se realizará un análisis de toda la información, seleccionando aquella que sea más rigurosa e interesante. Finalmente se elaborará el formato para que se muestre de manera más didáctica y amena para el lector.

3.5 Plan de trabajo

Este plan seguirá una serie de fases para su elaboración:

- Reunión y planificación

  Esta fase comenzará con la primera reunión con la tutora, en ella se establecerá la planificación de la realización del trabajo.

- Lectura y documentación

  En esta fase se recopilara toda la información necesaria estudiando las siguientes normas de gestión: ISO 27001:2017: "Tecnologías de la información, Técnicas de seguridad, Sistema de Gestión de la Seguridad de la Información, Requisitos"; ISO 19011:2018 :"Directrices para la auditoría de los sistemas de gestión" e ISO 9001:2015 "Sistemas de gestión de la calidad" la obtención de estas normas se realizará accediendo al servicio que tiene la Universitat Politécnica de Valencia *"AENORmas"*; además se revisará la guía de implantación de la norma ISO 27001 (realizada por AENOR) y demás documentos relacionados tanto con la norma como con la auditoría.

- Escritura de la guía

  Una vez adquiridos los conocimientos necesarios tras la lectura y estudio de los documentos anteriormente indicados, se comenzará a redactar la guía enfocada al auditor. Intentando abordar todos los aspectos necesarios que todo informático debe conocer para iniciarse en el mundo de la auditoria de sistemas de gestión de la seguridad de la información.

- Implantación del formato

  En esta fase se implantará el formato de la guía, para que sea más didáctico y ameno para el lector.

- Revisión

  Finalmente se revisarán los fallos pertinentes en cuanto a contenido y redacción y se modificará hasta llegar al trabajo final.

4. Diseño de la solución

Para el diseño de la solución cómo se ha comentado anteriormente en el punto "Identificación y análisis de soluciones posibles", se han planteado una serie de alternativas antes de elegir la solución final. El punto de partida consiste en ayudar al informático a como ejercer como auditor de sistemas de gestión de la seguridad de la información bajo la norma ISO 27001:2017, por esta razón la estructura y el formato de la guía tienen un papel trascendental, ya que tiene que ser claro, directo y conciso.

Se marcan tres puntos fundamentales que son la raíz del mismo: la norma ISO 27001:2017, el informático como auditor y la certificación y su funcionamiento.

Principalmente, se introduce al lector en el contexto. Tras ello, el primer concepto que se ha decidido explicar es la norma ISO 27001, dado que es la principal competencia que debe conocer un informático que ejerce como auditor bajo esta norma.

Una vez sentadas las bases de la norma, se explican los conceptos de auditor y auditoría, así como sus tipos (desde el punto de vista del sujeto que la realiza), dado que el tipo de auditoría de esta guía es de sistemas de gestión de la seguridad de la información.

Posteriormente, se procede a explicar las competencias y como debe actuar, es decir, como poner en práctica los conocimientos adquiridos hasta el momento una vez se tiene claro los conceptos de la norma, auditor y auditoría. Además sin estos conocimientos previos este apartado carecería de sentido y generaría confusión al lector.

A continuación, se presenta como obtener las competencias previamente explicadas, ya que el lector tiene estos conceptos recientes.

Finalmente se explican las herramientas de auditoría más trascendentales, y el proceso de certificación, este punto se explica al final dado, que para comprenderlo el lector debe conocer todos los aspectos explicado previamente.

Con respecto al formato, uno de los objetivos es que sea directo por ello, se emplean los signos de interrogación en gran parte de los títulos, para que el lector pueda acceder directamente a las respuestas que le interesen y sea lo más didáctico posible, añadiendo imágenes para que sea más ilustrativo.

5. Desarrollo de la solución propuesta

Para comenzar a desarrollar la solución primero hay que adquirir los conocimientos necesarios y asimilarlos para posteriormente explicarlos de manera clara y concisa.

Primero se realiza la planificación del desarrollo de la solución, en los distintos meses, además de fijar los objetivos del mismo.

Se establece comenzar con la lectura de la norma ISO 27001:2017, esta norma se obtiene mediante el servicio de la universidad llamado *"AENORmás"*. Este servicio es una base de datos que contiene todas las normas UNE. Para acceder a él se realiza la búsqueda mediante el polibuscador. Una vez se accede al servicio con posterior identificación como alumno de la universidad, se busca la norma mencionada, y se descarga, como se muestra a continuación:

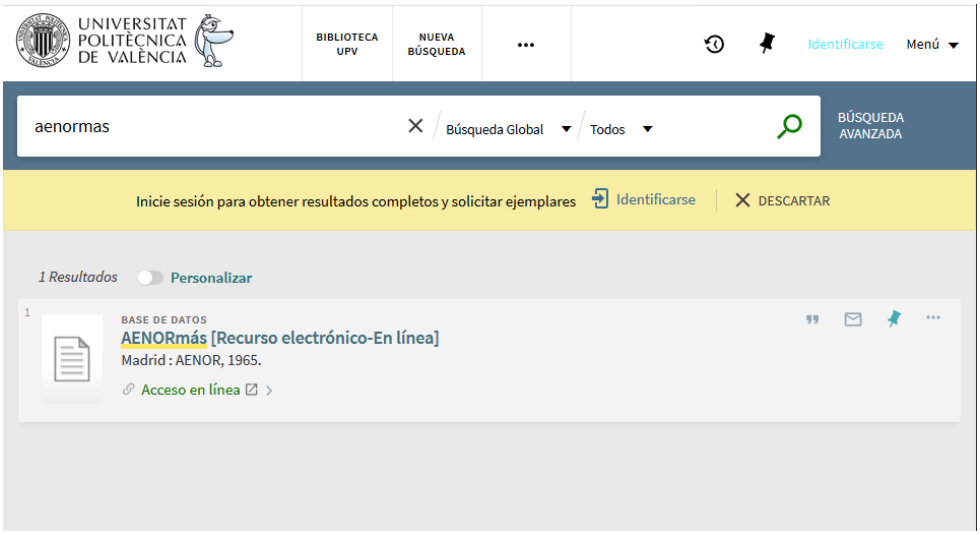

Ilustración 3 Servicio polibuscador

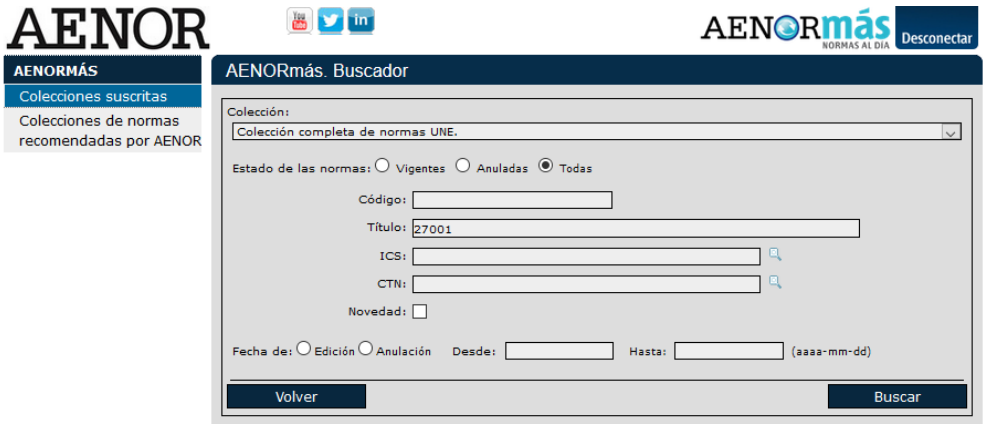

Ilustración 4 Servicio Aenormás búsqueda norma ISO 27001:2017

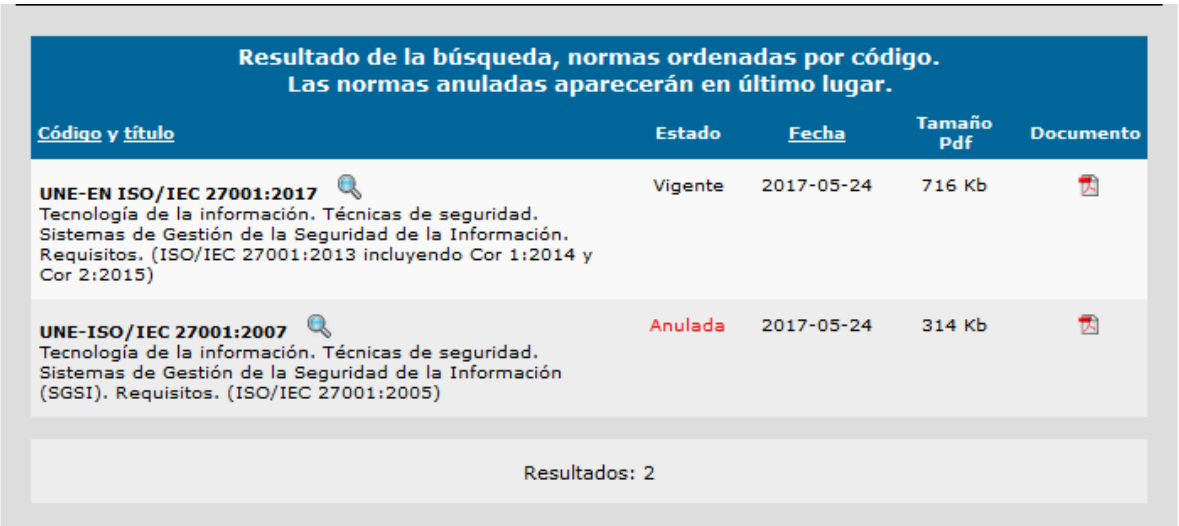

Ilustración 5 Resultados de la búsqueda realizada

Tras la obtención del documento de la norma se realiza una lectura para entender en que consiste y que abarca, subrayando aquello que es más destacable de la misma, además, tras la posterior lectura, se buscan artículos que expliquen que aporta esta norma, y se accede a la propia web oficial de ISO para obtener más información.

Mediante el servicio polibuscador también se obtiene un libro que será de gran ayuda: la guia de aplicación de la norma ISO 27001:2017 realizada por "AENOR".

Una vez sentadas las bases con respecto a la norma, se busca profundizar en el concepto de auditoría y auditor a través de una búsqueda de distintos artículos y libros, entendiendo que es un auditor de sistemas de gestión de la seguridad de la información.

En esta búsqueda previamente explicada se debe realizar un filtrado de la información, dado que cuando se realiza una búsqueda del concepto auditor o auditoría,

generalmente se encuentran artículos de auditoría financiera, auditoría que no tiene ninguna relación con la auditoría a tratar.

Dos recursos fundamentales para entender cómo funciona la auditoría y los sistemas de gestión son: la norma ISO 19011:2018 y la norma ISO 9001:2015, estas obtenidas de igual manera que la norma ISO 27001:2017 mediante el servicio *"AENORmás"* previamente mencionado. La norma ISO 19011:2018 contiene las directrices para la correcta realización de una auditoría de sistemas de gestión.

Posteriormente se accede a obtener información de la certificación y acreditación además de ayudarse de la guía anteriormente mencionada y buscar distintos artículos por la web, se accede a la web oficial de ENAC. En ella se realiza una búsqueda de todas aquellas empresas certificadoras acreditadas en España para el estándar de la norma ISO 27001:2017.

Por último se realiza la búsqueda de información sobre la formación de auditores de sistemas de gestión de la seguridad de la información, accediendo tanto a AENOR como a IRCA recogiendo información de los distintos cursos y exámenes.

Inmediatamente después de finalizar esta gran fase de lectura, búsqueda y asimilación de una gran cantidad de conceptos e información, se inicia la redacción de la guía; se comienza estableciendo el índice con los contenidos que va a contener.

Finalmente una vez hecho el índice y desarrollado el contenido, se realiza una búsqueda de distintos formatos para la guía, como se ha comentado anteriormente se busca que sea atractivo, ameno y didáctico por tanto ha de ser un formato accesible para el lector y de comprensión sencilla. Algunas de los ejemplos observados que sirvieron de inspiración, fueron las guías de *"Incibe"* y *"tufinanciación"*.

6. Conclusiones

A lo largo de este proyecto se han recogido los conceptos necesarios para guiar a los ingenieros informáticos, tanto los recién titulados como los profesionales, a como ejercer como auditor de sistemas de gestión de la información.

Analizando este trabajo de fin de grado desde el principio hasta su consecución, se puede decir que se ha cumplido con el objetivo principal estipulado, tanto a nivel de trabajo como a nivel personal, la ampliación de los conocimientos de este sector y su posterior reflejo en este trabajo.

Realizando un balance a nivel de trabajo, se ha conseguido que la guía contenga toda la información que se había planificado:

- Se han presentado la norma ISO 27001 explicando en que consiste en profundidad, además de mostrar la importancia y sus beneficios tanto para la empresa, como para la persona que la audita.

- Se ha profundizado en el concepto de auditoría explicando en que consiste tanto la auditoría como el auditor en conceptos generales. Matizando en el ámbito de sistemas de gestión de la información, además de indicar el perfil del auditor; las competencias.

- Se ha expuesto la correcta metodología que debe de realizar un auditor durante el proceso de auditoría explicando meticulosamente cada fase.

- Se han mostrado y explicado las herramientas de auditoría más empleadas durante la realización de la misma.

- Se ha explicado en que consiste la certificación, su respectivo proceso y las entidades.

No obstante, ha sido un proceso costoso, dado que se ha tenido que realizar una profunda investigación de los contenidos a tratar, en el que ha habido que manejar una gran cantidad de información, contrastarla y posteriormente asimilarla, sintetizarla y explicarla de una forma clara, amena y didáctica. Además de tener que realizar una mejora notable en la expresión y redacción, aspecto muy beneficioso, ya que para ejercer como auditor, el tener un gran dominio de la redacción y la sintaxis juega un papel fundamental.

6.1 Relación del trabajo desarrollado con los estudios cursados

A lo largo de la carrera del grado de ingeniería informática se han adquirido una gran cantidad de conceptos además de valores y competencias.

Para la realización de este trabajo se han requerido los conocimientos adquiridos en algunas de las asignaturas cursadas a lo largo de la carrera concretamente en la rama cursada de sistemas de información. Algunos de estos conocimientos son: sistemas de gestión, auditorías, normas de gestión, ética como informático, seguridad, ley de protección de datos, ley de propiedad intelectual, etc.

Por tanto en el desarrollo de este trabajo se han puesto en práctica los conocimientos adquiridos, profundizando más en ellos y ampliándolos, aspecto que en el ámbito profesional resultará muy beneficioso para el futuro. Por ejemplo, se ha profundizado en las normas de gestión, concretamente en la norma ISO 27001:2017 y también en la ejecución de una auditoría, en los tipos de auditores, su función etc; dado que de estos aspectos solo se tenía una noción muy básica y generalizada.

De esta manera, se deja constancia que el trabajo de fin de grado realizado es conforme a los estudios cursados. Con los resultados del trabajo realizado se ha podido desarrollar una guía de aproximación para informáticos o interesados en este sector de sistemas de gestión de la seguridad de la información.

Finalmente, con respecto a las competencias transversales que se han ido valorando a lo largo del grado de ingeniería informática, se considera que se han puesto en práctica durante el desarrollo del trabajo de fin de grado las siguientes:

- CT_01 - Comprensión e integración

  La integración de los conocimientos adquiridos, además de la lectura y comprensión de los mismos han hecho posible el desarrollo de este proyecto.

- CT_04 Innovación, creatividad y emprendimiento

  Se ha dado respuesta mediante la creación de una guía, recurriendo a la creatividad y emprendimiento durante su realización.

- CT_05 - Diseño y proyecto

  A lo largo del trabajo se ha dirigido, diseñado y evaluado el mismo hasta su consecución final buscando siempre un diseño atractivo y accesible.

- CT_08 - Comunicación efectiva

Este proyecto se ha desarrollado explicando los conocimientos adquiridos de una manera clara y didáctica para el lector.

- CT_09 - Pensamiento crítico

  Se ha realizado un análisis de la situación actual de este campo y su carencias.

- CT_10 - Conocimiento de problemas contemporáneos

  Se ha adquirido conciencia de la importancia de la seguridad de los datos y de la información.

- CT_11 - Aprendizaje permanente

  Se ha requerido aprender nuevos conocimientos para la realización del TFG

- CT_12 -Planificación y gestión del tiempo

  Ha sido necesaria una buena planificación y gestión del tiempo para poder finalizar el trabajo.

7. Trabajos futuros

Para concluir el trabajo, en este apartado se van a analizar las mejoras que se podrían haber realizado en el mismo y aquellas líneas de desarrollo que se abren para aplicar estos resultados a otras áreas.

En primer lugar, una vez finalizada la guía, se podría desarrollar una web con todos los contenidos de la misma, permitiendo otra forma de mostrar los conocimientos necesarios para guiar a los informáticos en el sector de la auditoría de sistemas de gestión de seguridad de la información. En segundo lugar, un aspecto que no se ha podido llevar a cabo, es presenciar la realización de una auditoría de sistemas de gestión de seguridad de la información, que hubiera permitido observar de primera mano las distintas fases de la que consta la misma.

Finalmente, con respecto a nuevas líneas de desarrollo, se podrían trasladar a otros ámbitos de la ciberseguridad, que puedan ayudar a que más profesionales se decidan por este sector tan necesario, por ejemplo, un fenómeno de rigurosas actualidad es la tecnología del 5G, un avance que genera incertidumbre debido a la revolución que va a suponer en la sociedad; tal y como dice el director del *Centro Nacional de Inteligencia CNI*, Félix Sanz Roldán, que lo califica como "una revolución", no obstante, también afirma que la ciberseguridad *"va a sufrir"* con esta nueva tecnología, por tanto se abre otro campo para auditar y controlar su seguridad.

8. Referencias

[0] Martha Isabel Ladino, Paula Andrea Villa S., Ana María López E. *"Fundamentos de ISO 27001 y su aplicación en las empresas" Universidad Tecnológica de Pereira*. Año de publicación: 2011.

Disponible en:
http://revistas.utp.edu.co/index.php/revistaciencia/article/download/1177/669

[1] Francis Nicolas Javier Solarte Solarte, Edgar Rodrigo Enriquez Rosero, Mirian del Carmen Benavides Ruano *"Metodología de análisis y evaluación de riesgos aplicados a la seguridad informática y de información bajo la norma ISO/IEC 27001". Revista Tecnológica ESPOL.* Año de publicación: 2015.

Disponible en:
http://www.rte.espol.edu.ec/index.php/tecnologica/article/view/456/321

[2*]* José Gregorio Árevalo Ascanio, Ramón Armando Bayona Trillos, Dewar Willmer Rico Bautista *"Implantación de un sistema de gestión de seguridad de información bajo la ISO 27001: análisis del riesgo de la información". Revista Tecnura*. Fecha de publicación: 24 de agosto de 2015.

Disponible en: http://www.scielo.org.co/pdf/tecn/v19n46/v19n46a11.pdf

[3] Luis Gómez Fernandez, Ana Andrés Álvares .*"Guía de aplicación de la Norma UNE-ISO/IEC 27001 sobre seguridad en sistemas de información para pymes"* AENOR ediciones. Año de publicación: 2012

[4] Alberto G. Alexander, Ph.D *"Análisis del Riesgo y el Sistema de Gestión de Seguridad de Información El Enfoque ISO 27001:2005" Eficiencia Gerencial y Productividad S.A*. Año de publicación: 2005.

Disponible en:
http://www.iso27000.es/download/Analisis_del_Riesgo_y_el_ISO_27001_2005.pdf

[5] Alejandro Corletti Estrada. *"Sistema de Gestión de Seguridad de la información: Análisis de ISO27001:2005" Servicios Belt de Seguridad de la información.*

Disponible en: http://www.belt.es/expertos/HOME2_experto.asp?id=3362

[7] *"ISO 27001: Funcionalidades y ventajas en la empresa", Blog especializado en Sistemas de Gestión de la seguridad de la información*. Fecha de publicación: 19 de julio de 2016.

Disponible en: https://www.pmg-ssi.com/2016/07/normativa-que-utiliza-norma-iso-27001/

[8] Jorge Anduix Fuentes. *"Implantación de la norma UNEISO/IEC 27001 en una empresa de sector servicios". UPV*. Año de publicación: 2015

Disponible en: https://riunet.upv.es/

[9] Mª Amparo Aguilar Escobí. *"Plan de auditoría del desarrollo de aplicaciones en una empresa informática"* Universitat Politécnica de Valencia. Fecha de publicación: 2012.

[10] Santiago Jiménez García *"Protección de Datos de Carácter personal"*. Boletin Oficial del Estado BOE. Fecha de última modificación: 19 de marzo de 2019.

