



UNIVERSITAT
POLITÈCNICA
DE VALÈNCIA



UNIVERSITAT POLITÈCNICA DE VALÈNCIA

Escuela Técnica Superior de Ingeniería Informática

Creación de un cuestionario de revisión de estado de los
controles de la Norma ISO27001 para una empresa pública
o privada.

Trabajo Fin de Máster

Máster Universitario en Ciberseguridad y Ciberinteligencia

AUTOR/A: Meana Serrano, Helios Miguel

Tutor/a: Oltra Gutiérrez, Juan Vicente

CURSO ACADÉMICO: 2023/2024



UNIVERSITAT
POLITÈCNICA
DE VALÈNCIA



Escola Tècnica
Superior d'Enginyeria
Informàtica

Escola Tècnica Superior d'Enginyeria Informàtica
Universitat Politècnica de València

Agradecimientos

Gracias a mi familia por sus innumerables esfuerzos que me han permitido dar este gran paso en mi vida y como no podía ser de otra forma, gracias por su apoyo incondicional.

Gracias también a todos y cada uno de mis compañeros de trabajo por la gran acogida que he recibido desde el primer día y sobre todo por todo lo que he aprendido, y continuo aprendiendo de vosotros día a día.

Agradecer también a mi tutor Juan Vicente Oltra, por su esfuerzo y predisposición en todo momento.



Resumen

En los últimos años la sociedad cada vez ha sido más consciente de una nueva dimensión de amenazas que acechan a su seguridad, sostenibilidad y por consiguiente a su actividad económica: las ciber amenazas o ataques cibernéticos.

Este tipo de amenazas han aparecido y evolucionado en paralelo con la expansión digital. Hoy en día, las empresas y gobiernos de todos los países del mundo destinan gran cantidad de recursos a combatirlas para de esta forma proteger sus intereses y su desarrollo. Fruto de esta situación, nace la necesidad de establecer una norma internacional que recoja una serie de buenas prácticas para combatirlas desde un punto de vista estructural y organizativo. En el 2005 de la mano de la International Organization for Standardization y de la International Electrotechnical Commission nace la norma ISO 27001.

El presente Trabajo Fin de Máster, en lo sucesivo, TFM, tiene como objetivo la realización de un cuestionario automático de cara a facilitar a empresas públicas o privadas una herramienta de autoevaluación automática del estado de implementación de la norma ISO 27001. De esta forma, de una manera rápida sencilla y eficaz la empresa objeto de la auditoría podrá conocer cuáles son los puntos necesarios de mejora para obtener la certificación pertinente, lo que consecuentemente hará más eficientes las conversaciones con la empresa certificadora, al poseer la empresa objeto de la auditoría, un mayor grado de conocimiento de su estado de implementación.

Para la realización de la herramienta se ha considerado la opción más adecuada por su versatilidad y conocimiento del público en general, la herramienta Microsoft Excel, la cual haciendo uso de las Macro de Visual Basics ha permitido obtener los resultados en formato PDF.

Palabras Clave: herramienta, automática, autoevaluación, estándares, ciberseguridad, empresas, seguridad de la información.



Abstract

In recent years, society has become increasingly aware of a new dimension of threats to its security, sustainability and consequently to its economic activity: cyber threats or cyber-attacks.

These threats have emerged and evolved in parallel with digital expansion. Nowadays, companies and governments in all countries of the world devote a great deal of resources to combat them in order to protect their interests and their development. As a result of this situation, there is a need to establish an international standard that includes a series of good practices to combat them from a structural and organizational point of view. In 2005, the International Organization for Standardization and the International Electrotechnical Commission created the ISO 27001 standard.

The aim of this master's Thesis, hereinafter referred to as TFM, is to create an automatic questionnaire to provide public or private companies with an automatic self-assessment tool for the implementation status of the ISO 27001 standard. In this way, in a quick, simple and effective way, the audited company will be able to know which points need to be improved in order to obtain the relevant certification, which will consequently make the conversations with the certifying company more efficient, as the audited company will have a greater degree of knowledge of its implementation status.

For the creation of the tool, Microsoft Excel was considered the most suitable option due to its versatility and knowledge of the general public, which by using Visual Basics Macros has allowed us to obtain the results in PDF format.

Keywords: tool, automatic, self-assessment, standards, cybersecurity, companies, information security.



En els últims anys, la societat cada vegada ha sigut més conscient d'una nova dimensió d'amenaques que assetgen la seua seguretat, sostenibilitat i, per tant, la seua activitat econòmica: les ciberamenaces o atacs cibernètics.

Aquest tipus d'amenaques han aparegut i evolucionat en paral·lel amb l'expansió digital. Hui en dia, les empreses i els governs de tots els països del món destinen una gran quantitat de recursos a combatre-les per tal de protegir els seus interessos i el seu desenvolupament. Com a resultat d'aquesta situació, naix la necessitat d'establir una norma internacional que arreplegue una sèrie de bones pràctiques per a combatre-les des d'un punt de vista estructural i organitzatiu. En 2005, de la mà de la International Organization for Standardization i de la International Electrotechnical Commission, naix la norma ISO 27001.

El present Treball de Fi de Màster, d'ara en avant, TFM, té com a objectiu la realització d'un qüestionari automàtic per a facilitar a empreses públiques o privades una eina d'autoavaluació automàtica de l'estat d'implementació de la norma ISO 27001. D'aquesta manera, de manera ràpida, senzilla i eficaç, l'empresa objecte de l'auditoria podrà conèixer quins són els punts necessaris de millora per a obtenir la certificació pertinent, la qual cosa, consegüentment, eficientarà les converses amb l'empresa certificadora, en posseir l'empresa objecte de l'auditoria un major grau de coneixement del seu estat d'implementació.

Per a la creació de l'instrument, el Microsoft Excel es considerarà la possibilitat d'omplir most sobre la seva versatilitat i experiència en general, que mitjançant Visual Basics Macros s'obté per obtenir resultats en format PDF.