Disponible en: https://www.boe.es/biblioteca_juridica/index.php?tipo=C

[11] *"Real Decreto Legislativo 1/1996, de 12 de abril, por el que se aprueba el texto refundido de la Ley de Propiedad Intelectual, regularizando, aclarando y armonizando las disposiciones legales vigentes sobre la materia."* Ministerio de Cultura BOE. Fecha de última modificación: 2 de marzo de 2019.

Disponible en: https://www.boe.es/buscar/act.php?id=BOE-A-1996-8930

[12] *"Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales."* Jefatura del Estado BOE. Fecha de publicación: 6 de Diciembre de 2018.

Disponible en: https://www.boe.es/buscar/doc.php?id=BOE-A-2018-16673

[13] *"Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, del 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)"* .DOUE. Fecha de publicación: 4 de mayo de 2016.

Disponible en: https://www.boe.es/buscar/doc.php?id=DOUE-L-2016-80807

[14] Marcos Martínez "El 87% de las empresas no puede hacer frente a las amenazas digitales" Hablemos de empresas. Fecha de publicación: 21 de marzo de 2019.

Disponible en: https://hablemosdeempresas.com/empresa/ciberseguridad-en-pymes/

[15] *radware. "Radware's 2018-2019 Global Application & Network Security Report"*

Disponible en: https://www.radware.com/ert-report-2018/

Disponible en: https://www.ey.com/es/es/home/ey-global-information-security-survey-2019

[16] Bárbara Sánchez. *"Se necesitan urgentemente expertos en ciberseguridad: ¿qué estudiar para ser uno de ellos?". elPaís*. Fecha de publicación: 16 de Enero de 2019.

Disponible en: https://elpais.com/economia/2019/01/14/actualidad/1547486152_048652.html

9. Glosario de términos

Para facilitar la comprensión tanto de la memoria como de la guía, se han definido una serie de términos, dentro del contexto de la auditoría y los sistemas de gestión de la seguridad de la información.

- **Activo:** Cualquier elemento propiedad de la empresa relacionado con la información.

- **Norma ISO 9001:2015**: Norma que establece los requisitos necesarios que una empresa debe cumplir para realizar un correcto uso de un sistema de gestión de calidad.

- **Auditoría**: Proceso sistemático de carácter objetivo, que consiste en analizar y evaluar el entorno junto con sus componentes y determinar el cumplimiento con la metodología y requisitos establecidos por una norma o unos criterios determinados.

- **Auditor:** Persona encargada de realizar la auditoría y verificar que los requisitos establecidos por una empresa o los que dicta una norma se cumplen

- **Alcance:** Cantidad de elementos de la empresa que abarcará la auditoría

- **Norma ISO 19011:2018 "Directrices para la auditoría de sistemas de gestión":** Norma que establece las directrices que se deben seguir para la correcta realización de una auditoría de sistemas de gestión.

- **Análisis de riesgos:** Estudio sobre los posibles inconvenientes que puedan aparecer en la empresa durante la realización de la auditoría y su posterior clasificación con respecto al grado de amenaza.

- **Auditoría primera parte:** Realización del proceso de auditoría por o en nombre de la empresa sobre la que audita.

- **Auditoría segunda parte:** Realización del proceso de auditoría por organizaciones que tienen un interés o relación con la empresa que se va a auditar, tales como clientes o proveedores.

- **Auditoría tercer parte:** Realización del proceso de auditoría por organizaciones auditoras independientes y completamente externas a la organización.

- **Confidencialidad:** Propiedad de la información que garantiza su acceso solo a personal autorizado.

- **Disponibilidad:** Propiedad de uno o varios elementos que indica su accesibilidad

- **ENAC:** Entidad Nacional de Acreditación, organismo que regula el funcionamiento de la acreditación en España.

- **Entidad de acreditación:** Organismo encargado de acreditar a las organizaciones para que puedan conceder certificaciones y por consiguiente ejercer como entidades certificadoras.

- **Entidad certificadora:** Entidad acreditada encargada de auditar y conceder certificados a las empresas según distintas normas.

- **Seguridad de la información:** Mantener la información protegida ante cualquier peligro.

- **ISO 27001:2017 "Tecnología de la información técnicas de seguridad sistemas de gestión de la seguridad de la información":** norma internacional que permite la ratificación, la confidencialidad e integridad de los datos y de la información, así como de los sistemas que la procesan.

- **Objetivo:** Propósito o meta que se quiere alcanzar.

- **Evidencia:** Muestra o prueba obtenidas tras el proceso de análisis que no puede ser refutada.

- **PDCA:** "Plan-Do-Check-Act" en castellano "Planificar-Hacer-Verificar-Actuar". Ciclo tradicionalmente empleado en los sistemas de gestión de la calidad que permite a las empresas y organizaciones mejorar continuamente.

- **SGSI:** Sistema de Gestión de la Seguridad de la Información. Parte del sistema de gestión general empleado para mantener y mejorar la seguridad de la información.

- **Riesgo:** Posibilidad de que una amenaza pueda convertirse en un daño o pérdida para la empresa.

- **Salvaguardar:** Protección de cualquier activo de información.

- **Vulnerabilidad:** Debilidad o fallo de un activo de información con posibilidad de explotación, es decir, que puede ser empleada para causar daños sobre el activo.

- **Amenaza:** Acción que utiliza una vulnerabilidad para atacar la seguridad de un activo de información.

- **Debilidad:** Tipo de defecto o fallo.

- **Informe de auditoría:** Documento donde se exponen las conclusiones sacadas por el auditor tras la realización completa de la auditoría.

- **Auditado:** Entidad o empresa sobre la que se realiza la auditoría.

- **Requisito:** Capacidad que se debe tener para satisfacer una norma o un contrato.

- **Checklist:** Documento que recoge una serie de preguntas para evaluar a la empresa u organización.

- **Programa de auditoría:** Documento que contiene todas las actividades que se van a realizar en la auditoría.

- **ISO:** "International Organization for standarization" en castellano "Organización Internacional de Normalización". Organización encargada de crear, establecer y gestionar estándares internacionales.

- **IEC:** "International Electrotechnical Commission" en español "Comisión electrónica mundial" es una organización encargada de publicar estándares.

- **Políticas:** Serie de medidas establecidas por una empresa o por una norma.

- **Persistencia:** Propiedad de la información para que esta no se pierda.

Anexo

A continuación se muestra la guía realizada.

EL PAPEL DEL INFORMÁTICO COMO AUDITOR EN LA ISO 27001:2017

TECNOLOGÍA DE LA INFORMACIÓN
TÉCNICAS DE SEGURIDAD
SISTEMAS DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACION
REQUISITOS

GUIA DE APROXIMACIÓN PARA EL INFORMÁTICO

Por Jorge Asensi Shaw

ÍNDICE

1 INTRODUCCIÓN

La auditoría de sistemas de gestión de seguridad de la información vive un momento de gran trascendencia debido a los avances tecnológicos que han llegado a las empresas y a las organizaciones. En la actualidad, cualquier empresa cuenta con un sistema de red dónde se encuentran conectados una enorme cantidad de ordenadores y una base de datos con toda la información relacionada con la empresa, los trabajadores y los clientes. Esta información es el principal patrimonio de las empresas, dado que como dice la frase a la que muchos atribuyen al filósofo Francis Bacon: *"La información es poder"*. Esta se encuentra constantemente sometida a riesgos y amenazas, según ***"Privacy Rights Clearinghouse"***, en EEUU únicamente en el año 2018 se robaron 1.371 millones de documentos de datos personales, además, según la macroencuesta realizada por ***"EY Global Information Security Survey"*** a más de 1400 ejecutivos, que forman parte de compañías globales de reconocido prestigio *"el coste medio de filtraciones de información del año pasado fue de 3.620 dólares"*, por tanto, para garantizar la seguridad y su correcta gestión, es necesario implementar un Sistema de Gestión de Seguridad de la Información SGSI.

La norma internacional que especifica los requisitos necesarios para el establecimiento, la implantación, el mantenimiento y la mejora continua de un sistema de seguridad de la información es la norma **ISO/IEC 27001:2017 Tecnología de la información Técnicas de seguridad Sistemas de Gestión de la Seguridad de la Información Requisitos**. El encargado de verificar que esta norma se cumple rigurosamente, es el auditor de sistemas de gestión de la información, que es la figura física que constata la seguridad de la información. Mientras que la persona perteneciente a la empresa que debe velar para que esta norma se cumpla en la empresa es el responsable de sistemas de información.

En este documento se recogen las instrucciones necesarias para ejercer como auditor de sistemas de gestión de la seguridad de la información, que resultará de interés a cualquier profesional informático o recién titulado que quiera iniciarse en este campo. Se asume, que el lector posee un nivel básico de conocimiento informático para poder comprender algunos conceptos.

El objetivo fundamental de esta guía es invitar a los informáticos a iniciarse en el mundo de la auditoría de sistemas de gestión de seguridad de la información y mostrar la trascendencia y necesidad que tiene este campo actualmente en el mundo laboral.

2 NORMA DE GESTIÓN ISO 27001:2017

2.1 ¿QUÉ ES UN SISTEMA DE GESTIÓN?

Es un sistema que consta de una serie de procesos que se realizan sobre el conjunto de elementos que conforman una organización, para cumplir con los objetivos y políticas establecidos, mejorando aspectos tales como: productividad, costes, eficacia, etc.

2.2 ¿QUÉ ES UN SGSI?

Un Sistema de Gestión de Seguridad de la Información (SGSI), es según la norma ISO/IEC 27001:2017[1] *"una parte del sistema de gestión general, basada en un enfoque de riesgo empresarial, que se establece para crear, implementar, operar, supervisar, revisar, mantener y mejorar la seguridad de la información".* Tiene como objetivo mantener la confidencialidad, integridad y disponibilidad de los activos[2] de la información y a su vez minimizar los riesgos de seguridad que puedan sufrir las empresas u organizaciones. No obstante, es imposible alcanzar la seguridad absoluta en cualquier sistema, porque como dijo el experto estadounidense en ciberseguridad[3] Gene Spafford *"el único sistema verdaderamente seguro es aquel que se encuentra apagado, encerrado en una caja fuerte de titanio, enterrado en un bloque de hormigón, rodeado de gas nervioso y vigilado por guardias armados y muy bien pagados. Incluso entonces yo no apostaría mi vida por ello"*

Este sistema de gestión contiene, como el resto de sistemas, la información necesaria tanto de soporte como de las tareas que se efectúan (las políticas, la planificación, las responsabilidades, las prácticas, los procedimientos, los procesos y los recursos). Son activos de gran importancia para la empresa, donde garantizar su confidencialidad, integridad y disponibilidad es fundamental.

[1] **Norma ISO/IEC 27001:2017:** es una norma internacional que contiene las directrices enfocadas al correcto manejo de un sistema de gestión de la seguridad de la información

[2] **Activos de información:** Todos los recursos que traten información dentro de la organización y que tienen valor para la empresa

[3] **Ciberseguridad**: "Protección de activos de información, a través del tratamiento de amenazas que ponen en riesgo la información que es procesada, almacenada y transportada por los sistemas de información que se encuentran interconectados" ("ISACA Information Systems Audit and Control Association")

2.2.1 VISION POR PROCESOS

Un proceso *"es un conjunto de tareas lógicas relacionadas, que usan los recursos de la organización para proporcionar resultados, con el fin de alcanzar los objetivos de la empresa." fuente (apuntes asignatura SIO)*

A continuación se puede observar una visión esquemática que según la norma ISO/IEC 9001:2015[4] muestra la interacción entre los elementos de cualquier proceso:

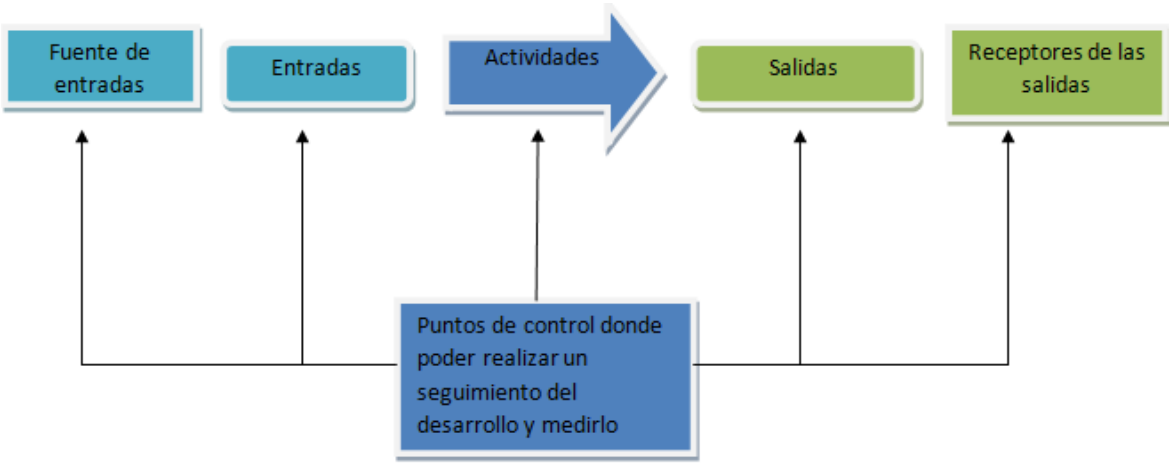

Ilustración 1 Esquema de cualquier proceso, según la norma ISO 9001:2015

Los procesos se pueden clasificar en tres tipos:

- **Procesos clave u operativos**: Aquellos que tienen un contacto directo con el cliente.
- **Procesos estratégicos o de gestión**: Son los encargados de analizar las necesidades que tiene la sociedad.
- **Procesos de soporte o de apoyo**: Su función es satisfacer a la empresa u organización en sus necesidades con respecto a personas, maquinaria y materia prima.

La gestión por procesos tiene la función de proporcionar a la empresa u organización, siguiendo tanto los procesos como la perspectiva del cliente, una estructura horizontal[5]. Esta gestión permite: evaluar las limitaciones que puede presentar la organización, identificar procesos críticos, necesidades del cliente,

[4] **Norma ISO:9001:2015 :** Norma que establece los requisitos necesarios para la correcta implantación de un sistema de gestión de calidad

[5] **Estructura horizontal**: Estructura organizada en procesos donde afectan a varios departamentos a la vez a diferencia de la vertical, división en departamentos, que es el sistema tradicional basado en tareas.

mejorar de forma global, además de medir el grado de satisfacción, entre otros aspectos.

2.2.2 PLAN-DO-CHECK-ACT

"Pon una buena persona en un mal sistema y siempre ganará el mal sistema"

W. Edwards Deming

PDCA de sus siglas en ingles ***"Plan-Do-Check Act"*** de traducción al castellano **"Planificar-Hacer-Verificar-Actuar"** también conocido como **"Ciclo de Deming"**, fue creado por **Edwards Deming**[6] a partir del concepto ideado por su mentor Walter A. Shewart, es un ciclo de mejora continua empleado en los sistemas de gestión de la calidad, constituido por cuatro fases que permiten a las empresas y organizaciones mejorar continuamente. Este ciclo es la base de los sistemas de gestión. Las fases previamente citadas son las que se muestran a continuación:

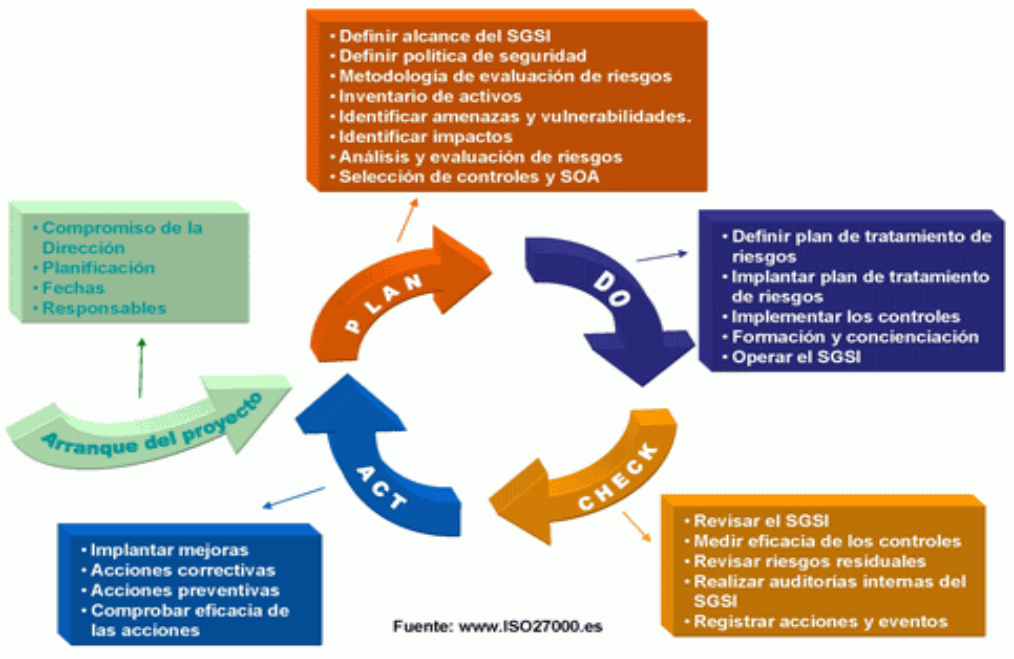

Ilustración 2 Esquema del ciclo PDCA

- **Planificar (Plan):** Esta fase constituye el establecimiento del sistema de gestión de seguridad de la información. Se estipulan el alcance, los objetivos, la organización que se va a llevar a cabo, las políticas, los medios, los activos disponibles, los riesgos… Y tras definir y estipular estos aspectos citados, se constituye el programa para la implantación del sistema de gestión.

[6] **Edward Deming** (1900-1993)**:** Fue un estadístico y profesor universitario, conocedor fundamentalmente por difundir el concepto de calidad total.

- **Hacer (Do):** Todos los aspectos definidos durante la planificación se ejecutan en esta fase, implementando y poniendo en funcionamiento el sistema de gestión de seguridad de la información.

- **Verificar (Check):** Se comprueba que todos los aspectos establecidos, definidos e implementados funcionan correctamente según lo constituido previamente mediante un proceso de monitorización y revisión.

- **Actuar (Act):** En esta fase se mejora el sistema de gestión de la seguridad de la información, corrigiendo los fallos detectados durante el proceso de monitorización y efectuando mejoras preventivas, contribuyendo de esta forma a un ciclo de mejora continua.

En conclusión, PDCA es un ciclo de mejora continua que permite a las empresas mejorar su sistema de gestión, además de ir mejorando continuamente, lo que posibilita a las empresas tener una alta probabilidad de éxito.

2.3 ¿QUÉ ES ISO?

ISO ("International Organization for standardization") en castellano la Organización Internacional de Normalización con sede central en Génova, Suiza *"es una organización para la creación de estándares*[7] *internacionales compuesta por diversas organizaciones nacionales de estandarización*."

Su fundación tiene lugar el 23 de febrero de 1947 por un conjunto de delegados procedentes de 25 países que decidieron crear una nueva organización para facilitar la coordinación y unificación de los estándares o normas en las industrias.

ISO es una organización independiente, no gubernamental con un total de 164 organismos nacionales de normalización, que participan en el desarrollo de las normas internacionales y que cubren una gran cantidad de campos. Como indica la página web oficial de ISO, se han publicado alrededor de 22683 estándares internacionales como es el estándar de la norma ISO/IEC 27001:2017.

Según la página web oficial de ISO, existen cuatro principios claves en el momento de desarrollar un estándar: responder a una necesidad del mercado, basarse en opiniones de expertos globales, desarrollar las normas mediante un proceso de múltiples partes interesadas y basarse en el consenso. Cualquier persona ya sea consumidora o forme parte del negocio, puede involucrarse en el desarrollo de estándares, formando parte del comité elegido por los miembros nacionales de la ISO.

[7] **Estándares:** Proporcionan especificaciones a nivel mundial para para todo tipo de productos servicios y sistemas, para garantizar la calidad la seguridad y la eficiencia.

2.4 ¿EN QUÉ CONSISTE LA NORMA ISO/IEC 27001?

La norma de gestión ISO 27001 de nombre completo **"ISO/IEC[8] 27001:2017 Tecnología de la información Técnicas de seguridad Sistemas de Gestión de la Seguridad de la Información"**, es una norma internacional que contiene las directrices enfocadas al correcto manejo de un sistema de gestión de la seguridad de la información, para preservar la confidencialidad e integridad de los datos y de la información, así como de los sistemas que la procesan.

Esta norma permite a cualquier tipo de empresa u organización, evaluar si cumple las condiciones necesarias para tratar los datos de una manera segura y correcta al implementar un sistema de gestión de la seguridad de la información. La norma ISO/IEC 27002:2013, *"especifica el sistema de controles aplicables a la seguridad de la información alineados a la norma ISO/IEC 27001:2017"* este sistema de control se encuentra en el anexo de la norma ISO/IEC 27001:2017.

Esta norma es certificable; tras la verificación de que se cumple la norma por parte de una entidad certificadora, se podría obtener el certificado. La norma ISO/IEC 27001:2017 es emitida por la Organización Internacional de Normalización (ISO).

Evidentemente el cliente se sentirá más seguro tratando con empresas certificadas bajo esta norma y para la propia empresa u organización, supondrá una mejora sustancial.

[8] **IEC**: "International Electrotechnical Commision" "Comisión electrotécnica Internacional" en castellano es una organización de normalización que trabaja conjuntamente con ISO en el desarrollo de una gran cantidad de normas.

2.5 ¿CÓMO ES LA ESTRUCTURA DE LA NORMA?

La norma se encuentra compuesta por diez puntos o capítulos además del prólogo, una breve introducción y el anexo, a continuación se realizará un breve resumen de cada uno de estos.

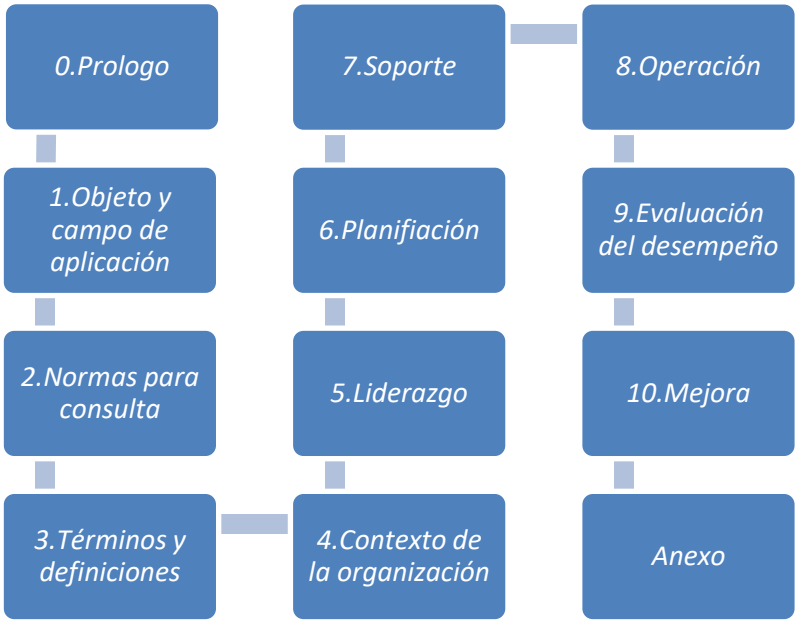

Ilustración 3 Esquema de la estructura de la norma ISO/IEC 27001:2017

1. ***"Objeto y campo de aplicación":*** En este punto se citan los contenidos de los que cuenta la misma, además indica que esta norma es aplicable a todo tipo de organización sin importar su tamaño, tipo o naturaleza.

2. ***"Normas para consulta":*** En este apartado se indica que la norma forma parte de la familia ISO/IEC 27000:2018.

3. ***"Términos y definiciones" :*** Se apunta que para mejor comprensión de la norma se usan los términos de la ISO/IEC 27000:2018

4. ***"Contexto de la organización":*** Hace referencia a varios aspectos de la organización que hay que tener en cuenta para implantar un sistema de gestión de la seguridad de la información. Primero, determinar aquellos aspectos tanto internos como externos relevantes de la organización; después, la misma debe identificar aquellas partes interesadas relevantes del SGSI y asegurarse de cumplir con sus requisitos, además debe determinar el alcance de este sistema en base a las necesidades de la empresa teniendo en cuenta las partes interesadas. Finalmente indica que la organización debe establecer los límites y la aplicabilidad del mismo.

5. ***"Liderazgo":*** En esta sección se informa de que la alta dirección debe demostrar su compromiso y liderazgo en todos aquellos aspectos relativos al sistema de gestión de la seguridad de la información, incluyendo: el cumplimiento de la política y los objetivos del mismo, asegurando los recursos necesarios, etc. También indica que la alta dirección debe establecer una adecuada política, incluyendo los roles y responsabilidades pertinentes para velar por la seguridad de la información.

6. ***"Planificación":*** En este capítulo se expone que la organización debe considerar todos los peligros que rodean el contexto de la información e identificar todos los riesgos y oportunidades que necesitan abordarse a fin de asegurar que se cumplan los objetivos planificados, reducir aquellos efectos no deseados y lograr la mejora continua. De igual modo, debe planificar la forma de cómo tratar los riesgos y oportunidades y evaluar la eficacia de esa forma. También se ha de implementar un proceso de manejo de riesgos para la seguridad de la información para evitar pérdidas, se debe conservar la información documentada sobre el proceso. La norma incita a la empresa a que se proponga objetivos y establezca una planificación para lograrlos.

7. ***"Soporte":*** En este punto se busca que la organización cuente con los recursos necesarios para lograr lo establecido en el punto anterior, incluyendo la competencia de las personas en lograr la seguridad de la información y la concienciación sobre la política y contribución de la seguridad de la información, además de las consecuencias de no cumplir con los requisitos del mismo.

   La organización debe comunicar activamente las políticas y objetivos de seguridad de la información, asegurando su cumplimiento y gestión constante, además de manejar y controlar toda la información documentada que respalde el sistema de gestión, incluyendo la requerida por la norma y la información que la organización ha considerado necesaria para lograr la efectividad del sistema.

8. ***"Operación":*** En este capítulo se ponen en marcha las medidas de seguridad de la información que se han definido en las etapas anteriores, concretando la fase del contexto de la organización (identificación de las partes interesadas) y la planificación (la forma de tratar los riesgos)

9. ***"Evaluación del desempeño":*** La organización debe evaluar el funcionamiento de la seguridad de la información y a su vez la eficacia del sistema de gestión de seguridad de la información; asimismo realizar auditorías internas en intervalos planificados. La alta dirección de igual forma debe revisar el cumplimiento del sistema de gestión de la seguridad

de la información y la organización tiene la responsabilidad de conservar la información documentada como prueba de los resultados de las revisiones por parte de la alta dirección.

10. ***"Mejora":*** Cuando se dé lugar a una no conformidad, la organización debe actuar ante ella, controlarla y corregirla intentando que no vuelva a ocurrir, mejorando de manera continua la eficacia del sistema de gestión de seguridad de la información.

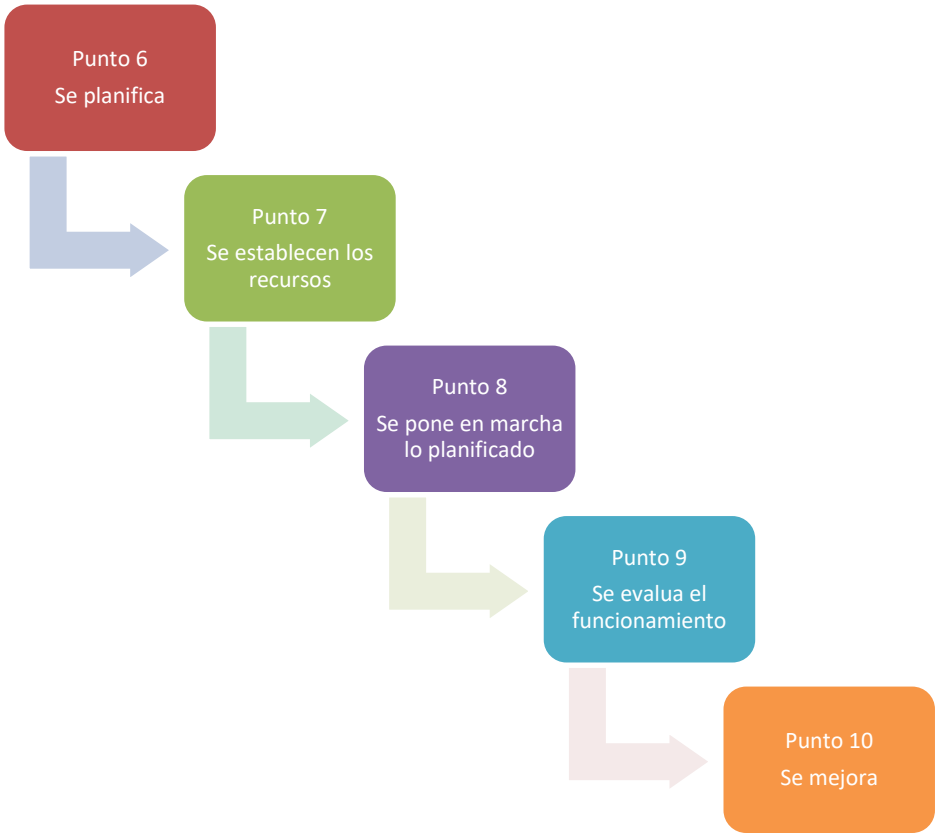

Ilustración 4 Síntesis de los puntos 6 al 10 de la norma ISO/IEC 27001:2017

2.6 ¿QUÉ REQUISITOS HA DE CUMPLIR?

La norma introduce una serie de requisitos sobre los que la empresa debe trabajar desarrollando el sistema de gestión de seguridad de la información. Seguidamente se explicaran algunos de los requisitos más destacables:

2.6.1 RESPONSABILIDAD Y AUTORIDAD

Tal y como indica la norma, concretamente en el capítulo 5 de la misma llamado *"Liderazgo",* la alta dirección de la organización debe asignar los roles pertinentes para asegurarse de que se lleve a cabo correctamente la implantación de un correcto sistema de gestión de la seguridad de la información.

Existe distintas técnicas para asignar roles, una de ellas es la llamada *"Matriz RASCI"* conocida como "matriz de asignación de responsabilidades" empleada para ayudar a asignar roles correctamente. *"RASCI"* hace referencia a *"**R**esponsible"* responsable de ejecutar la tarea, *"**A**ccountable"* responsable del proceso, *"**S**upport"* responsable del apoyo a un ejecutivo, *"**C**onsulted"* debe ser consultado antes de realizar la tarea y finalmente "*Informed":* responsable que debe ser informado de la realización de la tarea.

Un ejemplo de cómo es esta matriz es el siguiente:

Tabla 1 Ejemplo "Matriz RASCI"

RASCI Matrix Template							
Manager	TE	TE	VA	VA	VA	TE	VA
	Finanzas		Marketing			Producción	
Project Deliverable (or Activity) / Role	Juan Gris	Pedro Azul	Margarita Blanca	Rosa Roja	Carlos Amarillo	Rubén Marrón	Violeta Rosa
Nominas	**A/R**	R/S					
Presupuestos	R/S	**A/R**					
Generación	R/S	A/R					
Impresión	R/S	A/R					
Seguimiento	S	A/R					
Publicidad		C	S		**A/R**		
Contacto Clientes				**A/R**	S		
Eventos	I		**A**	**R**	S		
Organización			A	R			
Invitaciones			A	R			
Valorar resultados			A	R			
Introducción Nuevo Producto			S		**A/R**		
Soporte Producto A						**A/R**	S
Soporte Producto B						**A/R**	S
Soporte Producto C						**A/R**	S

2.6.2 POLÍTICAS

Se deben establecer unas políticas de seguridad de la información que estén disponibles para su consulta. Esta política debe adaptarse a la organización y debe ser revisada de forma continua. Un ejemplo de política sería que los usuarios solo pudieran acceder a la información estrictamente necesaria en el momento de realizar su trabajo o que se realicen copias de seguridad de los archivos de la empresa todos los días.

2.6.3 ANÁLISIS Y GESTIÓN DE RIESGOS

Esta norma requiere que la organización o empresa establezca una metodología para el análisis de riesgos de la seguridad de la información, estableciendo criterios sobre los mismos y evaluando las consecuencias de los riesgos encontrados. Este análisis se realiza porque, como se ha comentado anteriormente, la seguridad absoluta no existe. Siempre existe la posibilidad de que surja algún riesgo, por tanto en el momento que aparezcan hay que saber gestionarlos.

Existen distintas metodologías para el análisis de riesgos, una de las más famosas es *"MAGERIT"* dado que es desarrollada por el *"Consejo Superior de Administración Electrónica" CSAE* y en la que se basan algunas metodologías de análisis y gestión de riesgos, también existen otras como *"ENISA" , "PILAR".* etc. A continuación se mostrará una serie de fases seleccionadas por *"INCIBE"*[9] que como ellos afirman *"son comunes en la mayor parte de las metodologías para el análisis de riesgos".*

Ilustración 5 Fases del proceso de análisis de riesgos

- ***"Definir Alcance":*** En esta fase se define el alcance de este análisis de riesgos, la norma indica que lo debe definir la organización, un ejemplo sería los procesos de la escuela de informática.

- ***"Identificar activos":*** Tras definir este alcance, se identifican los activos de más trascendencia del mismo, en este caso que guarden relación con la escuela de informática. Por ejemplo realizando una tabla, un ejemplo de la clasificación de un activo sería el siguiente:

9 INCIBE: Es el "Instituto Nacional de Ciberseguridad en España" definida como "una sociedad independiente del Ministerio de Economía y Empresa a través de la Secretaria del Estado para el Avance Digital y consolidada como entidad de referencia para el desarrollo de ciberseguridad…"

Tabla 2 Ejemplo clasificación activo

Nombre del activo	Descripción	Departamento	Crítico
Base de datos de alumnos	Contiene el DNI, la dirección, las asignaturas cursadas y notas de los alumnos	Sistemas de información	Sí
Aula virtual	Contiene la documentación recursos y asignaturas de las tareas	General	Sí

- ***"Identificar amenazas":*** Después de identificar y clasificar los activos más importantes, se seleccionan e identifican las amenazas de los mismos, evidentemente hay una gran cantidad de amenazas, por tanto hay que ser prácticos y considerar amenazas posibles, es más probable que un servidor pueda ser destruido por un cortocircuito a que sea destruido por un rayo.

- ***"Identificar vulnerabilidades y salvaguardas":*** En esta se estudian los activos y se identifican las vulnerabilidades[10] y las salvaguardas[11] implantadas en la organización. Un ejemplo de vulnerabilidad sería un programa desactualizado y una salvaguarda un antivirus actualizado.

- ***"Evaluar el riesgo":*** Una vez identificados todos los factores anteriormente mencionados, se procede a calcular el valor de cada uno de los riesgos, mediante criterios tanto cualitativos como cuantitativos. Un ejemplo de clasificación es el siguiente:

10 **Vulnerabilidad**: Debilidad o fallo de un activo de información
11 **Salvaguarda**: Medida de seguridad, para proteger un activo

Ilustración 6 Ejemplo de clasificación de riesgos

Si se realiza un análisis cualitativo se realizará una matriz de probabilidad e impacto, mientras que si se realiza un análisis cuantitativo el nivel de riesgo según *"INCIBE"* se calcula: *"Riesgo = Probabilidad x impacto".*

- ***"Tratar el riesgo":*** Finalmente una vez se calcula el nivel de riesgo de cada uno de ellos, se deben tratar en función de unos criterios establecidos. Por ejemplo: se trataran aquellos riesgos que sean de nivel alto o superior (cualitativo), o nivel 4 o superior (cuantitativo), y se decide si contratar un tercero para arreglarlo, por ejemplo si se tiene un seguro, si el riesgo es elevado y el activo no es imprescindible se puede considerar la eliminación del activo, etc. Estas decisiones se deben realizar de manera justificada. Un ejemplo de riesgo sería una pérdida de datos y el tratamiento del mismo se llevaría a cabo realizando copias de seguridad.

Toda esta información recogida de los riesgos debe ser conservada por la organización.

2.6.4 OBJETIVOS Y ESTRATEGIAS

Se deben tener muy claros los objetivos necesarios de seguridad y cuáles serán las estrategias que se establecerán para lograr dichos objetivos. Estos objetivos tienen que ser coherentes con la política establecida y ser medibles, si es posible.

2.6.5 COMPETENCIAS

Hay que establecer las competencias necesarias y controlar que las personas responsables de hacer cumplir la norma estén suficientemente cualificadas. Por ejemplo mediante una matriz de competencias.

2.6.6 COMPROMISOS

La empresa u organización debe comprometerse y exigir los cambios pertinentes para cumplir con las normas de seguridad de la información motivando a los empleados.

2.7 ¿QUÉ BENEFICIOS APORTA A LA EMPRESA?

Los principales beneficios que aporta esta norma a la organización o empresa son los siguientes:

- **Reduce pérdidas de información:** El riesgo a la pérdida de datos o robos es reducido gracias a la implantación de esta norma.
- **Control exhaustivo;** Se lleva a cabo mediante controles de manera periódica.
- **Establecimiento de una metodología:** Permite gestionar la información de forma clara y concisa.
- **Medidas de seguridad:** Se establecen para el acceso de los clientes.
- **Mejora continua:** Gracias al SGSI, se realizan auditorías de manera periódica para identificar incidencias, lo que conlleva que el sistema de gestión de la seguridad de la información mejore continuamente.
- **Garantía:** Garantía de seguridad en el sistema de gestión de la información frente a los clientes y competidores.
- **Persistencia:** En caso de haber alguna incidencia permite que las operaciones sigan funcionando.
- **Cumplimiento con la legislación vigente:** Sobre la política de seguridad de la información.
- **Ventaja frente a la competencia:** Una empresa que obtiene esta certificación, siempre resultará más atractiva y segura al cliente.

- **Reducción de costes:** Y además un mejor funcionamiento de los procesos tras la implantación.

- **Optimización:** Tanto en recursos como en inversión tecnológica.

2.8 ¿A QUÉ EMPRESAS ES APLICABLE?

La norma ISO 27001:2017 es aplicable a cualquier empresa sin importar el tamaño de la misma ni la ubicación geográfica. Como se muestra en la **ilustración 7** se pueden observar empresas certificadas bajo la norma ISO 27001 de todo tipo. Por su parte, en la **ilustración 8** se muestran empresas certificadas bajo la norma ISO 27001 en todas las partes del mundo.

En la primera ilustración, el sector que tiene más certificados bajo esta norma es el sector de la información tecnológica. Los datos muestran en ambas el avance que está teniendo la certificación de esta norma, dado que cada año más empresas deciden implementar y lograr su certificación bajo la norma ISO 27001:2017, como se refleja claramente en la **ilustración 9**.

La fuente de todos los datos que se muestran a continuación son de la propia ISO.