Paraules Clau: eina, automàtica, autoavaluació, estàndards, ciberseguretat, empreses, seguretat de la informació

Tabla de contenido

Resumen	3
Abstract.....	4
Resum	5
1. Introducción	10
1.1. Motivación.....	12
1.2. Objetivos.....	13
1.3. Estructura de la memoria	14
2. Estado del arte.....	15
2.1. Evolución histórica de la ciberseguridad.....	15
2.1.1. El nacimiento de Internet: ARPANET.....	15
2.1.2. El primer virus autónomo informático: El Gusano Morris	15
2.1.3. La comercialización de Internet: el nacimiento de WWW.....	16
2.1.4. La aparición de las primeras normativas: desde la BS-7799 a la ISO 27001	17
2.2. Evolución de la norma ISO 27001.....	18
2.2.1. <i>ISO/IEC 27001:2005</i> : La primera versión.....	18
2.2.2. Norma UNE-ISO/IEC 27001:2007 “Sistemas de Gestión de la Seguridad de la Información (SGSI). Requisitos”	18
2.2.3. Primera reforma de la ISO 27001: <i>ISO/IEC 27001:2013</i>	18
2.2.4. Norma UNE-ISO/IEC 27001:2017 “Sistemas de Gestión de la Seguridad de la Información (SGSI). Requisitos”	19
2.2.5. Análisis de la implantación de la ISO 27001.....	21
2.3. Otras normativas: ENS.....	24
2.3.1. ENS: Esquema Nacional de Seguridad	24
3. Solución Propuesta	26
3.1. Estructura de la herramienta	27
3.1.1. Introducción.....	27
3.1.2. Instrucciones.....	28
3.1.3. Información General.....	28
3.1.4. Formulario	29



3.1.5. Resumen	44
3.1.6. Resultados	45
3.2. Funcionamiento y navegación de la herramienta.....	46
3.3. Análisis y obtención de resultados	50
4. Conclusiones.....	56
4.1. Posibles Mejoras.....	57
4.2. Posibles Trabajos	58
Anexo I	59
ANEXO OBJETIVOS DE DESARROLLO SOSTENIBLE	60
Bibliografía	63



Índice de Figuras

ILUSTRACIÓN 1. EVOLUCIÓN PIB MUNDIAL (2006-2022). FUENTE: BANCOMUNDIAL.....	21
ILUSTRACIÓN 2. EVOLUCIÓN Nº CERTIFICADOS ISO 27001 (2006-2016). FUENTE: NORMAISO27001	22
ILUSTRACIÓN 3. COMPARATIVA DE CRECIMIENTO PIB-NºCERT. FUENTE: ELABORACIÓN PROPIA.....	23
ILUSTRACIÓN 4. ENS. FUENTE: AENOR	25
ILUSTRACIÓN 5. HOJA "INTRODUCCIÓN". FUENTE: ELABORACIÓN PROPIA	27
ILUSTRACIÓN 6. HOJA "INSTRUCCIONES". FUENTE: ELABORACIÓN PROPIA	28
ILUSTRACIÓN 7. HOJA "INFORMACIÓN GENERAL". FUENTE: ELABORACIÓN PROPIA	29
ILUSTRACIÓN 8. HOJA "5. POLITICAS DE SEGURIDAD DE LA INFORMACIÓN". FUENTE: ELABORACIÓN PROPIA	30
ILUSTRACIÓN 9. HOJA "ORGANIZACIÓN SEG. INFORMACIÓN". FUENTE: ELABORACIÓN PROPIA	30
ILUSTRACIÓN 10. HOJA "7. SEGURIDAD RELATIVA A LOS RECURSOS HUMANOS". FUENTE: ELABORACIÓN PROPIA	31
ILUSTRACIÓN 11. HOJA "8. GESTIÓN DE ACTIVOS". FUENTE: ELABORACIÓN PROPIA	32
ILUSTRACIÓN 12. HOJA "9. CONTROL DE ACCESO". FUENTE: ELABORACIÓN PROPIA	33
ILUSTRACIÓN 13. HOJA "9. CONTROL DE ACCESO". FUENTE: ELABORACIÓN PROPIA	34
ILUSTRACIÓN 14. HOJA "10. CRIPTOGRAFÍA". FUENTE: ELABORACIÓN PROPIA.....	34
ILUSTRACIÓN 15. HOJA 11 "SEGURIDAD FÍSICA Y ENTORNO". FUENTE: ELABORACIÓN PROPIA.....	35
ILUSTRACIÓN 16. HOJA "12. SEGURIDAD DE LAS OPERACIONES". FUENTE: ELABORACIÓN PROPIA	36
ILUSTRACIÓN 17. HOJA "12. SEGURIDAD DE LAS OPERACIONES". FUENTE: ELABORACIÓN PROPIA	37
ILUSTRACIÓN 18. HOJA "13. SEGURIDAD DE LAS COMUNICACIONES". FUENTE: ELABORACIÓN PROPIA .	38
ILUSTRACIÓN 19. HOJA " 14. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN". FUENTE: ELABORACIÓN PROPIA.....	39
ILUSTRACIÓN 20. HOJA " 14. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN". FUENTE: ELABORACIÓN PROPIA.....	40
ILUSTRACIÓN 21. HOJA "15. RELACIÓN CON PROVEEDORES". FUENTE: ELABORACIÓN PROPIA.....	40
ILUSTRACIÓN 22. HOJA "16. GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN ". FUENTE: ELABORACIÓN PROPIA.....	41
ILUSTRACIÓN 23. HOJA "17. ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN PARA LA GESTIÓN DE LA CONTINUIDAD DE NEGOCIO ". FUENTE: ELABORACIÓN PROPIA	42
ILUSTRACIÓN 24. HOJA "18. CUMPLIMIENTO". FUENTE: ELABORACIÓN PROPIA	43
ILUSTRACIÓN 25. HOJA "RESUMEN". FUENTE: ELABORACIÓN PROPIA.....	44
ILUSTRACIÓN 26. HOJA "RESULTADOS". FUENTE: ELABORACIÓN PROPIA.....	45
ILUSTRACIÓN 27. PROCEDIMIENTO 1. FUENTE: ELABORACIÓN PROPIA	46
ILUSTRACIÓN 28. PROCEDIMIENTO 2. FUENTE: ELABORACIÓN PROPIA	47
ILUSTRACIÓN 29. PROCEDIMIENTO 3. FUENTE: ELABORACIÓN PROPIA	47



ILUSTRACIÓN 30. PROCEDIMIENTO 4. FUENTE: ELABORACIÓN PROPIA	48
ILUSTRACIÓN 31. PROCEDIMIENTO 5. FUENTE: ELABORACIÓN PROPIA	48
ILUSTRACIÓN 32. PROCEDIMIENTO 6. FUENTE: ELABORACIÓN PROPIA	48
ILUSTRACIÓN 33. PROCEDIMIENTO 7. FUENTE: ELABORACIÓN PROPIA	49
ILUSTRACIÓN 34. PROCEDIMIENTO 8. FUENTE: ELABORACIÓN PROPIA	49
ILUSTRACIÓN 35. ANÁLISIS Y OBTENCIÓN DE RESULTADOS 1. FUENTE: ELABORACIÓN PROPIA	50
ILUSTRACIÓN 36. ANÁLISIS Y OBTENCIÓN DE RESULTADOS 2. FUENTE: ELABORACIÓN PROPIA	51
ILUSTRACIÓN 37. ANÁLISIS Y OBTENCIÓN DE RESULTADOS - EJEMPLO 1. FUENTE: ELABORACIÓN PROPIA	51
ILUSTRACIÓN 38. ANÁLISIS Y OBTENCIÓN DE RESULTADOS - EJEMPLO 2. FUENTE: ELABORACIÓN PROPIA	52
ILUSTRACIÓN 39. ANÁLISIS Y OBTENCIÓN DE RESULTADOS - EJEMPLO 3. FUENTE: ELABORACIÓN PROPIA	52
ILUSTRACIÓN 40. VISIONADO DE RESULTADOS 1. FUENTE: ELABORACIÓN PROPIA.....	53
ILUSTRACIÓN 41. VISIONADO DE RESULTADOS 2. FUENTE: ELABORACIÓN PROPIA.....	53
ILUSTRACIÓN 42. VISIONADO DE RESULTADOS 3. FUENTE: ELABORACIÓN PROPIA.....	54
ILUSTRACIÓN 43. FUNCIÓN GENERARPDF(). FUENTE: ELABORACIÓN PROPIA	54



1. Introducción

Desde la aparición de las primeras tecnologías informáticas, fruto de su gran utilidad para nuestra sociedad han sido objeto de deseo y control. Con el nacimiento y posterior auge de internet, estos activos digitales han sido cada vez fruto de mayores ataques indeseados. A finales de la década de los 60 se comenzó a acuñar el término estando en un primer momento orientado a la protección física de los activos digitales y en el control de acceso.

Sería ya en el 1980 cuando alcanzaría mayor importancia a raíz de que se comenzase a producir la expansión de las redes y por consiguiente también la aparición de los primeros virus informáticos, los cuáles continuaron desarrollándose hasta nuestros días, alcanzando un punto crítico con la proliferación y expansión de internet a partir de 1990.

Fruto de esta expansión y proliferación de internet en paralelo se expandieron consecuentemente las diversas amenazas cibernéticas que también provocaron que se comenzasen a desarrollar las primeras defensas para esta serie de nuevas amenazas, defensas que alcanzaron su primer gran hito con la creación del primer antivirus en 1987.

Ya en tiempos más recientes, en el siglo XXI el campo de la ciberseguridad se expandió rápidamente, abarcando desde la protección contra malware, hasta la seguridad de la información personal y corporativa. Por ello hoy en día, las empresas y gobiernos de todos los países del mundo destinan gran cantidad de recursos a combatirlas para de esta forma proteger sus intereses y su desarrollo.

Fruto de esta situación, nace la necesidad de establecer una norma internacional que recoja una serie de buenas prácticas para combatirlas desde un punto de vista estructural y organizativo. Lo que se traduce como un conjunto de procedimientos formalizados y aprobados por las propias empresas de obligado cumplimiento para todos los dispositivos de las empresas. En el 2005 de la mano de la International Organization for Standardization y de la International Electrotechnical Commission nace la norma ISO 27001.

La norma ISO 27001 es un estándar internacional que establece los requisitos para la implementación, mantenimiento y mejora continua de un Sistema de Gestión de la Seguridad de la Información (SGSI). Este sistema se utiliza para proteger la confidencialidad, integridad y disponibilidad de la información. La norma proporciona un marco para la seguridad de la información que ayuda a las organizaciones a identificar y gestionar sus riesgos de seguridad de la información de manera efectiva. («ISO 27001 - Certificado ISO 27001 punto por punto - Presupuesto Online» 2024)



Para la realización de la presente herramienta, se ha fundamentado en el sólido marco normativo proporcionado por la norma *UNE-ISO/IEC 27001:2017 "Sistemas de Gestión de la Seguridad de la Información (SGSI). Requisitos"*. Que se trata de la versión normalizada por la Asociación Española de Normalización (UNE). («ISO/IEC 27001» 2024)

Es la norma principal de requisitos de un Sistema de Gestión de Seguridad de la Información, adicionalmente, en su *Anexo A*, contempla una lista con los objetivos de control y controles que desarrolla la ISO 27002, que son el principal objeto de estudio de esta herramienta de autoevaluación.

Dado que cada empresa muestra unas particularidades de acuerdo con múltiples factores, este TFM será planteando desde un punto de vista general, centrándose en dar apoyo a las fases 5 y 6 de una auditoría certificadora de ISO 27001.



1.1. Motivación

De acuerdo con todo lo mencionado anteriormente, es fácilmente concluyente la importancia de un entorno ciberseguro para todos los usuarios de un entorno digital, ya sea desde una gran empresa hasta el último consumidor. Si existe el medio de ataque, existe el riesgo o lo que es lo mismo, no existe el riesgo cero.