ISO/IEC 27001 - Certificates by Industrial Sector

EA* Code Nos.	ISO/IEC 27001 BY INDUSTRIAL SECTOR	2006	2007	2008	2009	2010	2011	2012	2013	2014	2015	2016	2017
1	Agriculture, fishing	1	45	1	13	8	14	13	13	10	9	5	11
2	Mining and quarrying	0	1	3	6	2	12	31	34	25	8	9	7
3	Food products, beverages and tobacco	3	14	1	10	6	8	10	24	10	12	61	17
4	Textiles and textile products	0	1	1	3	3	2	12	10	4	10	132	11
5	Leather and leather products	0	0	0	1	2	5	1	2	0	1	1	2
6	Wood and wood products	0	0	0	1	3	5	4	4	1	12	12	12
7	Pulp, paper and paper products	2	6	6	7	4	7	13	17	15	9	10	12
8	Publishing companies	1	5	6	10	11	20	18	22	20	11	10	17
9	Printing companies	34	84	30	62	78	101	121	148	126	143	130	187
10	Manufacture of coke & refined petroleum products	3	6	9	8	3	5	4	14	10	4	3	7
11	Nuclear fuel	0	0	0	0	0	1	1	2	0	0	0	1
12	Chemicals, chemical products & fibres	7	3	3	9	9	9	11	24	12	10	18	20
13	Pharmaceuticals	0	1	3	4	6	3	0	3	6	6	9	9
14	Rubber and plastic products	7	5	0	10	15	16	16	36	14	16	32	36
15	Non-metallic mineral products	1	3	0	16	16	8	0	5	13	3	7	1
16	Concrete, cement, lime, plaster, etc.	1	1	1	6	6	14	27	25	26	13	17	7
17	Basic metal & fabricated metal products	10	5	2	16	25	28	36	50	42	37	51	50
18	Machinery and equipment	18	10	9	29	31	36	43	52	66	51	68	73
19	Electrical and optical equipment	38	58	50	135	221	280	342	289	287	296	311	316
20	Shipbuilding	0	0	2	5	3	3	4	8	4	1	2	
21	Aerospace	0	7	12	22	24	17	22	18	19	21	27	29
22	Other transport equipment	1	3	2	4	4	7	4	25	10	19	27	13
23	Manufacturing not elsewhere classified	4	14	2	5	5	23	8	5	7	6	13	22
24	Recycling	2	10	4	11	32	44	61	72	57	36	57	49
25	Electricity supply	8	10	11	20	9	12	15	45	38	34	61	87
26	Gas supply	0	2	2	4	3	2	6	6	10	10	12	25
27	Water supply	1	1	2	11	13	13	10	23	24	23	19	20
28	Construction	55	17	12	127	266	350	409	396	454	186	216	193
29	Wholesale & retail trade; repairs of motor vehicles, motorcycles & personal & household g	12	38	26	93	164	214	215	224	206	198	202	283
30	Hotels and restaurants	2	4	0	6	10	32	4	5	2	6	7	10
31	Transport, storage and communication	60	70	63	170	184	241	288	322	327	301	401	930
32	Financial intermediation, real estate, rental	47	54	68	148	185	113	138	169	187	197	250	344
33	Information technology	890	1236	1152	2086	3217	3588	4558	5059	4933	5573	6578	7478
34	Engineering Services	25	33	48	173	122	126	189	211	217	201	245	382
35	Other Services	189	204	228	380	579	564	755	849	867	959	1432	1369
36	Public administration	23	33	79	181	79	106	155	192	191	212	235	185
37	Education	8	9	25	47	75	65	102	101	83	104	109	54
38	Health and social work	14	10	61	102	102	145	201	201	215	231	220	216
39	Other social services	8	13	16	46	54	75	98	106	102	125	163	105
TOTAL		1475	2016	1940	3987	5579	6314	7945	8811	8640	9094	11162	12590

Ilustración 7 Empresas certificadas en la norma ISO 27001 en los distintos sectores industriales

ISO/IEC 27001 - 1					
Year	**2013**	**2014**	**2015**	**2016**	**2017**
TOTAL	**21604**	**23005**	**27536**	**33290**	**39501**
Africa	99	79	129	224	301
Central / South America	272	273	347	564	620
North America	712	814	1445	1469	2108
Europe	7952	8663	10446	12532	14605
East Asia and Pacific	10116	10414	11994	14704	17562
Central and South Asia	2002	2251	2569	2987	3382
Middle East	451	511	606	810	923

Ilustración 8 Empresas certificadas bajo la norma ISO 27001 en las distintas zonas del mundo

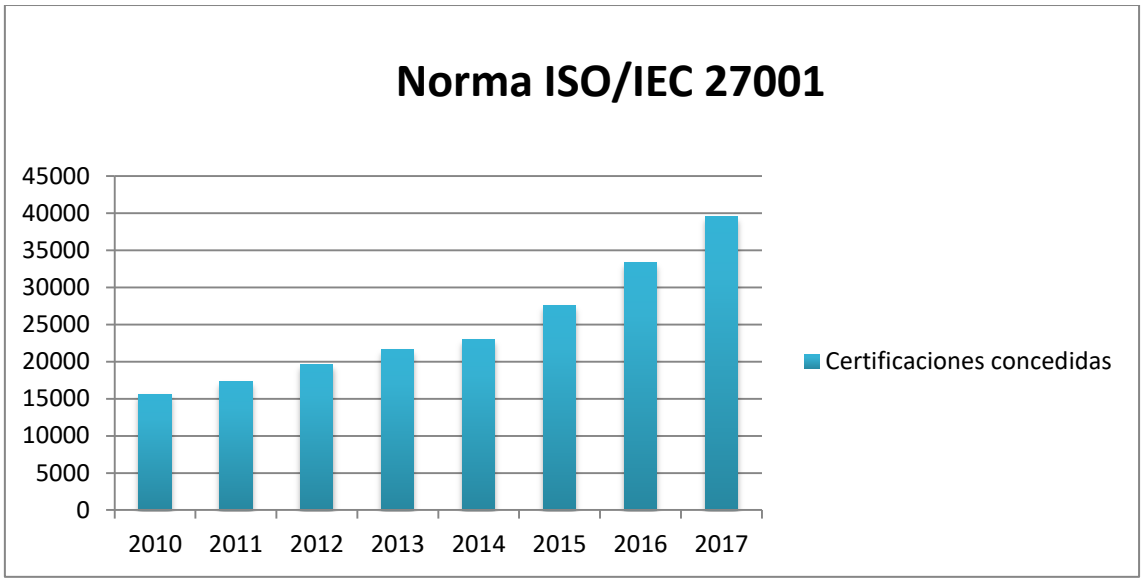

Ilustración 9 Gráfica de certificaciones ISO/IEC 27001 de 2010 a 2017 fuente ISO

De 2010 a 2017 se puede observar como el número de certificaciones concedidas de la norma ISO 27001:2017 ha ido aumentando gradualmente, llegando a alcanzar un número elevado de certificaciones en el año 2017, rozando las 40000 concretamente 39501.

3 EL INFORMÁTICO COMO AUDITOR

3.1 ¿QUÉ ES LA AUDITORÍA?

La auditoría es un proceso sistemático de carácter objetivo, que consiste en analizar y evaluar un entorno junto con sus componentes así como, determinar el cumplimiento con la metodología y requisitos establecidos por una norma o unos criterios determinados.

A continuación, se muestran definiciones de este concepto por la norma ISO 9001 y la Real Academia Española de la lengua:

Norma ISO 9001:2015: *"Es el proceso sistemático, independiente y documentado para obtener evidencias objetivas y evaluarlas de forma objetiva para determinar el grado en que se cumplen los criterios de auditoria".*

El diccionario de la Real Academia Española de la lengua (RAE) establece las siguientes definiciones para este término:

> 1 *"Revisión sistemática de una actividad o de una situación para evaluar el cumplimiento de las reglas o criterios objetivos a aquellas que deben someterse".*
> *2 "Revisión y verificación de las cuentas y de la situación económica de una empresa o entidad".*
> *3 "Empleo de auditor".*
> *4 "Tribunal o despacho del auditor".*

La definición establecida por la norma y la primera de la RAE, son las dos que mejor describen este término, puesto que ambas coinciden en su descripción como una revisión o proceso sistemático, así como en su utilidad para evaluar.

La auditoría es un proceso primordial para las empresas, puesto que les permite mantenerse en continuo control y en consecuencia en una continua mejora, localizando y corrigiendo sus puntos flacos, sus debilidades y amenazas, y así alcanzar los objetivos de la empresa. La auditoría puede ser tanto de carácter obligatorio como de carácter voluntario.

Una vez explicado en qué consiste la auditoría en general, se explicará que es una auditoría de sistemas de gestión de la seguridad de la información:

Una auditoría de sistemas de gestión de la seguridad de la información, es un proceso sistemático que consiste en evaluar de manera objetiva dicho sistema bajo unos criterios definidos. La norma que rige estos criterios es la norma ISO/IEC 27001:2017.

3.1.1 ¿QUÉ ES UN AUDITOR?

Un auditor es el encargado de **realizar la auditoría y verificar** que los requisitos establecidos por una empresa o los que dicta una norma se cumplen.

La Real Academia Española de la lengua determina las siguientes **definiciones con respecto al auditor:**

> *1"Que realiza auditorías".*
> *2 "Persona nombrada por el juez entre las elegidas por el obispo o entre los jueces del tribunal colegial, cuya misión consiste en recoger laspruebas y e ntregárselas al juez, si surge alguna duda en el ejercicio de su ministerio".*
> *3. "oyente".*

De las tres definiciones de la RAE, la que más se ajusta al concepto “auditor”, es la primera. No obstante, es destacable también la tercera ya que define una de las cualidades fundamentales que debe tener un auditor, que es ser “oyente”.

Un auditor debe ser un gran conocedor de la materia sobre la que audita, dado que sobre él recae la responsabilidad de la correcta realización de la auditoría. No obstante, además de tener los conocimientos necesarios, también debe contar con habilidades como: una actitud positiva, buenas dotes de liderazgo, tener una mente analítica, tener iniciativa y como se ha comentado anteriormente ser oyente y por consiguiente saber escuchar.

Un auditor de sistemas de gestión de la seguridad de la información es un profesional altamente cualificado, que aparte de conocer las directrices establecidas por la norma UNE-EN ISO/IEC 19011:2018 debe contar con altos conocimientos en el manejo de estos sistemas y evidentemente de la norma ISO 27001:2017.

3.1.2 ¿QUÉ TIPOS DE AUDITORÍA HAY?

Existen distintos tipos de auditoría con respecto al contenido: auditorías financieras, de gestión, operativa… En esta guía siempre se tratará la auditoría teniendo como referencia los sistemas de gestión de la seguridad de la información. Por tanto al explicar los tipos de auditoría se realizará, con respecto al sujeto que efectúa la auditoría.

La auditoría consta de tres tipos distintos: de primera parte, de segunda parte y de tercera parte, y con sus respectivos tipos de auditor. Tanto los auditores de segunda como de tercera son externos. En la siguiente tabla extraída de la norma ISO 19011:2018 *“Directrices para la auditoría de los sistemas de gestión”* se muestran explicadas brevemente las auditorías mencionadas.

Tabla 3 Tipos distintos de auditoría

Auditoría de primera parte	Auditoría de segunda parte	Auditoría de tercera parte
Auditoría interna	Auditoría externa de proveedor	Auditoría de certificación y/o acreditación
	Otra auditoría externa de parte interesada	Auditoría legal, reglamentaria o similar

A continuación se explicará de una manera clara estos distintos tipos de auditoría y auditores citados.

- AUDITORÍA INTERNA O PRIMERA PARTE

La auditoría interna o de primera parte, consiste en la realización del proceso de auditoria por, o en nombre de la empresa sobre la que se audita. Como establece la norma ISO 19011:2018: *"la independencia es la base de la imparcialidad"*, por tanto el auditor interno o de primera parte que realice este tipo de auditoría deberá ser independiente de la función que se audita. Sin embargo, hay organizaciones pequeñas donde puede que no siempre se cumple esa independencia respecto a la actividad que auditan, debiendo eliminar ese sesgo para ser totalmente objetivos.

Según "The Institute of Internal Auditors" la auditoria interna es: "*una actividad de aseguramiento y consultoría objetiva e independiente diseñada para agregar valor y mejorar las operaciones de una organización, ayudando a la organización a alcanzar sus objetivos aportando un enfoque sistemático y disciplinado con el fin de evaluar y mejorar la eficacia de los procesos de gestión de riesgos, control y gobierno*".

El trabajo que debe realizar el auditor interno esencialmente, es comprobar que el SGSI funciona y está implementado de acuerdo con lo establecido en la norma ISO 27001:2017. Y elaborar un informe para la empresa sobre la que audita, sirviendo únicamente como asesoramiento o guía para la propia empresa.

- AUDITORÍA EXTERNA: AUDITORÍA DE SEGUNDA PARTE Y TERCERA PARTE

La auditoría externa, consiste en la realización del proceso de auditoria por agentes externos a la empresa sobre la que se audita, a este sujeto se le llama auditor externo.

El auditor externo no guarda absolutamente ningún vínculo con la empresa a auditar y es contratado por una empresa externa.

El alcance de trabajo que debe realizar el auditor externo debe ser coherente con el programa de auditoría. El informe es elaborado por el auditor de una manera completamente objetiva incluyendo sugerencias que se pueden implementar para

ayudar a que la empresa mejore. Este tipo de auditoría, al ser realizada por terceros tiene un grado de altísima credibilidad y se puede dar fe pública de ella.

Hay dos tipos de auditoría externa:

a. AUDITORÍA DE SEGUNDA PARTE

Las auditorías de segunda parte son realizadas por organizaciones que tienen un interés o relación con la empresa que se va a auditar, tales como clientes o proveedores.

b. AUDITORÍA DE TERCERA PARTE

Las auditorias de tercera parte las llevan a cabo organizaciones auditoras independientes y completamente externas a la organización, como las que otorgan certificaciones.

Seguidamente se muestra una tabla con las principales diferencias entre la auditoría interna o de primera parte y la auditoría externa:

Tabla 4 Principales diferencias entre auditoría interna y auditoría externa

Criterio	Auditoría Interna	Auditoría Externa
Realización	Personal de la empresa	Personal ajeno a la empresa
Objetivo	En función de los requerimientos de la empresa y se realiza como parte de trabajo de la misma	Obtener certificados
Informe	Para la gestión de la empresa	Para la posterior obtención de la certificación en caso de informe positivo.
Información	Para la propia empresa	Empleada por personas ajenas a la empresa

3.2 ¿QUÉ COMPETENCIAS Y CONOCIMIENTOS SE DEBE TENER?

Un auditor de sistemas de gestión de la seguridad de la información, debe tener una serie de conocimientos y competencias: conocer la norma UNE-EN ISO 19011:2018 *"Directrices para la auditoría de sistemas de gestión"* para actuar correctamente en una auditoría, conocimientos de gestión e informática, y evidentemente conocimiento total de la norma ISO 27001:2017 para desempeñar la función de auditor de sistemas de gestión de la seguridad de la información.

3.2.1 COMPETENCIAS

Las competencias que debe tener un informático para ejercer como auditor de sistemas de gestión de la seguridad de la información son las siguientes.

- **GENERALES:** El auditor de sistemas de gestión de la información debe conocer una serie de principios procesos y métodos que todo buen auditor de sistemas de gestión conoce para realizar las auditorias de manera congruente y metódica.

  El auditor debe saber planificar y organizar el trabajo de una manera eficaz, dado que una buena planificación da lugar a una alta probabilidad de éxito en la correcta realización de la auditoría. Además, con una buena planificación, normalmente la auditoría se realiza en el plazo establecido y acordado, que es un requisito esencial. El auditor debe establecer una escala de prioridades con respecto a la materia a auditar y centrarse primordialmente en aquellas que tengan una mayor trascendencia.

  Evidentemente, como se ha comentado anteriormente en esta guíal, el auditor debe saber comunicarse tanto de forma oral como escrita eficazmente.

  Durante el proceso de auditoría, el auditor debe recopilar toda la información necesaria y posteriormente revisarla así como verificarla, además de tener en cuenta las opiniones de los técnicos altamente cualificados.

  En el proceso de elaborar el informe, las conclusiones y los hallazgos han de estar sustentados por una evidencia indicándolo de una manera concisa y clara, manteniendo la confidencialidad y seguridad de la información.

- **ESPECÍFICAS**

  - Mezcla de conocimientos de gestión y de informática en general, tales como:

    - Gestión de Proyectos
    - Administración del Departamento de informática
    - Análisis de riesgos en un entorno informático
    - Sistemas Operativos
    - Redes y Telecomunicaciones
    - Bases de Datos
    - Seguridad Informática
    - Comercio Electrónico
    - Ofimática
    - Administración de datos
    - Administración del cambio
    - Encriptación de datos

  - Ser un experto conocedor de la norma UNE-EN ISO/IEC 27001:2017.

  - Conocer los procesos y productos, incluyendo los servicios, permitiendo así al auditor entender el contexto tecnológico donde se está llevando la auditoría.

    - La terminología específica del sector informático.
    - Las características técnicas de los procesos y productos.
    - Los procesos y las prácticas específicas de la informática.

  - Conocer técnicas de administración de empresas y de cambio.

3.2.2 PRINCIPIOS DE AUDITORÍA

La auditoría es un proceso que requiere objetividad y responsabilidad por parte del auditor que la realiza, para cumplir con estos requisitos principales, se debe obedecer un conjunto de principios establecidos por la UNE-ISO 19011.

- **INTEGRIDAD:** Los auditores y el personal encargado del programa de auditoría deben:

    - Desempeñar su trabajo de forma ética, honesta y responsable
    - Realizar las actividades de auditoría si son lo suficientemente competentes
    - Ser ecuánimes

- **VERACIDAD:** Todos los informes, revelaciones y resultados durante la auditoría deberán evidenciar autenticidad y certeza, del mismo modo que el comportamiento y la comunicación del auditor.

- **DILIGENCIA Y JUICIO AL AUDITAR:** El auditor debe tener la aptitud de hacer juicios razonados durante la auditoría, además de proceder con escrupulosidad en las actividades que realice.

- **CONFIDENCIALIDAD:** El auditor deberá actuar con sutileza en el manejo de la información, no empleando el uso de la misma para obtener beneficios propios o para el cliente, de modo que damnifique los objetivos del auditado.

- **IMPARCIALIDAD E INDEPENDENCIA:** Los auditores deben ser ajenos a la actividad a auditar y actuar de forma libre e independiente.

- **EVIDENCIA: METODO RACIONAL:** Las conclusiones de la auditoría deberán ser constatables. En general deberán basarse en muestras de la información disponible.

3.3 PAUTAS DE ACTUACIÓN DEL AUDITOR EN LA AUDITORÍA

Hasta ahora se ha explicado que es un auditor, la auditoría y los tipos de auditoría. A continuación se explicará el procedimiento a realizar por el auditor en base a la norma ISO 19011:2018, que consta de varias fases:

- **Fase de Planificación**
    - **El primer paso consiste en establecer contacto con la empresa que desea ser auditada asegurándose de:** Establecer las comunicaciones directamente con el auditado o con sus representantes, confirmando que tiene la autoridad para llevar a cabo la auditoría. Además, facilitar toda la información necesaria de los objetivos, el alcance, los criterios, los métodos, el equipo auditor y los técnicos altamente cualificados que van a trabajar en la auditoría. Evidentemente, el auditor debe solicitar el acceso a la información necesaria para poder llevar a cabo la planificación y determinar los requisitos legales y reglamentarios entre otros. Finalmente confirmar el tratamiento de la información confidencial con el auditado, establecer el calendario y otros aspectos concretos como la ubicación y asistentes para el equipo auditor.

- **El segundo paso consiste en determinar la viabilidad de la auditoría:** Para así poder asegurarse de que los objetivos se cumplan teniendo en cuenta los siguientes factores: que la información obtenida sea necesaria, que se tenga la cooperación del auditado y verificar si el tiempo y los recursos son los adecuados para lograr la auditoría.

- **Planificación de las actividades**

  El proceso de planificación de las actividades se llevará a cabo de la siguiente manera.

  - Realizando un proceso de revisión de la información documentada en relación al sistema de gestión que emplea la empresa auditada.

  - Analizando los riesgos de las actividades de auditoría y realizando una planificación para lograr una programación de tiempo y coordinación eficientes, con el fin de lograr los objetivos de manera eficaz

  - La planificación debe ser lo suficientemente flexible como para permitir cambios necesarios conforme se vayan realizando las actividades.

  - El líder del equipo auditor debe asignar a cada miembro del equipo las funciones correspondientes, incluso en algunos casos, la función de toma de decisiones. Realizando estás asignaciones desde la completa imparcialidad. No obstante, cada cierto tiempo el líder del equipo auditor debe convocar reuniones para reasignar tareas en caso de haber cambios.

  - Recopilar información pertinente a las tareas asignadas y preparar esa información, la cual se deberá conservar al menos hasta que haya finalizado la auditoría.

- **Realización de las actividades planificadas**

  - Las actividades se realizan de manera secuencial. Siempre que el líder del equipo auditor, el auditado o el cliente lo permita. Tanto los guías como los observadores pueden acompañar pero no interferir en la realización; en caso de que el líder del equipo auditor tenga la

sensación de que este hecho no se puede asegurar, podrá negar la entrada a los guías y observadores durante la auditoría.

- Habrá una reunión de apertura para comunicar que se está realizando la auditoría y para confirmar los siguientes aspectos:

  - Unanimidad con respecto al plan de auditoría.
  - Presentar al equipo auditor y sus roles.
  - Asegurar que se puede realizar todo lo planificado.

- Durante la realización de la auditoría se debe comunicar periódicamente el estado del proceso, así como cualquier tipo de imprevisto o error que pueda surgir durante la misma.