Ahora bien, a título personal, durante este último año he podido realizar mis prácticas de empresa como Auditor IT, donde he podido estar en contacto con múltiples empresas de distintos tamaños y tipos. A través de esta experiencia, he podido apreciar como multitud de empresas destinan grandes cantidades de recursos a novedosas soluciones perimetrales de ciberseguridad, si bien en algunos casos estas soluciones no resultan tan eficientes como se pensaría en un inicio. En muchas ocasiones la causa de esta falta de eficiencia no recaía en que la solución de ciberseguridad fuese mala o ineficiente sino en una aparente falta de formalización en la seguridad a nivel organizativo y procedimental. Esta formalización en gran medida hace especialmente hincapié en la parte más vulnerable del eslabón, nosotros, los usuarios.

Adicionalmente, en alguna ocasión estos problemas podrían ser fácilmente mejorados en base a una correcta adecuación a alguno de estos estándares que recogen un conjunto de best practices para cualquier empresa.

En definitiva, se pretende crear una herramienta de autoevaluación generalista, sencilla e intuitiva, con el fin de que cualquier responsable de la empresa auditada pueda emplear y así obtener fácilmente unos resultados gráficos del estado de implementación del estándar ISO 27001, facilitando también por consiguiente la labor de la empresa auditora.



1.2. Objetivos

En este apartado se ahondará en los principales objetivos a cubrir por el presente TFM. Para ello es de especial criticidad diferenciar entre el objetivo principal que persigue y los objetivos secundarios.

El objetivo principal que persigue este TFM sería la realización de un cuestionario automático de autoevaluación de la norma ISO 27001 destinado a la empresa pública o privada. Este cuestionario tendría como objetivo proporcionar un conocimiento más profundo del estatus de las medidas restantes a adoptar o implementar para poder obtener la certificación ISO27001 tanto a la empresa objeto de la auditoría como a la empresa certificadora.

A continuación se desglosan los objetivos secundarios:

- Realizar una revisión del marco normativo de una auditoría ISO27001.
- Hacer más eficiente la planificación de una certificación de la ISO27001 a través de un enfoque sencillo e incorporando herramientas automáticas.
- Realizar automatizaciones que mejoren la eficiencia del cuestionario a través de las funciones Macro de Microsoft Excel.

Adicionalmente, el presente TFM ha perseguido un objetivo adicional para el caso concreto de empresas que deseen obtener la certificación ISO 27001 o revisar su estado de implementación en el momento de la auditoría y que ya disponen de la certificación ENS. Dado que la certificación ENS es un esquema inspirado en la familia de estándares ISO 27000 y, más concretamente, en la ISO 27001, si se tiene la certificación ENS esta certificación ya garantiza la cumplimentación de gran cantidad de los controles que cubre la ISO 27001, por lo tanto, el cuestionario podría contemplar esta situación.

A continuación, se desglosan los objetivos secundarios adicionales fruto de esta nueva situación.

- Revisión del marco normativo de una auditoría ENS.
- Mapeo de controles de la norma ISO 27001 en función de la certificación ENS.



1.3. Estructura de la memoria

En este subapartado se detallará la estructura que compone esta memoria. Esta memoria se encuentra dividida en cuatro apartados principales ordenados según el nivel de abstracción de estos, estos apartados se componen de subapartados y subsubapartados.

El primer apartado sería el correspondiente a la introducción. En este apartado se detallará la motivación que persigue este TFM así como los objetivos que trata de satisfacer.

En el segundo apartado será el correspondiente al Estudio del Arte. Este apartado tendrá como principal objetivo proporcionar una visión de la situación actual de la normativa sobre la que se fundamenta el TFM a través de aportar un contexto tecnológico e histórico que evidencie las necesidades que solventa la solución aportada.

El tercer apartado de esta memoria es el más importante del presente TFM, en este apartado se detallará la solución propuesta para la realización de este TFM. Se explica la estructura de la solución, herramientas utilizadas, así como el procedimiento seguido hasta la obtención y el visionado de resultados.

El cuarto apartado es el correspondiente a las conclusiones, en el cual se detallan las conclusiones y aprendizajes obtenidos mediante la realización del presente TFM así como las posibles mejoras adicionales o posibles futuros trabajos nacidos de este.

Finalmente, se proporciona en el Anexo 1, el código correspondiente a la función GenerarPDF() y el Anexo ODS.



2. Estado del arte

El presente apartado tendrá como objetivo proporcionar una visión de la situación actual de la normativa sobre la que se fundamenta el TFM a través de aportar un contexto tecnológico que evidencie las necesidades que solventa la solución aportada.

Asimismo, se estructurará en dos subapartados diferenciados entre sí a fin de poder ofrecer una vista más estructurada y concisa del contexto histórico que engloba a este trabajo.

2.1. Evolución histórica de la ciberseguridad

En el presente apartado se estudiará la evolución histórica de la ciberseguridad y como esta evolución ha acabado por desarrollar el marco normativo que la rige y califica hoy en día.

2.1.1. El nacimiento de Internet: ARPANET

El nacimiento de Internet se podría establecer como el primer gran hito en la evolución histórica de la ciberseguridad. Internet nació fruto de un proyecto militar conocido como ARPANET en los años 60, diseñado para compartir información de manera eficiente y segura entre varias ubicaciones, con todas las ventajas que eso suponía desde un punto bélico en aquella época. («ARPANET») Por aquel entonces sería cuando se comenzó a acuñar el término “Ciberseguridad” estando en un primer momento más orientado a la protección física de los activos digitales y en el control de acceso. (Bastero 2024)

2.1.2. El primer virus autónomo informático: El Gusano Morris

En noviembre de 1988, un nuevo acontecimiento cambio totalmente la perspectiva y la propia índole de la ciberseguridad, el Gusano Morris, considerado el primer virus informático hizo su aparición.

Haciendo uso de la red ARPANET, un estudiante de la universidad de Connel con el objetivo de conocer el verdadero tamaño de la red infectó un 10% de los ordenadores de esta, o lo que es lo mismo, unas 6000 computadoras, causando por error una gran ralentización de estos equipos y con ello grandes pérdidas económicas.



Lo más novedoso fue el propio modelo de este ataque, el cual haciendo uso de vulnerabilidades conocidas permitía al virus ir accediendo de una computadora a otra infectándolas en el proceso.(Sánchez 2024)

A raíz de este suceso, el cual supuso un antes y un después en la propia percepción del mundo de la seguridad de las redes se constituyó la primera organización destinada íntegramente a la ciberseguridad, la Computer Emergency Response Team Coordinator Center (CERT/CC). («CERT Coordination Center» 2024)

2.1.3. La comercialización de Internet: el nacimiento de WWW

No sería hasta el año 1991 con el impulso dado por el nacimiento del primer navegador web gráfico, llamado WorldWideWeb que nacería el Internet tal y como lo conocemos hoy en día.

Este navegador supuso un hito en la comercialización de Internet y en su expansión posteriormente al público en general. Prueba de ello es que en 1993 tan solo existían 100 World Wide Web Sites y en 1997 ya eran más de 200.000.

En paralelo a este crecimiento, la comercialización de Internet también trajo consigo un aumento drástico en las amenazas de seguridad, como los virus informáticos ya mencionados en el punto anterior, pero también surgieron otros de distinta índole como el fraude en línea, los ataques de denegación de servicio (DNS) entre muchos otros.

A medida que más empresas comenzaron a depender de Internet para operaciones críticas, la necesidad de estándares de seguridad robustos se fue haciendo cada vez más evidente. (Bastero 2024)



2.1.4. La aparición de las primeras normativas: desde la BS-7799 a la ISO 27001

Ante la cada vez más creciente preocupación por la ciberseguridad, varios países y organizaciones comenzaron a desarrollar regulaciones y estándares que regulasen una serie de buenas prácticas a incorporar por las empresas para proteger su información.

A primeros de la década de los 90, el Departamento de Comercio e Industria del Reino Unido inició el desarrollo de una norma británica (en adelante BS), para proteger y regularla gestión de la seguridad en la empresa, y como respuesta a las peticiones de la industria, el gobierno y los comerciantes para crear una estructura común de seguridad de la información. La primera norma fue aprobada oficialmente en 1995, así nacería la BS 7799 y nace como un código de buenas prácticas para la gestión de seguridad de la información. («Asociación Española para la Calidad I AEC» 2024)

A partir de entonces, la norma BS7799 sufriría diversas actualizaciones. («Asociación Española para la Calidad I AEC» 2024)

- En 1998, se publica la BS 7799-2, en la que se recogen especificaciones para la gestión de la seguridad de la información y se crean los primeros requisitos certificables.
- En 1999, ante la incorporación del ecommerce a la norma BS la International Organization for Standardization (ISO) comienza a interesarse por los trabajos de la BS en materia de seguridad de la Información. Fruto de este interés, nacería la norma ISO 17799 que ya incorporan un conjunto de controles en materia de seguridad de la información.
- En el caso de España, no sería hasta el año 2002 donde surge la primera norma referente a la seguridad de la información. De la mano de la Asociación Española de la Normalización surge la norma (UNE-EN ISO/IEC 17799/1:2002). («UNE-ISO/IEC 17799:2002 Tecnología de la Información. Código de...» 2024)
- Finalmente, en el año 2005 nacería la norma ISO 27001:2005 que sustituirá a la BS-7799 y la ISO 27002 que a su vez sustituirá a la norma ISO 17799. («Asociación Española para la Calidad I AEC» 2024)



2.2. Evolución de la norma ISO 27001

En el anterior subapartado se explicó detalladamente la evolución histórica de los comienzos de la ciberseguridad hasta el surgimiento de las primeras normativas, incluyendo el surgimiento de la norma ISO 27001, que es el eje central del presente TFM.

Dado su relevancia, en el presente subapartado se realizará un análisis contextual de la evolución de la norma desde su nacimiento hasta la versión que se encuentra operativa actualmente.

2.2.1. ISO/IEC 27001:2005: La primera versión

En el 2005 surgiría primera norma ISO 27001. Se trata de la norma ISO/IEC 27001:2005, esta norma establecería un marco para la implementación de un SGSI, proporcionando para ello una metodología destinada a gestionar la seguridad de la información basada en el análisis de riesgos.

Tal y como ya se ha descrito, un SGSI (Sistema de Gestión de la Seguridad de la Información) se trata sistema se utiliza para proteger la confidencialidad, integridad y disponibilidad de la información. La norma proporciona un marco para la seguridad de la información que ayuda a las organizaciones a identificar y gestionar sus riesgos de seguridad de la información de manera efectiva. (Solutions 2023)

2.2.2. Norma UNE-ISO/IEC 27001:2007 “Sistemas de Gestión de la Seguridad de la Información (SGSI). Requisitos”

En 2007, A raíz de la regularización y consecuente expansión de la norma ISO/IEC 27001:2005, la UNE (Asociación Española de Normalización) realizó una adopción idéntica (IDT) de esta. («ISO/IEC 27001» 2024)

La principal diferencia radica en que incluye en su Anexo A una lista con los objetivos de control y controles que desarrolla la ISO 27002, que como ya hemos visto en el punto anterior incorporaba y actualizaba a su vez los controles de la norma ISO 17799. («UNE-ISO/IEC 27001:2007 Tecnología de la información. Técnicas ...» 2024)

2.2.3. Primera reforma de la ISO 27001: ISO/IEC 27001:2013

Como es sobradamente conocido, la informática y especialmente la ciberseguridad se encuentran en una constante y rápida evolución, fruto de esto surge la necesidad de actualización constante de cualquier tipo de metodología o solución de ciberseguridad. La norma ISO 27001 no es una excepción y de ahora en adelante se



comprobará como ha sufrido numerosas actualizaciones a raíz de la evolución de la informática en general. («Asociación Española para la Calidad I AEC» 2024)