- Revisar la información documentada durante la auditoría y verificarla. El proceso que se lleva a cabo es el siguiente:

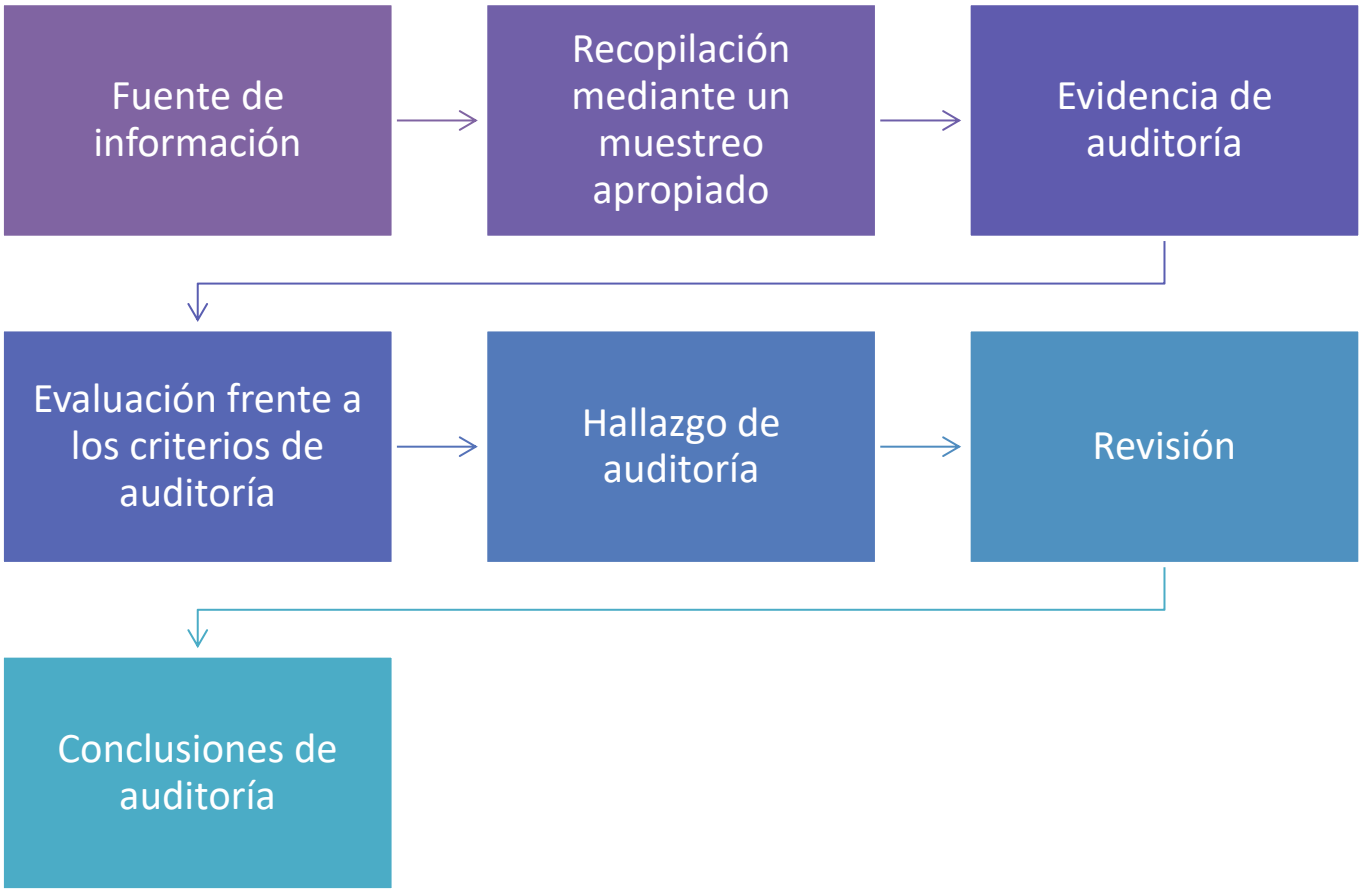

Ilustración 10 Proceso típico de recopilación y verificación de información (fuente: UNE-EN ISO 19011:2018)

- Determinar las conclusiones de la auditoría y presentarlas mediante una reunión de cierre; esta reunión será presidida por el líder del equipo auditor y los representantes del auditado. Deberán estar presentes así mismo los responsables de los procesos que se hayan auditado, el cliente, el resto de miembros del equipo auditor y otras partes interesadas.

- **Elaboración del informe de la auditoría:** El líder del equipo auditor elaborará un informe, donde se proporcionará un registro completo, riguroso, breve y claro de la auditoría, donde se hará referencia a: los objetivos, el alcance, la identificación del cliente, el equipo auditor y los participantes, las fechas, los criterios… Finalmente este informe se emitirá en el periodo de tiempo acordado, en caso de retraso las razones se deberán comunicar al auditado.

- **Finalización de la auditoría:** La auditoría finaliza una vez realizadas todas las actividades o por mutuo acuerdo con el cliente. La información documentada se deberá conservar o eliminar si las partes participantes están conformes. Además está información, en caso de que no se requiera por ley, no debe ser revelada sin la aprobación explícita del cliente.

3.4 ¿CÓMO OBTENER LAS COMPETENCIAS?

Se han explicado las competencias y requisitos que debe tener un informático para ejercer como auditor de sistemas de gestión de la seguridad de la información, pero ¿Cómo se obtienen estas competencias? Se pueden obtener mediante formación y experiencia en una empresa o mediante cursos. Evidentemente un curso, con posterior certificado, es más recomendable. El auditor que trabaja por parte de la entidad de certificación[12] es el auditor externo.

IRCA *International Register of Certificated Auditors* es un organismo a nivel mundial de certificación para auditores de sistemas de gestión, con sede en Reino Unido, que cuenta con distintos cursos tales como: **auditor interno provisional,** para empezar en el mundo de auditoría; **auditor interno,** adecuado para iniciarse y especializarse en auditorías internas; **auditor,** orientado a personas que han asistido a algún curso pero nunca han realizado una auditoría; **auditor jefe,** enfocado para profesionales que quieran adquirir un conocimiento avanzado y finalmente; **auditor principal,** curso para profesionales con una gran experiencia y conocimiento avanzado. No obstante, en caso de duda, la propia página web de IRCA cuenta con un cuestionario para indicarte cual es el curso más adecuado.

[12] **Certificación: La prueba que acredita a una empresa u organización el cumplimiento de una norma**

Estos cursos son impartidos tanto por IRCA como por entidades acreditadas por la propia IRCA, como es el caso de *Bureau Veritas Iberia*, donde el curso de auditor jefe tiene un precio de 1020 euros y dura 40 horas – 5 días. Los cursos acreditados por IRCA tienen la siguiente marca:

Además de los cursos IRCA, hay otras entidades de certificación acreditadas que ofrecen cursos, entre ellas se encuentra AENOR[13].

AENOR dispone de los siguientes cursos: **auditor interno ISO 27001,** este curso tiene como objetivos enseñar los conocimientos necesarios para la planificación y realización de auditorías de sistemas de gestión de la seguridad de la información y todo lo que le envuelve, tiene una duración de 2 días de 9:00 a 18:00 y un precio de 760 euros + 21% de IVA. **Auditor líder ISO 27001,** este curso está enfocado a adquirir unos conocimientos muy avanzados de auditoría, tiene una duración de 5 días con horario de 9:00 a 18:00 y un precio de 1665 euros + 21% de IVA.

Curso	Precio (IVA no incluido)	Duración	Requisitos
Auditor líder ISO 27001	1665 euros	5 días 35 horas	Haber realizado los cursos de: S-01[14] S-02[15] S-05[16]
Auditor interno ISO 27001	760 euros	2 días 14 horas	S-01 S-02

Ilustración 11 Especificaciones cursos "*AENOR*"

13 AENOR: Certificadora acreditada española.
14 Curso: Fundamentos de la gestión de la seguridad de la información según ISO 27002
15 Curso: Implantación de un sistema de gestión de la seguridad de la información según ISO 27001
16 Curso: Auditor Interno ISO 27001

3.5 HERRAMIENTAS DE AUDITORÍA

La auditoría cómo se ha explicado en esta guía, es un proceso complejo que requiere seguir una serie de pautas para su correcta realización. Alguna de las herramientas de auditoría que facilitan la realización del mismo son:

3.5.1 PROGRAMA DE AUDITORÍA

El programa de auditoría es el resultado principal de la fase de planificación y contiene todas las actividades que se van a realizar en la auditoría y que se han establecido durante esta fase. Por tanto, El objetivo principal de esta herramienta es ayudar a los miembros de la auditoría a llevar un orden controlado de todas las actividades hechas y las que restan por ejecutar, comprobando si se están ejecutando tal y como se había estipulado durante la fase de planificación.

3.5.2 CHECKLIST

Los checklist son fundamentales en el momento de afrontar una auditoría, su finalidad es realizar una serie de preguntas que deben estar relacionadas con los requisitos de la norma a auditar, recopilando así las pruebas suficientes para asegurar si el proceso auditado cumple con unos requisitos definidos. Se adjunta un ejemplo de checklist en el anexo.

3.5.3 INFORME DE AUDITORÍA

El informe de auditoría es el resultado del trabajo realizado por el auditor, en este documento se exponen las conclusiones obtenidas tras la realización completa de la auditoría. Este documento es muy importante, ya que permite conocer el estado en el que se encuentra la empresa con respecto a la auditoría. Los informes de auditoría tienen una estructura definida con respecto al contenido del mismo.

En la siguiente ilustración se observa un ejemplo de informe de auditoría:

Número auditoría	Fecha auditoría
Área/Proceso clave auditado	
Auditor	
Grupo auditor	

Hallazgos detectados:

Requisito de la norma	Hallazgos	No conformidad	Observación

Comentarios

Elaborado por	Nombre	Fecha	Firma
Revisa y aprueba	Nombre	Fecha	Firma

Ilustración 12 Ejemplo informe de auditoría procedente de la guía de implantación de la norma ISO 27001 AENOR

4 LA CERTIFICACIÓN Y SU FUNCIONAMIENTO

La prueba que acredita a una empresa u organización el cumplimiento de una norma, es el certificado obtenido tras el proceso de certificación, realizado por una certificadora.

La certificadora es una entidad externa que se encarga de verificar que el servicio o producto de una empresa u organización, cumple con una serie de requisitos estipulados bajo una norma, como por ejemplo la ISO/IEC 27001:2017.

Para poder ejercer como certificadora, la entidad debe estar acreditada. La entidad encargada de realizar la acreditación en España es *ENAC*.

La Entidad Nacional de Acreditación *ENAC* : *"es la entidad designada por el Gobierno, para operar en España como el único Organismo Nacional de Acreditación, en aplicación del Reglamento (CE) nº 765/2008 que regula el funcionamiento de la acreditación en Europa."*

En España, actualmente hay seis certificadoras acreditadas para de la norma ISO/IEC 27001:2017 según establece *ENAC* y son las siguientes:

- **AENOR INTERNACIONAL, S.A. (Unipersonal)**
- **BUREAU VERITAS IBERIA, S.L.**
- **IGC CERTIFICACIÓN GLOBAL, S.L. (Unipersonal)**
- **IVAC-INSTITUTO DE CERTIFICACIÓN, S.L.**
- **LGAI TECHNOLOGICAL CENTER, S.A (APPLUS)**
- **OCA Instituto de certificación, S.L (Unipersonal) (OCA GLOBAL)**

La certificación, según la propia *AENOR* INTERNACONAL es : *"el proceso llevado a cabo por una entidad reconocida como independiente de las partes interesadas, mediante el que se manifiesta la conformidad de una determinada empresa, producto, proceso servicio o persona con los requisitos definidos en normas o especificaciones técnicas. La certificación va dirigida a cualquier tipo de empresa, independientemente de su tamaño, ubicación o área de actividad."* La certificación es un proceso voluntario.

Para llevar a cabo el proceso de certificación, la empresa debe solicitar el certificado a una entidad certificadora acreditada y esta entidad se encarga de recoger la información necesaria para asignar al equipo auditor adecuado y determinar el tiempo en que se realizará la auditoría. Las fases que comprenden este proceso son las siguientes:

- **FASE 1: REVISIÓN DE DOCUMENTACIÓN**
  En esta fase el equipo auditor analiza si la empresa cumple todos los requisitos de la norma. Si cumple todos los requisitos, el equipo auditor

realiza un informe favorable y se lo transmite a la empresa para que solicite la certificación, si por el contrario detectaran fallos leves, deberían corregirse antes de la siguiente fase. Por último, en caso de fallos graves se le transmitiría a la empresa la imposibilidad de conseguir el certificado actualmente.

- **FASE 2 AUDITORÍA DE CERTIFICACIÓN**
  El equipo auditor verificará si la empresa cumple con todos los requisitos de la norma y si los auditores detectan que no hay disconformidades, se le concederá el certificado a la empresa.

5 BIBLIOGRAFÍA

INFORMACIÓN

[0] John Bendermarcher. "*Perspectivas y percepciones globales. Auditoría Interna y auditoría externa [en línea]"*. THE INSTITUTE OF INTERNATIONAL AUDITORS. Edición 8. Fecha de Publicación: Noviembre de 2017.

Disponible en: https://na.theiia.org/translations/PublicDocuments/GPI-Distinctive-Roles-in-Organizational-Governance-Spanish.pdf

[1] ISO International Organization for Standarization. All about ISO

Disponible en:

https://www.iso.org/home.html

[2] Gerencie.com. "*Diferencias entre auditoría interna y externa*" *Gerencia.com*. Fecha del artículo 13: Octubre 2017.

Disponible en: https://www.gerencie.com/diferencias-entre-auditoria-interna-y-externa.html

[3] IRCA International Register of Certificated Auditors

Disponible en: https://www.quality.org/IRCA-grades

[4] Quintero Arias, Andrés. Conclusiones y Lecciones Aprendidas. *Auditoría informática*. Fecha del artículo: 22 de Noviembre 2015.

Disponible en: https://chaui201521701020289.wordpress.com/

[5] Aguilar Escobí, Maria Amparo. Plan de auditoría del desarrollo de aplicaciones en una empresa informática . Fecha. 25 de Junio de 2012.

Disponible en: https://riunet.upv.es/handle/10251/16268

[6] ISOTools [en línea].

Disponible en: https://www.isotools.org/

[7] ISOTools Excellence. La norma ISO 27001 para los Sistemas de Gestión de Seguridad de la Información. *SGSI Blog especializado en Sistemas de Gestión de Seguridad de la Información*. Fecha de publicación: 28 Febrero 2019.

Disponible en: https://www.pmg-ssi.com/2019/02/sistemas-de-gestion-de-seguridad-de-la-informacion/

[8] Muñoz Martín, Manuel, "*Guía de implantación de un SGSI basado en la norma UNE-ISO/IEC 27001"*. Universitat Oberta de Catalunya. Junio de 2015

Disponible en: http://openaccess.uoc.edu/webapps/o2/bitstream/10609/42965/7/mmanozTFC0615memoria.pdf

[9] ENAC Entidad Nacional de Acreditación.

Disponible en: https://www.enac.es/

[10] AENOR. ¿En qué consiste la certificación?

Disponible en: https://www.aenor.com/certificacion/en-que-consiste-la-certificacion

[11] Agencia Estatal de Administración Tributaria*. "Auditoría informática en la administración: un reto para los profesionales de TIC"*. Fernando Rodríguez Rivadulla. 2 Junio 2006.

Disponible en:

https://administracionelectronica.gob.es/pae_Home/dam/jcr:e24c6a42-52ef-4963-ace6-256ad9a817d6/auditoria_informatica.pdf

[12] Germán E. Chávez S. Auditoría Informática Manual Para Estudiantes. 1ra edición – Barinas. 2014.

Disponible en:

https://chaui201521701020289.files.wordpress.com/2015/11/auditoria-informc3a1tica-manual-para-estudiantes.pdf

[13] AENOR. Guía de implantación de la norma UNE-ISO/IEC 27001 sobre seguridad en sistemas de información para pymes. Luis Gómez Fernández y Ana Andrés Álvarez. 2ª Edición.

[14] INTECO Instituto Nacional de Tecnologías de la Comunicación. Implantación de un SGSI en la empresa.

Disponible en:

https://www.incibe.es/extfrontinteco/img/File/intecocert/sgsi/img/Guia_apoyo_SGSI.pdf

[15] El portal de ISO 27001 en español.

Disponible en:

http://www.iso27000.es/index.html

[16] *Hablemos de empresa. "El 87€ de las empresas no puede hacer frente a las amenazas digitales".* Marcos Martínez. fecha: 21 de Marzo de 2019

Disponible en: https://hablemosdeempresas.com/empresa/ciberseguridad-en-pymes/

[17] *EY. EY Global Information Security Survey*

Disponible en: https://www.ey.com/es/es/home/ey-global-information-security-survey-2019

[18] Pontifica Universidad Católica del Perú. "*Sistema de gestión de seguridad de la información para una institución financiera".*Moises Antonio Villena Aguilar. Año de publicación: 2006

Disponible en: http://tesis.pucp.edu.pe/repositorio/bitstream/handle/20.500.12404/362/VILLENA_MOIS%c3%89S_SISTEMA_DE%20GESTI%c3%93N_DE_SEGURIDAD_DE_INFORMACI%c3%93N_PARA_UNA_INSTITUCI%c3%93N_FINANCIERA.pdf?sequence=1&isAllowed=y

[19] Ministerio de fomento. "*La gestión por procesos".* Fecha de publicación Mayo de 2005.

Disponible en: https://www.fomento.es/NR/rdonlyres/9541ACDE-55BF-4F01-B8FA-03269D1ED94D/19421/CaptuloIVPrincipiosdelagestindelaCalidad.pdf

[20] INCIBE. "Fácil y sencillo Análisis de riesgos en 6 pasos". Fecha de publicación: 16 de enero de 2017.

Disponible en: https://www.incibe.es/protege-tu-empresa/blog/analisis-riesgos-pasos-sencillo

[21] QA:news. *"Como gestionar un equipo: La Matriz RASCI".* QANEWSBLOG. Fecha de publicación: 21 de Julio, 2015

Disponible en: https://qanewsblog.com/2015/07/21/como-gestionar-un-equipo-la-matriz-rasci/

[22] Llanos Cuenca. *"Enfoque de Procesos. Modelos de Referencia".* Universitat Politécnica de Valencia.

[23] Colegio oficial de ingenieros de telecomunicación. *"Guía de iniciación a Actividad Profesional Implantación de Sistemas de Gestión de la Seguridad de la Información (SGSI) según la norma ISO 27001".*

[24] www.iso27001security.com

IMÁGENES

[0] Imagen incluida en la portada:

Disponible en: https://pixabay.com/es

[1] Página 7:

Disponible en: www.iso27001.es

[2] Página 8:

Disponible en: https://dqsiberica.com/wp-content/uploads/2018/09/iso-logo.jpg

[3] Página 9:

Disponible en: https://www.tripolis.com/wp-content/uploads/2019/02/iso_27001_surus-inversa.jpg

[4] Página 9:

Disponible en: https://cdn.pixabay.com/photo/2017/07/14/09/28/matrix-2503236_960_720.jpg

[5] Página 18:

Disponible en: https://lequid.es/blog/wp-content/uploads/2017/11/grupo-de-empresas.jpg

[6] Página 20:

Disponible en: http://www.pcecuador.com/web/images/stories/Cursos/auditoria_informatica.png

[7] Página 21:

Disponible en: https://auditest.es/wp-content/uploads/2018/05/Captura-de-pantalla-2018-05-11-a-las-11.10.55.png

[8] Página 21:

Disponible en: https://pixabay.com/es/photos/auditor%C3%ADa-gr%C3%A1fico-mano-por-escrito-3229739/

[9] Página 23

Disponible en: http://www.minambiente.gov.co/images/control-interno/imagenes/pormenorizado_y_contrataci%C3%B3n_2.jpg

[11] Página 32

Disponible en: https://3foldtraining.com/wp-content/uploads/2018/01/CQI-IRCA-Certified-Course-logo-600x236.jpg

[10] Página 33

Disponible en: https://i2.wp.com/www.eldinero.com.do/wp-content/uploads/la-auditoria.jpg?fit=900%2C574&ssl=1

ANEXO

En las siguientes páginas se muestra un ejemplo de checklist de la norma ISO 27001:2017 que contiene los objetivos de control y controles de referencia de la norma, con una serie de preguntas para comprobar si se llevan a cabo estos controles correctamente. (Fuente: www.ISO27001security.com)