En consecuencia de todo esto, en 2013, la norma ISO/IEC 27001 fue actualizada para alinearse con la estructura de alto nivel (HLS) de las normas de gestión ISO. La nueva versión, ISO/IEC 27001:2013, introdujo mejoras en la flexibilidad de la gestión de riesgos y actualizó los controles para adaptarse a las amenazas emergentes. («ISO 27001:2013 Mejora» 2024)

2.2.4. Norma UNE-ISO/IEC 27001:2017 “Sistemas de Gestión de la Seguridad de la Información (SGSI). Requisitos”.

Cuatro años después de la actualización de la norma ISO 27001 sucedida en 2013. La UNE actualizaría a su vez la norma *UNE-ISO/IEC 27001:2007 “Sistemas de Gestión de la Seguridad de la Información (SGSI). Requisitos”*. De acuerdo con las actualizaciones realizadas en la norma *ISO 27001: ISO/IEC 27001:2013*. («Norma ISO 27001» 2020)

De esta forma nacería la Norma *UNE-ISO/IEC 27001:2017 “Sistemas de Gestión de la Seguridad de la Información (SGSI). Requisitos”* La cual se trata del marco normativo en el que se fundamenta este trabajo.

En esta actualización se implementaron los siguientes cambios: («ISOWin: La nueva ISO 27001 2013» 2024)

- Menos controles: Se produce una eliminación de duplicidades eliminando consecuentemente 19 controles
- Reestructuración: Se reestructura en 14 secciones o apartados de control.
- Se crea el concepto de Información Documentada.
- Mayor libertad en la evaluación de Riesgos. Se elimina la necesidad de identificar los Activos de información, las Amenazas y sus Vulnerabilidades proporcionando una mayor libertad.

Finalmente, si bien la norma *UNE-ISO/IEC ISO 27001:2017* cuenta con una nueva actualización denominada la norma *UNE-ISO/IEC ISO 27001:2023*, se ha escogido esta versión de la norma al contar con una mayor disponibilidad y acceso a la literatura.



Otro aspecto que se ha considerado para decidirse por la versión de 2017 ha sido que los certificados emitidos conforme a la norma *ISO/IEC 27001:2013* contarán con validez hasta 31 de octubre de 2025. («ISO/IEC 27001 Nueva edición de la Norma: cambios y plazo - RINA.org» 2024)

2.2.5. Análisis de la implantación de la ISO 27001

Una vez realizado la contextualización de las principales predecesoras que han existido y generado la norma que regula como marco normativo este TFM, a continuación, en este sub-subapartado se hará un análisis de la expansión e implantación de la norma ISO 27001 hoy en día.

A modo de contextualización, dos años después del nacimiento de la norma ISO 27001 sucedía una etapa de gran desarrollo de la tecnología que contrastaba con una situación económica global comprometida, golpeada por la grave crisis del 2008. («PIB (US\$ a precios actuales) | Data» 2024)

Esta situación sin embargo no comprometió la expansión de la norma ISO 27001 a través de las principales empresas del Mundo («ISO 27001 - Certificado ISO 27001 punto por punto - Presupuesto Online» 2024). Tal y como se pueden apreciar en las dos siguientes imágenes que se facilitan a continuación:

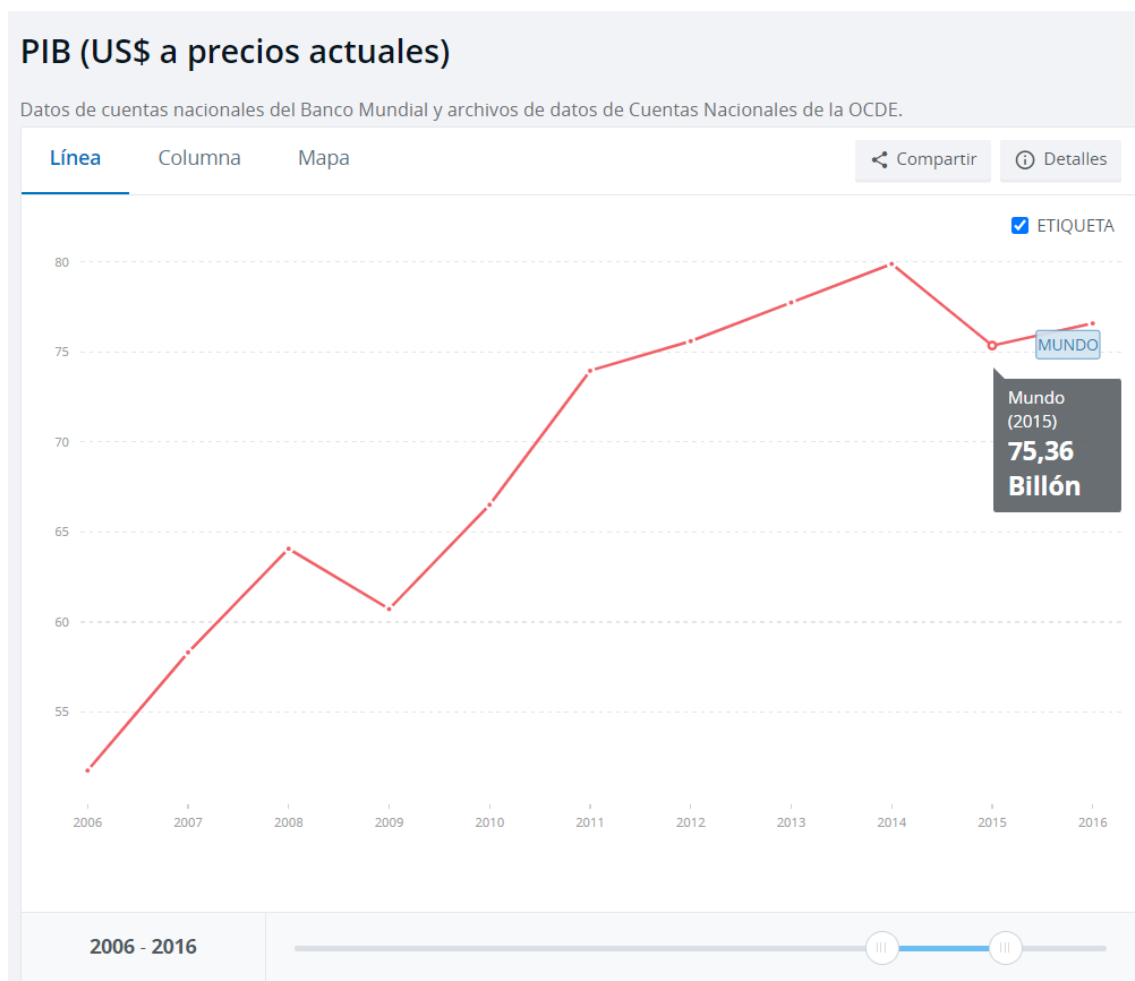


Ilustración 1. Evolución PIB mundial (2006-2022). Fuente: Bancomundial

Como se puede apreciar en esta imagen, el PIB mundial sufrió un crecimiento lineal durante los años 2006-2008, para luego sufrir una fuerte caída en 2009 y recuperar el crecimiento original en el periodo 2009-2011. A raíz de entonces, se produce una desaceleración del crecimiento del PIB hasta el final de los datos mostrados, en 2016.

Esta situación contrasta con el crecimiento del número de certificados ISO 27001 que tal y como se puede apreciar en la siguiente imagen muestra un crecimiento lineal mayor en todo momento e incluso se incrementa en una mayor medida a partir del año 2014.



Ilustración 2. Evolución Nº Certificados ISO 27001 (2006-2016). Fuente: NormalISO27001

Finalmente, para una comparación de mayor calidad y un visionado más sencillo se ha elaborado una gráfica comparativa año a año de evolución por PIB mundial (billones €) y número de certificados ISO 27001 en el mundo hasta 2022, estos datos son publicados en la ISO Survey 2022. («ISO - The ISO Survey» 2024)

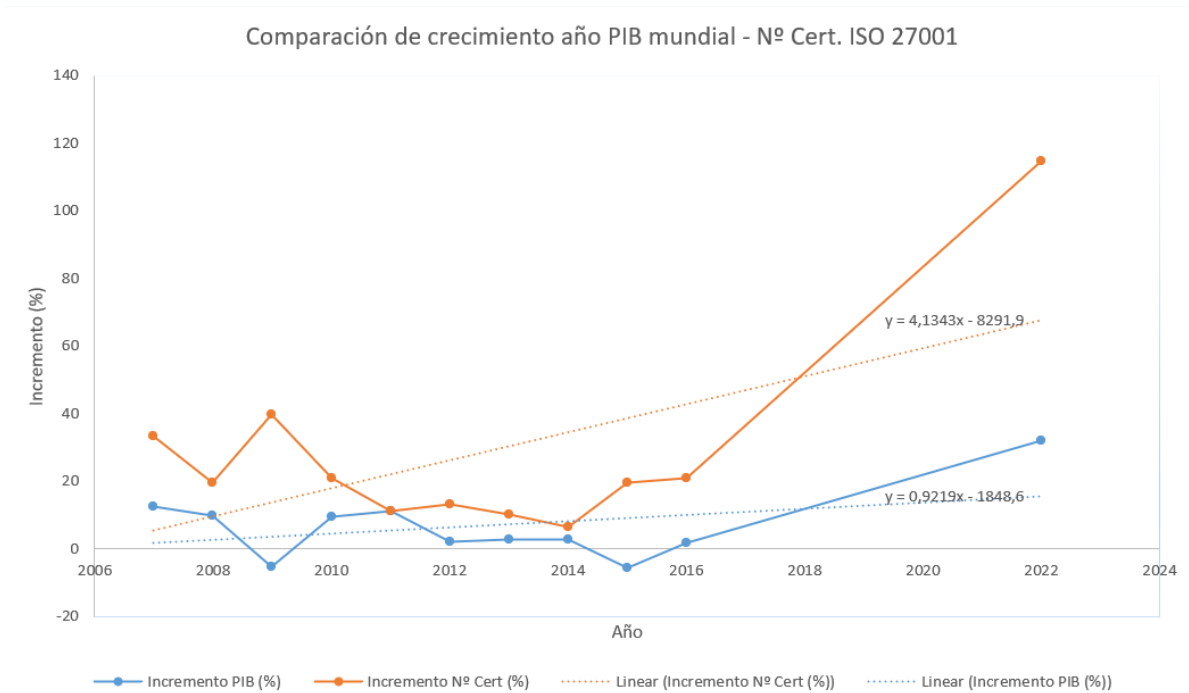


Ilustración 3. Comparativa de crecimiento PIB-NºCert. Fuente: Elaboración propia

Como se puede apreciar en la imagen anterior, el crecimiento del número de certificaciones en el periodo 2006-2022 es más de 4 veces superior al crecimiento del PIB mundial, dándonos un reflejo de la gran importancia e implantación que ostenta la ISO 27001.



2.3. Otras normativas: ENS

En paralelo a las actualizaciones sufridas por la norma ISO 27001 desde comienzos de la década del 2010, surgieron otra serie de estándares y normativas que ya sea de una forma directa o indirecta también recogieron recomendaciones y normas en materia de Ciberseguridad. En este apartado se profundizará en ellos y en sus posibles relaciones con la versión de la norma ISO 27001 escogida para la realización del presente TFM.

2.3.1. ENS: Esquema Nacional de Seguridad

El Esquema Nacional de Seguridad (ENS), se trata de un estándar normativo desarrollado y promovido por el Centro Criptológico Nacional (CCN), el cual tiene como principal objetivo garantizar la protección de la privacidad de los datos de los ciudadanos durante la realización de trámites electrónicos. Para ello, establece una serie de medidas destinadas a asegurar la protección de los sistemas, los datos, las comunicaciones y los servicios electrónicos, permitiendo a los ciudadanos ejercer sus derechos y cumplir con sus deberes a través de estos medios.

Se trata de una normativa que cuenta con una gran importancia en nuestro país, prueba de ello es que actualmente es de obligado cumplimiento para las Administraciones Públicas (AAPP) y los proveedores de servicios tecnológicos que trabajan con ellas.