Estado y Aplicabilidad de controles de Seguridad de la Información

Sección	Controles de Seguridad de la Información	Estado	Recurso	Preguntas
A5	**Políticas de seguridad de la información**			
A5.1	**Directrices de gestión de la seguridad de la información**			
A5.1.1	Políticas para la seguridad de la información	? Desconocido		¿Existe una clara evidencia de un marco / estructura / jerarquía global razonablemente diseñada y administrada? ¿Las políticas son razonablemente completas y cubren todos los riesgos de información y áreas de control relevantes? ¿Cómo se autorizan, comunican, comprenden y aceptan las políticas? ¿Están formalmente obligados a cumplir todos los trabajadores y, en su caso, sus empleadores? ¿Hay acuerdos adecuados de cumplimiento y refuerzo? ¿Hay referencias cruzadas a buenas prácticas (como ISO27k, NIST SP800, CSC20 y otras normas y directrices relevantes)? ¿Están las políticas bien escritas, legible, razonable y viable? ¿Incorporan controles adecuados y suficientes? ¿Cubren todos los activos de información esenciales, sistemas, servicios, etc.? ¿Cuán madura es la organización en esta área?
A5.1.2	Revisión de las políticas para la seguridad de la información	? Desconocido		¿Todas las políticas tienen un formato y estilo consistentes? ¿Están todos al día, habiendo completado todas las revisiones debidas? ¿Se han vuelto a autorizar y se han distribuido?
A6	**Organización de la seguridad de la información**			
A6.1	**Organización interna**			
A6.1.1	Roles y responsabilidades en seguridad de la información	? Desconocido		¿Se le da suficiente énfasis a la seguridad y al riesgo de la información? ¿Hay apoyo de la administración? ¿Existe un foro de alta gerencia para analizar el riesgo de la información y las políticas, los riesgos y los problemas de seguridad? ¿Los roles y las responsabilidades están claramente definidos y asignados a personas adecuadamente capacitadas? ¿Tiene cada rol responsabilidad específica con respecto al riesgo y la seguridad de la información? ¿Hay suficiente presupuesto para las actividades de seguridad y riesgo de la información? ¿Hay coordinación dentro de la organización entre las unidades de negocio? ¿funciona efectivamente en la práctica? ¿Existe una conciencia y un apoyo adecuados para la estructura de riesgo y seguridad de la información?
A6.1.2	Segregación de tareas	? Desconocido		¿Son los deberes / funciones segregados entre roles o individuos cuando sea relevante para reducir la posibilidad de incompetencia, negligencia y actividades inapropiadas? ¿Se utiliza una matriz tipo RACI para mantener la identificación para cada tarea? Responsable | Accountable | Consulted | Informed ¿Existe una política que cubra la segregación de deberes? ¿Cómo llegan las decisiones con respecto a tal segregación? ¿Quién tiene la autoridad para tomar tales decisiones? ¿Se realiza un seguimiento regular de las actividades y los registros de auditoría?
A6.1.3	Contacto con las autoridades	? Desconocido		¿Hay disponible una lista de detalles de contacto para las autoridades reguladoras u otras autoridades y organismos que podrían necesitar ser contactados en caso de consultas, incidentes y emergencias? ¿Quién es el responsable de contactar a las autoridades y en qué punto de un incidente / evento se realiza este contacto y cómo? ¿La lista es actual y correcta? ¿Hay un proceso de mantenimiento?
A6.1.4	Contacto con grupos de interés especial	? Desconocido		¿Hay un contacto regular, con grupos especiales de interés, foros y listas de correo profesionales en riesgo de la información y la seguridad, tales como los capítulos locales de ISACA, ISC 2, ISSA, ISO27k? ¿Se comparte información sobre amenazas emergentes, nuevas tecnologías de seguridad, buenas prácticas de seguridad, advertencias tempranas de alertas y advertencias, vulnerabilidades recientemente descubiertas y disponibilidad de parches?
A6.1.5	Seguridad de la información en la gestión de proyectos	? Desconocido		¿Se identifican y abordan los riesgos de la información y los requisitos de seguridad en todas las etapas de todos los proyectos, incluidos todos los tipos de proyectos relacionados con la información, los nuevos desarrollos y los cambios / mejoras en los sistemas, aplicaciones y procesos existentes? ¿La etapa del proyecto incluye actividades apropiadas?
A6.2	**Los dispositivos móviles y el teletrabajo**			
A6.2.1	Política de dispositivos móviles	? Desconocido		¿Existen política y controles seguridad relacionados con los usuarios móviles? ¿Se distinguen los dispositivos personales de los empresariales? ¿Cómo se mantienen y controlan los sistemas portátiles para garantizar que estén actualizados sobre las definiciones de antivirus y los parches de seguridad? ¿Se emplean soluciones de MDM y soluciones MAM para controlar las aplicaciones, el acceso y el cifrado completo de disco?
A6.2.2	Teletrabajo	? Desconocido		¿Los controles de seguridad para el teletrabajo son equivalentes a los de los lugares de trabajo de oficina? ¿Existen disposiciones adecuadas para la autenticación del usuario (2FA), la seguridad de la red (Always-on-VPN), antivirus, copias de seguridad, parches, registro de seguridad y monitoreo, encriptación y continuidad del negocio?
A7	**Seguridad relativa a los recursos humanos**			
A7.1	**Antes del empleo**			
A7.1.1	Investigación de antecedentes	? Desconocido		¿El proceso de evaluación previa al empleo toma en cuenta las leyes y regulaciones relevantes de privacidad y empleo? ¿Se hace en la empresa o se subcontrata a un tercero? Si se subcontrata a un tercero, ¿Se han revisado sus procesos y se han considerado aceptables? ¿Se hace contacto de referencias y una verificación de antecedentes, según corresponda durante el proceso de selección? ¿Existen procesos de selección mejorados para los trabajadores en roles críticos? ¿Cómo se logra todo esto? ¿Hay un proceso documentado, consistente y repetible, que sea propiedad y mantenido por RRHH?
A7.1.2	Términos y condiciones del empleo	? Desconocido		¿Están claramente definidos los términos y condiciones de empleo? ¿Se hace distinción entre profesionales de la seguridad, los administradores de redes / sistemas de TI, los gerentes, los auditores y los trabajadores en general? ¿Se identifican responsabilidades específicas relacionadas con el riesgo y la seguridad de la información de acuerdo con la naturaleza de los roles? ¿Se mantienen registros para probar que los trabajadores entendieron, reconocieron y aceptaron sus obligaciones de seguridad de la información?
A7.2	**Durante el empleo**			
A7.2.1	Responsabilidades de gestión	? Desconocido		¿Existe un programa de concientización / educación sobre la seguridad de la información dirigido a la gerencia? ¿Se hace de forma regular y está a día? ¿El contenido y la naturaleza / formato / estilo de la información y las actividades de sensibilización son adecuados? ¿Los gerentes reciben el conocimiento y la capacitación apropiados específicamente sobre su riesgo clave de información y roles y responsabilidades relacionados con la seguridad? ¿Se provee información sobre la postura, estrategias y políticas de seguridad de la información de la organización?

Estado y Aplicabilidad de controles de Seguridad de la Información

Sección	Controles de Seguridad de la Información	Estado	Recurso	Preguntas
A7.2.2	Concienciación, educación y capacitación en seguridad de la información	? Desconocido		¿Están las competencias necesarias y los requisitos de capacitación / concienciación para los profesionales de seguridad de la información y otros con funciones y responsabilidades específicas identificadas explícitamente? ¿Existe un programa estructurado de sensibilización y capacitación sobre seguridad de la información para todos los tipos de trabajadores? ¿Existe una estrategia o plan de comunicación, que incluya folletos, carteles, correos electrónicos, gestión de aprendizaje online, cuestionarios, concursos, videos, redes sociales y otros métodos? ¿Se cubren los requisitos legales, reglamentarios, contractuales, políticos, responsabilidad personal, responsabilidades generales, puntos de contacto y otros recursos? ¿Se actualiza el contenido para reflejar los riesgos de la información en evolución, como las amenazas emergentes, las vulnerabilidades recientemente identificadas y los incidentes, y los cambios, como las políticas nuevas / revisadas? ¿Hay exámenes y ejercicios periódicos para verificar el nivel de conocimiento? ¿Hay acciones de seguimiento para cualquiera que tenga problemas en dichas pruebas?
A7.2.3	Proceso disciplinario	? Desconocido		¿Existe un proceso disciplinario para incidentes de seguridad de la información, violaciones a la privacidad, piratería informática, fraude y espionaje industrial por parte de los trabajadores? ¿Cómo se informa a los trabajadores sobre el proceso, incluidas las expectativas de la organización y sus derechos? ¿Está esto cubierto por contratos y acuerdos, capacitación inicial y conocimiento continuo? ¿Se actualiza el proceso de forma regular?
A7.3	**Finalización del empleo o cambio en el puesto de trabajo**			
A7.3.1	Responsabilidades ante la finalización o cambio	? Desconocido		¿Existen políticas de revisión, estándares, procedimientos, directrices y registros relacionados con la seguridad de la información para los trabajadores que se mueven lateral o verticalmente dentro de la organización? ¿Se tienen en cuenta las promociones, degradaciones, cambios de roles, nuevas responsabilidades, nuevas prácticas de trabajo, renuncias, despidos? ¿Se tiene en cuenta la recuperación de los activos de información (documentos, datos, sistemas), las llaves, la eliminación de los derechos de acceso?
A8	**Gestión de activos**			
A8.1	**Responsabilidad sobre los activos**			
A8.1.1	Inventario de activos	? Desconocido		¿Hay un inventario de activos de la información? ¿Contiene la siguiente información? • Datos digitales • Información impresa • Software • Infraestructura • Servicios de información y proveedores de servicios • Seguridad física • Relaciones comerciales • Las personas ¿A quién pertenece el inventario? ¿Cómo se mantiene el inventario en una condición razonablemente completa, precisa y actualizada a pesar de los cambios de equipo / personal, nuevos sistemas, negocios y cambios de TI? ¿Es suficientemente detallado y está estructurado adecuadamente?
A8.1.2	Propiedad de los activos	? Desconocido		¿Los activos tienen propietario de riesgo? ¿Los activos tienen responsable técnico? ¿Cómo se asigna la propiedad poco después de crear o adquirir los activos críticos? ¿Cómo se etiquetan los activos? ¿Cómo se informa ante incidentes de seguridad de la información que los afectan?
A8.1.3	Uso aceptable de los activos	? Desconocido		¿Existe una política sobre el uso aceptable de los recursos tecnológicos, como el correo electrónico, la mensajería instantánea, el FTP, las responsabilidades de los usuarios, etc.? ¿Cubre el comportamiento del usuario en Internet y en las redes sociales? ¿Se permite el uso personal de los activos de la empresa? En caso afirmativo, ¿En qué medida y cómo se controla / asegura esto? ¿Se describe de forma explícita lo qué constituye un uso inapropiado? ¿Se distribuye esta información a toda la empresa? ¿El uso de la criptografía cumple con todas las leyes, acuerdos / contratos y normativas relevantes?
A8.1.4	Devolución de activos	? Desconocido		¿Existe un procedimiento para recuperar los activos tras una baja o despido? ¿Es un procedimiento automatizado o manual? Si es manual, ¿Cómo se garantiza que no haya desvíos? ¿Cómo se abordan los casos en los que los activos no han sido devueltos?
A8.2	**Clasificación de la información**			
A8.2.1	Clasificación de la información	? Desconocido		¿Existen políticas de revisión, estándares, procedimientos, directrices y registros asociados relacionados con la clasificación de la información? ¿La clasificación es impulsada por obligaciones legales o contractuales? ¿La clasificación se basa en los requisitos de confidencialidad, integridad y disponibilidad? ¿Se utilizan marcas apropiadas en los activos en función de la clasificación de la información que contienen? ¿El personal conoce los requisitos de seguridad correspondientes para el manejo de materiales clasificados?
A8.2.2	Etiquetado de la información	? Desconocido		¿Existe un procedimiento de etiquetado para la información tanto en forma física como electrónica? ¿Está sincronizado con la política de clasificación de la información? ¿Cómo se garantiza el correcto etiquetado? ¿Cómo se garantiza que solo aquellos con permisos de acceso aprobados accedan a la información de la clasificación relevante? ¿Cómo se garantiza que no haya acceso no autorizado? ¿Se revisan los niveles de clasificación en intervalos predefinidos?
A8.2.3	Manipulado de la información	? Desconocido		Más allá de A.8.2.1 ¿Están los niveles de clasificación adecuadamente asignados a los activos? ¿Se considera los gimiente? Método de etiquetado, transferencia, almacenamiento, manejo de medios extraíbles, eliminación de medios electrónicos y físicos, divulgación, intercambio, intercambio con terceros, etc.
A8.3	**Manipulación de los soportes**			
A8.3.1	Gestión de soportes extraíbles	? Desconocido		¿Existe un registro de activos completo y actualizado de CD / DVD, almacenamiento USB y otros medios extraíbles? ¿Los medios extraíbles están debidamente etiquetados y clasificados? ¿Los medios se mantienen y almacenan de forma adecuada? ¿Hay controles apropiados para mantener la confidencialidad de los datos almacenados?
A8.3.2	Eliminación de soportes	? Desconocido		Más allá de A.8.3.1 ¿Existen una política específica y documentación de obligaciones contractuales, legales o reglamentarias para la eliminación de los medios? ¿Se documenta la aprobación en cada etapa para la eliminación de los medios? ¿Los datos que aún deben conservarse se copian en otros medios y se verifican antes de su eliminación? ¿Se tiene en cuenta los periodos de retención? ¿Los datos particularmente confidenciales se eliminan de forma segura (borrado criptográfico, desmagnetización o destrucción física)?
A8.3.3	Soportes físicos en tránsito	? Desconocido		¿Se utiliza un transporte o servicio de mensajería confiable? ¿Se utiliza un mecanismo de cifrado adecuado durante el proceso de transferencia? ¿Se verifica la recepción por el destino?
A9	**Control de acceso**			

Estado y Aplicabilidad de controles de Seguridad de la Información

Sección	Controles de Seguridad de la Información	Estado	Recurso	Preguntas
A9.1	**Requisitos de negocio para el control de acceso**			
A9.1.1	Política de control de acceso	? Desconocido		¿Existe una política de control de acceso? ¿Es consistente con la política de clasificación? ¿Hay una segregación de deberes apropiada? ¿Existe un proceso documentado de aprobación de acceso? ¿El proceso de aprobación requiere que se involucre el propietario del sistema o la información en cuestión?
A9.1.2	Acceso a las redes y a los servicios de red	? Desconocido		¿Se asegura que el acceso VPN e inalámbrico es supervisado, controlados y autorizado? ¿Se utiliza autenticación de múltiples-factor para acceso a redes, sistemas y aplicaciones críticas, especialmente para los usuarios privilegiados? ¿Cómo monitoriza la red para detectar acceso no autorizado? ¿Los controles de seguridad de la red son evaluados y probados regularmente (Pentesting)? ¿La organización mide la identificación y los tiempos de respuesta ante incidentes?
A9.2	**Gestión de acceso de usuario**			
A9.2.1	Registro y baja de usuario	? Desconocido		¿Se utiliza un ID de usuario únicos para cada usuario? ¿Se genera en función a una solicitud con aprobaciones y registros apropiados? ¿Se deshabilitan los ID de usuario de forma inmediata tas una baja o despido? ¿Existen una comunicación eficiente ente la Administración de Seguridad y Recursos Humanos? ¿Existe una revisión / auditoría periódica para identificar y deshabilitar los ID de usuario redundantes? ¿Se eliminan los ID deshabilitados después de confirmar que ya no son necesarios? ¿Qué impide que los ID de usuario sean reasignados a otros usuarios?
A9.2.2	Provisión de acceso de usuario	? Desconocido		¿El acceso a sistemas y servicios de información se basa en las necesidades del negocio? ¿Se garantiza que todo acceso que se concede se ajuste a las políticas de control de acceso y segregación de funciones? ¿Existe un registro documental de la solicitud y aprobación de acceso?
A9.2.3	Gestión de privilegios de acceso	? Desconocido		Más allá de A.9.2.2 ¿Hay un proceso para realizar revisiones más frecuentes y periódicas de cuentas privilegiadas para identificar y deshabilitar / eliminar cuentas con privilegios redundantes y / o reducir los privilegios? ¿Se genera un ID de usuario separado para otorgar privilegios elevados? ¿Se ha establecido una caducidad para los ID de usuario con privilegios? ¿Se controlan las actividades de los usuarios privilegiados de forma más detallada?
A9.2.4	Gestión de la información secreta de autenticación de los usuarios	? Desconocido		¿Se implementan controles técnicos, como la longitud mínima de la contraseña, reglas de complejidad, cambio forzado de contraseñas en el primer uso, autenticación de múltiples factores, datos biométricos, contraseñas compartidas etc.? ¿Se verifica rutinariamente si hay contraseñas débiles? ¿Se requiere confirmar la identidad de los usuarios antes de proporcionarles contraseñas temporales nuevas? ¿Se transmite dicha información por medios seguros? ¿Se generan contraseñas temporales suficientemente fuertes? ¿Se cambian las contraseñas por defecto de los fabricantes? ¿Se recomienda a los usuarios usar el software adecuado de protección de contraseñas? ¿Se almacenen de forma cifrada las contraseñas en sistemas, dispositivos y aplicaciones?
A9.2.5	Revisión de los derechos de acceso de usuario	? Desconocido		¿Se hace una revisión periódica y documentada de los derechos de acceso de los usuarios en sistemas y aplicaciones? ¿Participan en dicha revisión los "propietarios" para verificar cambios en las funciones de los usuarios? ¿Se revisan los derechos de acceso para usuarios con privilegios de forma más exhaustiva y frecuente?
A9.2.6	Retirada o reasignación de los derechos de acceso	? Desconocido		¿Existe un proceso de ajuste de derechos de acceso? ¿Tiene en cuenta empleados, proveedores y contratistas al finalizar o cambiar su empleo, contrato o acuerdo? ¿Incluye el acceso físico a las instalaciones y el acceso lógico a la red? En casos en los que se usan credenciales compartidas, ¿Se cambian las contraseñas cuando ocurren ceses o despidos de empleados que las usan?
A9.3	**Responsabilidades del usuario**			
A9.3.1	Uso de la información secreta de autenticación	? Desconocido		¿Cómo se asegura la confidencialidad de las credenciales de autenticación? ¿Existe un proceso de cambio de contraseñas en caso de ser comprometida? ¿Existen controles de seguridad relativas a las cuentas compartidas?
A9.4	**Control de acceso a sistemas y aplicaciones**			
A9.4.1	Restricción del acceso a la información	? Desconocido		Más allá de A.9.2.2 ¿Existen controles de acceso adecuados? ¿Se identifican los usuarios de forma individual individuales? ¿Cómo se definen, autorizan, asignan, revisan, gestionan y retiran los derechos de acceso, los permisos y las reglas asociadas?
A9.4.2	Procedimientos seguros de inicio de sesión	? Desconocido		¿Se muestra una pantalla de advertencia en el proceso de inicio de sesión para disuadir el acceso no autorizado? ¿Cómo se autentican las identidades de usuario durante el proceso de inicio de sesión? ¿Se utiliza autenticación multifactor para sistemas / servicios / conexiones remotas críticas a través de VPN s etc.? ¿La información de inicio de sesión solo se valida una vez imputadas las credenciales? ¿Las contraseñas no válidas desencadenan demoras o bloqueos, entradas de registro y alertas / alarmas? ¿Se registran los inicios de sesión exitosos? ¿Se transmiten las contraseñas de modo seguro mediante el uso de cifrado?
A9.4.3	Sistema de gestión de contraseñas	? Desconocido		¿Los sistemas requieran una fortaleza de contraseñas establecidos en las políticas y estándares corporativos? ¿Las reglas tienen en cuenta lo siguiente? • Longitud mínima de la contraseña • Evitan la reutilización de un número específico de contraseñas • Imponen reglas de complejidad (mayúsculas, minúsculas, números, símbolos, etc.) • Requiere el cambio forzado de contraseñas en el primer inicio de sesión • Esconde la contraseña durante la imputación ¿Se almacenan y transmiten de forma segura (cifrado)?
A9.4.4	Uso de utilidades con privilegios del sistema	? Desconocido		¿Quién controla los servicios privilegiados? ¿Quién puede acceder a ellos, bajo qué condiciones y con qué fines? ¿Se verifica que estas personas necesidad comercial para otorgar el acceso según su roles y responsabilidades? ¿Existe un proceso auditable de aprobación, y cada instancia de su uso está registrado? ¿Se tiene en cuenta la segregación de tareas?
A9.4.5	Control de acceso al código fuente de los programas	? Desconocido		¿El código fuente se almacena en una o más bibliotecas de programas fuente o repositorios? ¿El entorno es seguro, con un acceso adecuado, control de versiones, monitoreo, registro, etc.? ¿Cómo se modifica el código fuente? ¿Cómo se publica y se compila el código? ¿Se almacenan y revisan los registros de acceso y cambios?
A10	**Criptografía**			
A10.1	**Controles criptográficos**			
A10.1.1	Política de uso de los controles criptográficos	? Desconocido		¿Existe una política que cubra el uso de controles criptográficos? ¿Cubre lo siguiente? • Los casos en los que información debe ser protegida a través de la criptografía • Normas que deben aplicarse para la aplicación efectiva • Un proceso basado en el riesgo para determinar y especificar la protección requerida • Uso de cifrado para información almacenada o transferida • Los efectos de cifrado en la inspección de contenidos de software • Cumplimiento de las leyes y normativas aplicables ¿Se cumple con la política y requerimientos de cifrado?

Estado y Aplicabilidad de controles de Seguridad de la Información

Sección	Controles de Seguridad de la Información	Estado	Recurso	Preguntas
A10.1.2	Gestión de claves	? Desconocido		¿La política de criptografía abarca todo el ciclo de vida de la gestión de claves (de principio a fin)? ¿Se protege el equipo utilizado para generar, almacenar y archivar claves criptográficas? ¿Se generan claves diferentes para sistemas y aplicaciones? ¿Se evitan claves débiles? ¿Existen reglas sobre cambio / actualización de claves (ej. autorizar, emitir, comunicar e instalar claves)? ¿Se hacen copias de respaldo de las claves? ¿Se registran las actividades clave de gestión? ¿Cómo se cumplen todos estos requisitos?
A11	**Seguridad física y del entorno**			
A11.1	**Áreas seguras**			
A11.1.1	Perímetro de seguridad física	? Desconocido		¿Las instalaciones se encuentran en una zona de riesgo? ¿Se definen los perímetros de seguridad (edificios, oficinas, redes informáticas, habitaciones, armarios de red, archivos, salas de máquinas, etc.)? ¿El techo exterior, las paredes y el suelo son de construcción sólida? ¿Están todos los puntos de acceso externos adecuadamente protegidos contra el acceso no autorizado? ¿Las puertas y ventanas son fuertes y con cerradura? ¿Se monitorea los puntos de acceso con cámaras? ¿Existe un sistema de detección de intrusos y se prueba periódicamente?
A11.1.2	Controles físicos de entrada	? Desconocido		¿Se utilizan sistemas de control de acceso adecuados (ej. Tarjetas de proximidad, biométrico, cerraduras de seguridad, monitorización CCTV, detección de intrusos)? ¿Hay procedimientos que cubran las siguientes áreas? • Cambio regular código de acceso • Inspecciones de las guardias de seguridad • Visitantes siempre acompañados y registrados en el libro de visitantes • Registro de movimiento de material • Entrada a áreas definidas del edificio según roles y responsabilidades (acceso a CPD, salas de comunicación y otras áreas críticas) ¿Se utiliza autenticación multi-factor de autenticación (ej. Biométrico más el código PIN)? ¿Se requiere para las áreas críticas? ¿Existe un registro de todas las entradas y salidas?
A11.1.3	Seguridad de oficinas, despachos y recursos	? Desconocido		¿Están los accesos (entrada y salida) de las instalaciones físicamente controlas (ej. Detectores de proximidad, CCTV)? ¿Son proporcionados los controles de seguridad utilizados para salvaguardar las oficinas, salas e instalaciones con respecto a los riesgos? ¿Se tiene en cuenta los activos de información almacenados, procesados o utilizados en dichas ubicaciones?
A11.1.4	Protección contra las amenazas externas y ambientales	? Desconocido		¿Qué tipo de protecciones existen contra el fuego, el humo, inundaciones, rayos, intrusos, vándalos, etc.? ¿Existe un procedimiento de recuperación de desastres? ¿Se contemplan sitios remotos?
A11.1.5	El trabajo en áreas seguras	? Desconocido		¿Se verifican al final del día las oficinas, las salas de informática y otros lugares de trabajo? ¿Se hace un análisis para evaluar que los controles adecuados están implementados? Controles de acceso físico Alarmas de intrusión Monitoreo de CCTV (verificar la retención y frecuencia de revisión) Se prohíbe el uso de equipos fotográficos, video, audio u otro tipo de grabación Políticas, procedimientos y pautas ¿Cómo se asegura que la información de carácter sensible permanece confidencial a personal autorizado?
A11.1.6	Áreas de carga y descarga	? Desconocido		¿Las entregas se hacen en un área segura con control de acceso y limitado a personal autorizado? ¿Se verifica que el material recibido coincide con un número de pedido autorizado? ¿Se registran los detalles de la recepción de material según las políticas y procedimientos de adquisición, gestión de activos y seguridad?
A11.2	**Seguridad de los equipos**			
A11.2.1	Emplazamiento y protección de equipos	? Desconocido		¿Las TIC y el equipo relacionado se encuentran en áreas adecuadamente protegidas? ¿Las pantallas de los equipos de trabajo, las impresoras y los teclados están ubicados o protegidos para evitar la visualización no autorizada? ¿Existen controles para minimizar los siguientes riesgos de amenazas físicas y medioambientales? • Agua / inundación • Fuego y humo • Temperatura, humedad y suministro eléctrico • Polvo • Rayos, electricidad estática y seguridad del personal ¿Se prueban estos controles periódicamente y después de cambios importantes?
A11.2.2	Instalaciones de suministro	? Desconocido		¿El sistema UPS proporciona una potencia adecuada, confiable y de alta calidad? ¿Hay una capacidad de UPS adecuada para abarcar todos los equipos esenciales durante un período de tiempo suficiente? ¿Hay un plan de mantenimiento pare los UPS y generadores en acuerdo con las especificaciones del fabricante? ¿Son probados con regularidad? ¿Hay una red de suministro eléctrico redundante? ¿Se realizan pruebas de cambio? ¿Se ven afectados los sistemas y servicios? ¿Hay sistemas de aire acondicionado para controlar entornos con equipos críticos? ¿Están ubicados apropiadamente? ¿Hay una capacidad adecuada de A / C para soportar la carga de calor? ¿Hay unidades redundantes, de repuesto o portátiles disponibles? ¿Hay detectores de temperatura con alarmas de temperatura?
A11.2.3	Seguridad del cableado	? Desconocido		¿Hay protección física adecuada para cables externos, cajas de conexiones? ¿Se separa el cableado de suministro eléctrico del cableado de comunicaciones para evitar interferencias? ¿Se controla el acceso a los paneles de conexión y las salas de cableado? ¿Existen procedimientos adecuados para todo ello?
A11.2.4	Mantenimiento de los equipos	? Desconocido		¿Se asigna personal cualificado para realizar el mantenimiento de los equipos (infraestructura y dispositivos de red, equipos de trabaja, portátiles, equipos de seguridad y servicios tales como detectores de humo, dispositivos de extinción de incendios, HVAC, control de acceso, CCTV, etc.)? ¿Hay programas de mantenimiento y registros / informes actualizados? ¿Se aseguran los equipos?
A11.2.5	Retirada de materiales propiedad de la empresa	? Desconocido		¿Existen procedimiento relativos al traslado de activos de información? ¿Hay aprobaciones o autorizaciones documentadas en los niveles apropiados? ¿Existe un control para limitar el traslado de activos de información mediante el uso de unidades de almacenamiento externo? ¿Existe un procedimiento para rastrear movimientos de activos de alto valor o alto riesgo?
A11.2.6	Seguridad de los equipos fuera de las instalaciones	? Desconocido		¿Existe una "política de uso aceptable" que cubra los requisitos de seguridad y "obligaciones" con respecto al uso de dispositivos móviles o portátiles que se utilizan desde casa o en ubicaciones remotas? ¿Contempla el almacenamiento seguro de los dispositivos, uso cifrado y uso de conexiones seguras? ¿Existen controles para asegura todo esto? ¿Cómo se les informa a los trabajadores sobre sus obligaciones? ¿Se les da suficiente apoyo para alcanzar un nivel aceptable de seguridad?

Estado y Aplicabilidad de controles de Seguridad de la Información

Sección	Controles de Seguridad de la Información	Estado	Recurso	Preguntas
A11.2.7	Reutilización o eliminación segura de equipos	? Desconocido		¿Cómo evita la organización que se revele la información almacenada en equipos tras su reasignación o eliminación? ¿Se utiliza cifrado fuerte o borrado seguro? ¿Se mantienen registros adecuados de todos los medios que se eliminan? ¿La política y el proceso cubren todos los dispositivos y medios de TIC?
A11.2.8	Equipo de usuario desatendido	? Desconocido		¿Se suspenden / finalizan las sesiones a aplicaciones para evitar la pérdida de datos o la corrupción? ¿Se define un tiempo de inactividad adecuado los riesgos de acceso físico no autorizado? ¿Se protegen los bloqueos de pantalla con contraseña? ¿Se aplica a todos los servidores, equipos de trabajo, portátiles, teléfonos y otros dispositivos TIC? ¿Cómo se verifica el cumplimiento?
A11.2.9	Política de puesto de trabajo despejado y pantalla limpia	? Desconocido		¿Existen políticas, normas, procedimientos y directrices para mantener las zonas de trabajo limpias y despejadas? ¿Funciona en la práctica? ¿Todos los dispositivos informáticos tienen un salvapantallas o bloqueo con contraseña que los empleados usan cuando se alejan de sus dispositivos? ¿Se activa automáticamente tras de un tiempo inactivo definido? ¿Se mantienen las impresoras, fotocopiadoras, escáneres despejados?
A12	**Seguridad de las operaciones**			
A12.1	**Procedimientos y responsabilidades operacionales**			
A12.1.1	Documentación de procedimientos operacionales	? Desconocido		¿Existen procedimientos para las operaciones de TI, sistemas y gestión de redes, gestión de incidencias, la administración de TI, seguridad de TI, seguridad física, gestión de cambios, etc.? ¿Existe un conjunto completo de procedimientos de seguridad y cuándo se revisaron por última vez? ¿Los procesos son razonablemente seguros y están bien controlados? ¿Los roles y responsabilidades están bien definidos y se capacita adecuadamente al personal? ¿Se tienen en cuenta los cambios, configuraciones, versiones, capacidad, rendimiento, problemas, incidentes, copias de seguridad, almacenamiento, restauración, registros de auditoría, alarmas / alertas, endurecimiento, evaluaciones de vulnerabilidad, parches, configuración / actualizaciones de antivirus, encriptación, etc.)? ¿Los procedimientos están siendo revisados y mantenidos rutinariamente, autorizados / ordenados, compartidos y usados?
A12.1.2	Gestión de cambios	? Desconocido		¿Existe una política de gestión de cambios? ¿Existen registros relacionados a la gestión de cambios? ¿Se planifican y gestionan los cambios? ¿Se evalúan los riesgos potenciales asociados con los cambios? ¿Los cambios están debidamente documentados, justificados y autorizados por la administración?
A12.1.3	Gestión de capacidades	? Desconocido		¿Existe una política de gestión de capacidad? ¿Existen registros relacionados a la gestión de capacidad? ¿Incluye aspectos tales como las SLA, seguimiento de las métricas relevantes (ej. uso de la CPU, almacenamiento y errores de página, capacidad de la red, demanda de RAM, la capacidad de aire acondicionado, espacio de rack, la utilización, etc.), alarmas / alertas en niveles críticos, la planificación hacia adelante? ¿Se basa la prioridad en asegurar el rendimiento y la disponibilidad de servicios críticos, servidores, infraestructura, aplicaciones, funciones en un análisis de riesgos?
A12.1.4	Separación de los recursos de desarrollo, prueba y operación	? Desconocido		¿Se segregan entornos de TIC de desarrollo, prueba y operacionales? ¿Cómo se logra la separación a un nivel de seguridad adecuado? ¿Existen controles adecuados para aislar cada entorno (ej. redes de producción, redes utilizadas para el desarrollo, redes de pruebas, la gestión)? ¿Se tienen acceso a través de perfiles de usuario debidamente diferenciados para cada uno de estos entornos? ¿Cómo se promueve y se lanza el software? ¿Se aplica la gestión de cambios a la autorización y migración de software, datos, metadatos y configuraciones entre entornos en cualquier dirección? ¿Se tiene en cuenta el riesgo de la información y los aspectos de seguridad que incluye el cumplimiento de privacidad si los datos personales se mueven a entornos menos seguros? ¿Se identifica un responsable de garantizar que el software nuevo / modificado no interrumpa las operaciones de otros sistemas o redes?
A12.2	**Protección contra el software malicioso (malware)**			
A12.2.1	Controles contra el código malicioso	? Desconocido		¿Existen políticas y procedimientos asociados a controles antimalware? ¿Se utilizan listas blancas o negras para controlar el uso de software autorizado y no autorizado? ¿Cómo se compila, gestiona y mantiene la lista y por quién? ¿Hay controles de antivirus de "escaneado en acceso" y "escaneo programático" en todos los dispositivos relevantes, incluidos servidores, portátiles, ordenadores de sobremesa y dispositivos integrados / IoT? ¿Se actualiza el software antivirus de forma automática? ¿Se general alertas accionables tras una detección? ¿Se toma acción de forma rápida y apropiada para minimizar sus efectos? ¿Cómo se gestionan las vulnerabilidades técnicas? ¿Existe una capacitación y una concienciación apropiada que cubra la detección, el informe y la resolución de malware para usuarios, gerentes y especialistas de soporte? ¿Existe un mecanismo de escalación para incidentes graves?
A12.3	**Copias de seguridad**			
A12.3.1	Copias de seguridad de la información	? Desconocido		¿Existen políticas y procedimientos asociados a las copias de seguridad? ¿Existe un mandato basado en el riesgo para un registro preciso y completo de copias de seguridad cuya política de retención y frecuencia reflejen las necesidades del negocio? ¿Las copias de seguridad cubren los datos y metadatos, sistema y programas de aplicación y los parámetros de configuración de copias de seguridad para todos los sistemas, incluyendo servidores, ordenadores de sobremesa, teléfonos / sistemas de red, sistemas de gestión de red, portátiles, sistemas de control, sistemas de seguridad, etc.? ¿Los medios de respaldo están físicamente protegidos / asegurados al menos al mismo nivel que los datos operacionales? ¿Las copias de seguridad se almacenan en ubicaciones adecuadas, protegiendo contra desastres físicos y acceso indebido? ¿Se mantienen copias off-line para evitar una propagación de ransomware catastrófica? ¿Las copias de seguridad se prueban regularmente para garantizar que puedan restaurar? ¿Hay una clara adherencia a principios de confidencialidad, integridad y disponibilidad?
A12.4	**Registros y supervisión**			

Estado y Aplicabilidad de controles de Seguridad de la Información

Sección	Controles de Seguridad de la Información	Estado	Recurso	Preguntas
A12.4.1	Registro de eventos	? Desconocido		¿Existen políticas y procedimientos para el registro de eventos? ¿Se monitorean y registran de manera consistente y segura todos los sistemas clave incluido el registro de eventos en sí? ¿Se registra lo siguiente? • cambios en los ID de usuario • permisos y controles de acceso • actividades privilegiadas del sistema • intentos de acceso exitosos y fallidos • inicio de sesión y cierre de sesión • identidades y ubicaciones de dispositivos • direcciones de red, puertos y protocolos • instalación de software • cambios a las configuraciones del sistema • uso de utilidades y aplicaciones del sistema • archivos accedidos y el tipo de acceso • filtros de acceso web ¿Quién es responsable de revisar y hacer un seguimiento de los eventos informados? ¿Cuál es el periodo de retención de eventos?
A12.4.2	Protección de la información del registro	? Desconocido		¿Los registros se almacenan / archivan en un formato seguro o mecanismo de control no-editable? ¿El acceso a los registros es adecuadamente controlado, autorizado y monitoreado? ¿Quién tiene o podría obtener acceso a leer / escribir / eliminar registros de eventos? ¿Hay suficiente capacidad de almacenamiento dado el volumen de registros que se generan y los requisitos de retención? ¿Existen copias de seguridad de los registros?
A12.4.3	Registros de administración y operación	? Desconocido		Hay responsables identificados para la administración de acceso privilegiado al análisis de eventos (SIEM)? ¿Cómo se recogen, almacenan y aseguran, analizan los registros? ¿Existen limitaciones a la capacidad de dichas personas para interferir con los registros o, al menos, no sin generar alarmas de seguridad?
A12.4.4	Sincronización del reloj	? Desconocido		¿Existen políticas, arquitecturas o procedimientos relativos a la sincronización del reloj del sistema su precisión? ¿Hay un tiempo de referencia definido (ej. Reloj atómicos, GPS o NTP)? ¿El método para sincronizar relojes con la referencia cumple con los requisitos comerciales, de seguridad, operacionales, legales, regulatorios y contractuales? ¿Está implementado en todo el entorno TI, incluidos los sistemas de monitoreo tales como CCTV, sistemas de alerta, mecanismos de control de acceso, sistemas de auditoría y registro, etc.? ¿Existe una configuración de respaldo para la referencia de tiempo?
A12.5	**Control del software en explotación**			
A12.5.1	Instalación del software en explotación	? Desconocido		¿Existe una política acerca de la instalación de software? ¿Se asegura que todo software instalado es probado, aprobado, permitido y mantenido para su uso en producción? ¿Se verifica que ya no se utiliza software sin soporte (firmware, sistemas operativos, middleware, aplicaciones y utilidades)? ¿Se hace esta verificación en ordenadores de sobremesa, portátiles, servidores, bases de datos, etc.? ¿Existen controles para evitar instalaciones de software, excepto por administradores capacitados y autorizados? ¿Existe un monitoreo y alerta para detectar instalaciones de software no aprobadas? ¿Existe un control de cambio y aprobación adecuado para la aprobación de software?
A12.6	**Gestión de la vulnerabilidad técnica**			
A12.6.1	Gestión de las vulnerabilidades técnicas	? Desconocido		¿Existe una política la gestión de vulnerabilidades técnicas? ¿Cómo se escanean los sistemas para detectar vulnerabilidades de forma automatizada? ¿Cómo responde la organización ante vulnerabilidades técnicas descubiertas en equipos, servidores, aplicaciones, dispositivos de red y otros componentes? ¿Existen procesos adecuados para verificar los inventarios de los sistemas e identificar si las vulnerabilidades divulgadas son relevantes? ¿Se ha realizado una evaluación integral de riesgos de los sistemas TIC? ¿Se han identificado los riesgos y se han tratado apropiadamente, se han priorizado según el riesgo? ¿Se identifican cambios tales como amenazas emergentes, vulnerabilidades conocidas o sospechadas, y consecuencias o impactos comerciales en evolución? ¿Los parches son evaluados por su aplicabilidad y riesgos antes de ser implementados? ¿Los procesos para implementar parches urgentes son adecuados? ¿Se emplea una administración automatizada de parches? ¿Existen registros de aprobación o rechazo de implementación de parchas asociado a vulnerabilidades (aceptación de riesgo) en los niveles de administración adecuados?
A12.6.2	Restricción en la instalación de software	? Desconocido		¿La instalación software en los sistemas está limitada personal autorizado con privilegios de sistema adecuados? ¿Los privilegios de instalación están divididos en categorías y permiten instalar tipos de sistemas específicos? ¿Los controles se aplican a parches, copias de seguridad y descargas de la web, así como a instalaciones de sistemas, servidores, etc.?
A12.7	**Consideraciones sobre la auditoria de sistemas de información**			
A12.7.1	Controles de auditoría de sistemas de información	? Desconocido		¿Existe una política que requiera auditorías de seguridad de la información? ¿Existe un programa definido y procedimientos para auditoría? ¿Las auditorías se planifican cuidadosamente y se acuerdan para minimizar el riesgo de interrupciones en los procesos comerciales? ¿Se define el alcance de la auditoría en coordinación con la administración? ¿El acceso a las herramientas de auditoría de sistemas están controladas para evitar el uso y acceso no autorizado?
A13	**Seguridad de las comunicaciones**			
A13.1	**Gestión de la seguridad de las redes**			
A13.1.1	Controles de red	? Desconocido		¿Existen políticas de redes físicas e inalámbricas? ¿Existe una separación de la administración de las operaciones de sistemas y la de infraestructuras de red? ¿Existe un mecanismo de registro i monitorización de la red y los dispositivos que se conectan ella? ¿Hay un sistema de autenticación para todos los accesos a la red de la organización? ¿El sistema limita el acceso de personas autorizadas a aplicaciones / servicios legítimos? ¿Los usuarios se autentican adecuadamente al inicio de sesión? ¿Cómo se autentican los dispositivos de red? ¿Existe una segmentación de red adecuada usando cortafuegos, VLAN, VPN, etc.? ¿Se controlan los puertos y servicios utilizados para funciones de administración de sistemas?
A13.1.2	Seguridad de los servicios de red	? Desconocido		¿Se gestionan, clasifican y protegen los servicios de red de forma adecuada? ¿Existe un monitoreo de servicios de red? ¿Se mantiene un derecho a auditar servicios de red gestionados por terceros (contratos, SLA y requisitos de informes de gestión)? ¿Se emplean mecanismos de autenticación en la red, cifrado de tráfico de red? ¿Se hace una revisión periódica de las configuraciones de cortafuegos, IDS / IPS, WAF, DAM?
A13.1.3	Segregación en redes	? Desconocido		¿Existe una política de segmentación de red? ¿Qué tipo de segmentación existe? ¿Es basada en la clasificación, los niveles de confianza, dominios (público, escritorios, servidor, funciones, etc.)? ¿Cómo se monitorea y controla la segregación? ¿Se segmenta la red inalámbrica de la red física? ¿Y la red de invitados? ¿Hay controles adecuados entre ellos? ¿Cómo se controla la segmentación con proveedores y clientes? ¿La seguridad es adecuada dados los riesgos y el apetito de riesgo de la organización?

Estado y Aplicabilidad de controles de Seguridad de la Información

Sección	Controles de Seguridad de la Información	Estado	Recurso	Preguntas
A13.2	**Intercambio de información**			
A13.2.1	Políticas y procedimientos de intercambio de información	? Desconocido		¿Existen políticas y procedimientos relacionados con la transmisión segura de información? ¿Contempla mecanismos como correo electrónico, FTP y otras aplicaciones de transferencia de datos y protocolos Web (ej. Los grupos / foros, Dropbox y servicios en la nube similares), WiFi y Bluetooth, CD / DVD, almacenamiento externo USB, mensajería, etc.? ¿Está basado en la clasificación de la información? ¿Existen controles de acceso adecuados para esos mecanismos? ¿Cómo se implementa el uso de criptografía para los mecanismos aceptados (ej. TLS, cifrado de correo electrónico, ZIP codificados)? ¿Se sigue el principio de confidencialidad y privacidad? ¿Existen un programa de concientización, capacitación y cumplimiento?
A13.2.2	Acuerdos de intercambio de información	? Desconocido		Más allá de A.13.2.1 ¿Qué tipos de comunicaciones se implementan las firmas digitales? ¿Qué tipo de responsabilidades se asocian a la perdida, corrupción o divulgación de datos? ¿Existe una identificación y sincronización de los niveles de clasificación de información de todas las partes involucradas? ¿Cómo se mantiene una cadena de custodia para las transferencias de datos?
A13.2.3	Mensajería electrónica	? Desconocido		¿Existe una política de mensajería que cubra controles de intercambio de datos por comunicación de red, incluyendo correo electrónico y FTP / SFTP, etc.? ¿Hay controles de seguridad adecuados (ej. cifrado de correo electrónico, la autenticidad, la confidencialidad y la irrenunciabilidad de mensajes, etc.)? ¿Existen controles de seguridad para la interacción con sistemas Internet, Intranet relacionados con foros y tableros de anuncios electrónicos?
A13.2.4	Acuerdos de confidencialidad o no revelación	? Desconocido		¿Existen acuerdos de confidencialidad? ¿Han sido revisados y aprobados por el Departamento Legal? ¿Cuándo fueron revisados por última vez (periódicos o basados en cambios)? ¿Han sido aprobados y firmados por las personas adecuadas? ¿Existen sanciones adecuadas y acciones esperadas en caso de incumplimiento y / o beneficios por el cumplimiento (ej. una bonificación de rendimiento)?
A14	**Adquisición, desarrollo y mantenimiento de los sistemas de información**			
A14.1	**Requisitos de seguridad en los sistemas de información**			
A14.1.1	Análisis de requisitos y especificaciones de seguridad de la información	? Desconocido		¿Existen políticas, procedimientos y registros relacionados al análisis de requisitos de seguridad para la adquisición de sistemas y software? ¿Existen procedimientos para analizar riesgos, requisitos funcionales y técnicos, arquitectura de seguridad, las pruebas de seguridad y la certificación de sistemas y desarrollo? ¿Son estos procedimientos obligatorios para todos los nuevos desarrollos y cambios en los sistemas existentes (ej. Actualizaciones de sistema operativo / aplicaciones en las actualizaciones, cambios de criptografía, etc.) ¿Se aplican estos controles para sistemas / software comercial, incluidos los productos "a medida" o personalizados?
A14.1.2	Asegurar los servicios de aplicaciones en redes públicas	? Desconocido		¿La organización usa o proporciona aplicaciones web de comercio electrónico? ¿Se verifican los aspectos de seguridad como control de acceso y autenticación de usuarios, integridad de datos y la disponibilidad del servicio? ¿Contiene controles tales como validación de datos de entrada, validación de procesamiento, encriptación, autenticación de mensajes e irrenunciabilidad? ¿Se fuerza https? ¿Los sitios web públicos están siendo monitoreados (ej. eventos, vulnerabilidades, etc.)? ¿Se analizan y documentan las amenazas de forma rutinaria? ¿Existe una gestión de incidentes y cambios para tratarlos?
A14.1.3	Protección de las transacciones de servicios de aplicaciones	? Desconocido		Más allá de A.14.1.2 ¿Las transacciones se realizan y almacenan en un entorno interno seguro o expuesto a internet? ¿Se protege la información mediante el uso de protocolos seguros, cifrado, firma electrónica, etc.? ¿Cumplen con todos los requisitos legales, regulatorios y de cumplimiento?
A14.2	**Seguridad en el desarrollo y en los procesos de soporte**			
A14.2.1	Política de desarrollo seguro	? Desconocido		¿Existe una política de desarrollo seguro que abarque la arquitectura de seguridad? ¿Los entornos de desarrollo usan repositorios seguros con control de acceso, seguridad y control de cambios? ¿Los métodos de desarrollo incluyen pautas de programación segura? ¿Se capacita a los desarrolladores para que tengan el conocimiento adecuado acerca de las prácticas seguras de programación?
A14.2.2	Procedimiento de control de cambios en sistemas	? Desconocido		¿Existen políticas, procedimientos y registros relacionados de la gestión de cambios? ¿Incluyen planificación y prueba de cambios, evaluaciones de impacto (incluido el riesgo de información y aspectos de seguridad, más los impactos de no cambiar), verificaciones de instalación y procedimientos de retroceso / reversión? ¿Incluye un procedimiento para cambios de emergencia? ¿Se aplica los cambios significativos en equipos informáticos y de telecomunicaciones? ¿Los cambios en el sistema están debidamente documentados, justificados y autorizados por la administración?
A14.2.3	Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo	? Desconocido		¿Se requiere una validación / evaluaciones de riesgo y, si es necesario, recertificación de sistemas tras actualizaciones / mantenimiento, parches, cambios sistema operativo, actualizaciones de aplicaciones y cambios de cifrado? ¿Hay registros de estas actividades?
A14.2.4	Restricciones a los cambios en los paquetes de software	? Desconocido		¿Se hacen cambios a paquetes software adquiridos? ¿Se verifica que los controles originales no han sido comprometidos? ¿Se obtuvo el consentimiento y la participación del proveedor? ¿El proveedor continúa dando soporte tras los cambios? ¿Se exploró la posibilidad de obtener actualizaciones de programas estándar por parte de los proveedores? ¿Se hace una comprobación de compatibilidad con otro software en uso?
A14.2.5	Principios de ingeniería de sistemas seguros	? Desconocido		¿Se siguen principios de SDLC que incluye controles de seguridad? ¿Se capacita a los desarrolladores para que tengan el conocimiento adecuado acerca de las prácticas seguras de programación?
A14.2.6	Entorno de desarrollo seguro	? Desconocido		¿Se aíslan los entornos de desarrollo? ¿Cómo se desarrolla, prueba y lanza el software? ¿Quién es responsable de garantizar que el software nuevo / modificado no interrumpa otras operaciones? ¿Se realizan comprobaciones de antecedentes de los desarrolladores? ¿Tienen que cumplir con un NDA? ¿Cuáles son los reglamentos y los requisitos de cumplimiento que afectan el desarrollo? ¿Cómo se protegen los datos de prueba de la divulgación y dónde están almacenados?
A14.2.7	Externalización del desarrollo de software	? Desconocido		Más allá de A.14.2.6 ¿Se tienen en cuanta los siguientes aspectos cuando el desarrollo es lleva a cabo por un tercero? • Los acuerdos de licencia, la propiedad del código y los derechos de propiedad intelectual • Requisitos contractuales para prácticas seguras de diseño, desarrollo y prueba • Acceso al código fuente si el código ejecutable necesita ser modificado • Controles de prueba de seguridad de aplicaciones • Evaluación de vulnerabilidad y tratamiento
A14.2.8	Pruebas funcionales de seguridad de sistemas	? Desconocido		Más allá de A.14.2.7 ¿Existe un procedimiento de pruebas y verificación para sistemas nuevos y actualizados? ¿Tiene en cuenta acuerdos de licencia, propiedad del código y propiedad intelectual?
A14.2.9	Pruebas de aceptación de sistemas	? Desconocido		¿Se efectúan pruebas de seguridad antes de la introducción de nuevos sistemas en la red? ¿Las pruebas replican situaciones y entornos operativos realistas? ¿Los defectos relacionados con la seguridad son tratados antes de que el producto sea certificado / aprobado? ¿Hay pruebas de aceptación del usuario (UAT) antes del lanzamiento al entorno operativo? ¿Se actualizan los controles de resiliencia y recuperación tras incidentes para reflejar los sistemas nuevos, modificados y retirados?
A14.3	**Datos de prueba**			

Estado y Aplicabilidad de controles de Seguridad de la Información

Sección	Controles de Seguridad de la Información	Estado	Recurso	Preguntas
A14.3.1	Protección de los datos de prueba	? Desconocido		¿Se utilizan mecanismos para proteger datos de prueba como la seudonimización, enmascaramiento, datos falsos, borrado, etc.? ¿Existe un mecanismo de verificación y aprobación para el uso de datos no protegidos para pruebas? ¿Existen registros de estas actividades?
A15	**Relación con proveedores**			
A15.1	**Seguridad en las relaciones con proveedores**			
A15.1.1	Política de seguridad de la información en las relaciones con los proveedores	? Desconocido		¿Existen políticas, procesos, prácticas y registros relacionados con la gestión de relaciones con proveedores que involucran servicios de TI? ¿Incluyen servicios de nube, logística, servicios públicos, recursos humanos, médicos, financieros, legales y otros servicios subcontratados de alto riesgo? ¿Los contratos y acuerdos abordan lo siguiente? • Arreglos de gestión de relaciones, incluyendo el riesgo de la información y los aspectos de seguridad, la métrica, el rendimiento, problemas, rutas de escalada • Información / propiedad intelectual, y obligaciones / limitaciones derivadas • Rendición de cuentas y responsabilidades relacionadas con el riesgo y la seguridad de la información • Requisitos legales y normativos, como el cumplimiento certificado de ISO 27001 • Identificación de controles físicos y lógicos • Gestión de eventos, incidentes y desastres incluyendo evaluación, clasificación, priorización, notificación, escalado, gestión de respuesta y aspectos de continuidad del negocio • Habilitación de seguridad de los empleados y concienciación • Derecho de auditoría de seguridad por parte de la organización ¿Existe una obligación contractual de cumplimento? ¿Los proveedores de servicios externos son monitoreados rutinariamente y auditados para cumplir con los requisitos de seguridad?
A15.1.2	Requisitos de seguridad en contratos con terceros	? Desconocido		¿Los contratos o acuerdos formales con proveedores cubren lo siguiente? • Gestión de las relaciones, incluyendo riesgos • Cláusulas de confidencialidad vinculantes • Descripción de la información que se maneja y el método de acceder a dicha información • Estructura de la clasificación de la información a usar • La Inmediata notificación de incidentes de seguridad • Aspectos de continuidad del negocio • Subcontratación y restricciones en las relaciones con otros proveedores • Aspectos de personal y RRHH (ej. Rendimiento, antecedentes, "robo de empleados", etc.)
A15.1.3	Cadena de suministro de tecnología de la información y de las comunicaciones	? Desconocido		Más allá de A.15.1.1 y A.15.1.2 ¿Cómo se validan los requisitos de seguridad de los productos o servicios adquiridos? ¿Cómo se logra una capacidad de recuperación cuando productos o servicios críticos son suministrados por terceros? ¿Se puede rastrear el origen del producto o servicio?
A15.2	**Gestión de la provisión de servicios del proveedor**			
A15.2.1	Control y revisión de la provisión de servicios del proveedor	? Desconocido		¿Existe una monitorización de servicios y quien responsable de esta actividad? ¿Se llevan a cabo reuniones de revisión del servicio, con qué frecuencia? ¿Se generan informes y / o métricas relacionadas a las reuniones y las decisiones tomadas? ¿Las reuniones abarcan riesgos, incidentes, políticas, cumplimiento e informes de auditoría? ¿Existen cláusulas de penalización o de bonificación en el contrato relacionadas con el riesgo de la información?
A15.2.2	Gestión de cambios en la provisión del servicio del proveedor	? Desconocido		¿Cómo se comunican cambios en los servicios relacionados con la información, servicios adicionales o cambios en la forma en que se prestan los servicios contratados? ¿Cómo se comunican cambios en las políticas y requerimientos legales de la organización? ¿Se actualizan los acuerdos relacionados con los cambios?
A16	**Gestión de incidentes de seguridad de la información**			
A16.1	**Gestión de incidentes de seguridad de la información y mejoras**			
A16.1.1	Responsabilidades y procedimientos	? Desconocido		¿Existen políticas, procedimientos e ITT´s para la gestión de incidentes? ¿Qué cubre? • I plan de respuesta a incidentes • Puntos de contacto para la notificación de incidentes, seguimiento y evaluación • Monitoreo, detección y reporte de eventos de seguridad • Asignación y escalado de incidentes (N1 > N2) incluyendo las respuestas de emergencia y la continuidad de negocio • Método de recolección de evidencias y pruebas forenses digitales • Revisión post-evento de seguridad y procesos de aprendizaje / mejora ¿Existen evidencias de la notificación de incidentes, registro, clasificación, asignación de resolución, la mitigación y la confirmación de cierre?
A16.1.2	Notificación de los eventos de seguridad de la información	? Desconocido		¿Cómo se informan los eventos de seguridad de la información? ¿Son conscientes los trabajadores de la necesidad de informar de inmediato y lo hacen? ¿Se crean informes de seguimiento de los incidentes? Desde la detección a la resolución. ¿Qué pasa con esos informes?
A16.1.3	Notificación de puntos débiles de la seguridad	? Desconocido		Más allá de A.16.1.2 ¿Existe una obligación contractual por parte de los empleados para reportar cualquier tipo de ocurrencia inusual? ¿Las políticas prohíben explícitamente a los trabajadores 'verificar', 'explorar', 'validar' o 'confirmar' vulnerabilidades a menos que estén expresamente autorizados para hacerlo?
A16.1.4	Evaluación y decisión sobre los eventos de seguridad de información	? Desconocido		¿Qué tipos de eventos se espera que informen los empleados? ¿A quién informan? ¿Cómo se evalúan estos eventos para decidir si califican como incidentes? ¿Hay una escala de clasificación? ¿Hay un proceso de clasificación y / o escalamiento para priorizar los incidentes graves? ¿En qué se basa?
A16.1.5	Respuesta a incidentes de seguridad de la información	? Desconocido		¿Cómo se recolecta, almacena y evalúa la evidencia? ¿Hay una matriz de escalación para usar según sea necesario? ¿Hay medios para comunicar información de tales incidentes a las organizaciones internas y externas pertinentes? ¿Se documentan las acciones tomadas para resolver y finalmente cerrar un incidente?
A16.1.6	Aprendizaje de los incidentes de seguridad de la información	? Desconocido		¿Existe un proceso de evaluación / investigación para identificar incidentes de impacto recurrentes? ¿Se aprovecha la información obtenida de la evaluación de incidentes para evitar recurrencias? Además, ¿Se está utilizado para formación y concienciación? ¿La organización cuenta con un proceso de gestión de incidentes relativamente maduro? ¿Se está aprendiendo de forma proactiva de incidentes, mejorando los conocimientos de riesgo y los controles de seguridad?
A16.1.7	Recopilación de evidencias	? Desconocido		¿La recolección de evidencias de hace de forma competente en la empresa o por terceros especializados y capacitados en esta área? ¿Haya personal capacitado, competente y confiable con herramientas adecuadas y procesos definidos para el rol? (cadena de evidencia rigurosamente mantenida, evidencia asegurada en almacenamiento, herramientas y técnicas) ¿Quién decide emprender un análisis forense, y en qué criterio se base? ¿Existen obligaciones relacionadas con la jurisdicción, las diferentes normas forenses y los requisitos legales asociados?
A17	**Aspectos de seguridad de la información para la gestión de la continuidad de negocio**			
A17.1	**Continuidad de la seguridad de la información**			

Estado y Aplicabilidad de controles de Seguridad de la Información

Sección	Controles de Seguridad de la Información	Estado	Recurso	Preguntas
A17.1.1	Planificación de la continuidad de la seguridad de la información	? Desconocido		¿Cómo se determinan los requisitos de continuidad del negocio? ¿Existe un plan de continuidad de negocio? ¿Existen un diseño adecuado de "alta disponibilidad" para sistemas de TI, redes y procesos críticos? ¿Se identifica el impacto potencial de los incidentes? ¿Se evalúan los planes de continuidad del negocio? ¿Se llevan a cabo ensayos de continuidad?
A17.1.2	Implementar la continuidad de la seguridad de la información	? Desconocido		¿Los planes tienen plazos definidos para restaurar servicios tras una interrupción? ¿Los planes tienen en cuenta la identificación y el acuerdo de responsabilidades, la identificación de pérdidas aceptables, la implementación de procedimientos de recuperación y restauración, la documentación de procedimientos y las pruebas regulares? ¿La planificación de la continuidad es consistente e identifica las prioridades de restauración? ¿Tienen los miembros de los equipos de recuperación / gestión de crisis / incidentes conocimiento de los planes y tienen claro sus roles y responsabilidades? ¿Los controles de seguridad son adecuados en los sitios de recuperación de desastres remotos?
A17.1.3	Verificación, revisión y evaluación de la continuidad de la seguridad de la información	? Desconocido		¿Existe un método de pruebas del plan de continuidad? ¿Con qué frecuencia se llevan a cabo dichas pruebas? ¿Hay evidencia de las pruebas reales y sus resultados? ¿Se han identificado deficiencias?, ¿Se han remediado? y ¿Se han vuelto a probar hasta que los resultados sean satisfactorios?
A17.2	**Redundancias**			
A17.2.1	Disponibilidad de los recursos de tratamiento de la información	? Desconocido		¿Cómo se identifican los requisitos de disponibilidad de servicios? ¿Se tienen en cuenta la capacidad de recuperación, la capacidad de rendimiento, el balanceo de carga? ¿Se tienen en cuenta servicios poco fiables, equipos, instalaciones, servidores, aplicaciones, enlaces, funciones, y la organización en sí? ¿Los controles clave de seguridad de la información están implementados y son funcionales en los sitios de recuperación de desastres?
A18	**Cumplimiento**			
A18.1	**Cumplimiento de los requisitos legales y contractuales**			
A18.1.1	Identificación de la legislación aplicable y de los requisitos contractuales	? Desconocido		¿Existe una política acerca del cumplimiento de requisitos legales? LOPD, GDPR, etc. ¿Se mantiene un registro o base de datos de cumplimiento enumerando todas las obligaciones, expectativas legales, reglamentarias y contractuales aplicables? ¿Hay una persona encargada de mantener, usar y controlar el registro? ¿Cómo se logra y se garantiza el cumplimiento? ¿Existen controles adecuados para cumplir con los requisitos?
A18.1.2	Derechos de Propiedad Intelectual (DPI)	? Desconocido		¿Existen políticas y procedimientos relativos a la adquisición, el uso y licencias de propiedad intelectual, gestión de licencias y cumplimiento?
A18.1.3	Protección de los registros de la organización	? Desconocido		¿Existe una política que contemple lo siguiente? Clasificación, categorización, períodos de retención y medios de almacenamiento permitidos. ¿Se almacenan las firmas digitales de forma segura? ¿Se contempla la posibilidad de destrucción, falsificación y acceso no autorizado? ¿Se verifica periódicamente la integridad de los registros? ¿Se utilizan medios de almacenamiento de larga duración para el almacenamiento a largo plazo?
A18.1.4	Protección y privacidad de la información de carácter personal	? Desconocido		¿Hay un mecanismo para instruir al personal en el manejo de información de carácter personal? ¿Hay un responsable de privacidad en la organización? ¿Es el responsable conocedor de la información de carácter personal que es recopilado, procesado y almacenados por la organización? ¿Cuáles son los controles de acceso a información de carácter personal? ¿Cuál es el nivel de acceso y roles (de personal) que tienen acceso a estos activos?
A18.1.5	Regulación de los controles criptográficos	? Desconocido		¿Existe una política que cubra actividades relacionadas con importación / exportación de material criptográfico? ¿Estas actividades cumplen con los requisitos legales y reglamentarios?
A18.2	**Revisiones de la seguridad de la información**			
A18.2.1	Revisión independiente de la seguridad de la información	? Desconocido		¿Están las prioridades de implementación de controles alineadas con los riesgos a activos de información? ¿Los requisitos de auditoría de sistemas son cuidadosamente planificados, autorizados, implementados y controlados para minimizar los riesgos? ¿Están los objetivos y el alcance de auditoria autorizados por la gerencia? ¿Está adecuadamente controlado el acceso a las herramientas / software de auditoría del sistema de información? ¿Se documentan los hallazgos de auditoría y las actuaciones para solventarlos?
A18.2.2	Cumplimiento de las políticas y normas de seguridad	? Desconocido		¿Cómo garantizar que todos los procedimientos de seguridad dentro de un área de responsabilidad se llevan a cabo correctamente? ¿Se hace una verificación periódica?
A18.2.3	Comprobación del cumplimiento técnico	? Desconocido		¿Se llevan a cabo escaneos de vulnerabilidades de red y pruebas de Pentesting regulares? ¿Las pruebas son realizadas por profesionales debidamente cualificados, competentes y confiables? ¿Cómo informa, analiza y utilizan los resultados de dichas pruebas? ¿La prioridad de tratamiento se basa en un análisis de riesgos? ¿Hay evidencias de medidas tomadas para abordar los problemas identificados?
		114		Número de Controles