Este esquema se inspira en la familia de normas ISO 27000, especialmente en la ISO 27001. Por tanto, su estructura y aplicación siguen el modelo de mejora continua PDCA (Planificar-Hacer-Comprobar-Actuar), que incluye el análisis de riesgos y la implementación de controles y medidas de seguridad. Fruto de este parecido, surge el objetivo adicional que constituye este trabajo, el cual ya ha sido detallado en el apartado anterior. («Esquema Nacional de Seguridad (ENS) Certificación - AENOR» 2024)

Uno de los principales puntos de diferencia entre el ENS y la ISO 27001 es la categorización de los sistemas de información en función de su importancia y las consecuencias que tendría la existencia de fallos en ellos. Existen 3 niveles: alto, medio y bajo. (sociall 2022)

Adicionalmente, en la siguiente imagen se muestran los principios básicos requisitos mínimos y medidas de seguridad del Esquema Nacional de Seguridad. («ISO/IEC 27001 y ENS, binomio perfecto para la ciberseguridad | N° 348» 2024)






Principios Básicos (6)	<p>Se tiene en cuenta para las decisiones en materia de seguridad</p> <ul style="list-style-type: none"> • Seguridad integral • Gestión basada en riesgos • Prevención, reacción y recuperación • Líneas de defensa • Evaluación periódica • Función diferenciada 	
Requisitos mínimos (15)	<p>Permitirán una protección adecuada de la información</p>	
Medidas de seguridad (75)	<p>Se tendrán que cumplir dentro de los principios básicos y requisitos mínimos establecidos y serán proporcionales a:</p> <ol style="list-style-type: none"> I) El tipo y nivel de la información gestionada II) Las dimensiones de seguridad relevantes en el sistema que hay que proteger III) La categoría del sistema de información que hay que proteger 	

Ilustración 4. ENS. Fuente: Aenor

3. Solución Propuesta

En el presente apartado se ahondará en la solución propuesta para la realización del presente TFM. Como ya se ha descrito en otros apartados, la finalidad de este trabajo es la realización de un cuestionario automático de autoevaluación de la norma ISO 27001 tanto para empresas públicas como privadas.

Dado que cada empresa muestra unas particularidades de acuerdo con múltiples factores según su tamaño, campo de aplicación, modelo de negocio..., este TFM será planteando desde un punto de vista general, centrándose en dar apoyo a las fases 5 y 6 de una auditoría certificadora de ISO 27001. («Norma ISO 27001» 2020)

Para ello se ha creado la herramienta "Cuestionario automático de autoevaluación de la norma ISO 270001.xlsm" tiene como principal finalidad facilitar a empresas públicas o privadas una herramienta de autoevaluación automática del estado de implementación de la norma ISO 27001. De esta forma, de una manera rápida sencilla y eficaz la empresa objeto podrá conocer cuáles son los puntos necesarios de mejora para obtener la certificación pertinente, lo que consecuentemente hará más eficientes las conversaciones con la empresa certificadora, al poseer la empresa objeto de la auditoría, un mayor grado de conocimiento de su estado de implementación.

La presente herramienta, se ha fundamentado en el sólido marco normativo proporcionado por la norma UNE-ISO/IEC 27001:2017 "Sistemas de Gestión de la Seguridad de la Información (SGSI). Requisitos". Que se trata de la versión normalizada por la Asociación Española de Normalización (UNE) de la norma ISO 27001:2013 tal y como ya se ha explicado en otros apartados de la presente norma.

Es la norma principal de requisitos de un Sistema de Gestión de Seguridad de la Información, adicionalmente, en su Anexo A, contempla una lista con los objetivos de control y controles que desarrolla la ISO 27002, que son el principal objeto de estudio de esta herramienta de autoevaluación y el eje sobre el que se estructura la herramienta, tal y como se describirá en el siguiente subapartado



3.1. Estructura de la herramienta

En el presente subapartado se explicará detalladamente la estructura de la solución propuesta. A continuación se detallarán el contenido de cada hoja.

3.1.1. Introducción

En esta hoja se realiza una breve introducción del marco normativo sobre el que se constituye la herramienta y se realiza una descripción del por qué es necesaria esta herramienta así como también describe la estructura de esta.

Normativa

Para la realización de la presente herramienta, se ha fundamentado en el sólido marco normativo proporcionado por la norma UNE-ISO/IEC 27001:2017 "Sistemas de Gestión de la Seguridad de la Información (SGSI). Requisitos". Que se trata de la versión normalizada por la Asociación Española de Normalización (UNE). Es la norma principal de requisitos de un Sistema de Gestión de Seguridad de la Información, adicionalmente, en su Anexo A, contempla una lista con los objetivos de control y controles que desarrolla la ISO 27002, que son el principal objeto de estudio de esta herramienta de autoevaluación.

[Norma UNE-ISO/IEC 27001:2017 "Sistemas de Gestión de la Seguridad de la Información \(SGSI\).](#)

Estructura de la herramienta

En el presente apartado se detallará la estructura de la herramienta automática, para ello, el principal eje sobre el que se ha estructurado han sido los objetivos de control recopilados en el anexo A de la norma UNE-ISO/IEC 27001:2017 "Sistemas de Gestión de la Seguridad de la Información (SGSI). Requisitos".

A continuación, se detallarán todos los apartados de la herramienta:

Instrucciones

En este apartado se explica:

- El funcionamiento de la herramienta
- El procedimiento de autoevaluación
- La generación del archivo ".pdf" con los resultados obtenidos

Información General

Recopilación de la siguiente información:

- Fecha y datos principales de la auditoría



Ilustración 5. Hoja "Introducción". Fuente: Elaboración propia

3.1.2. Instrucciones

En esta hoja se detallan las instrucciones para una rápida comprensión del funcionamiento del cuestionario automático de autoevaluación ISO 27001.

Adicionalmente, se explica cómo proceder si se desea descargar un PDF con los resultados obtenidos.

Instrucciones

En el presente apartado se detallan las instrucciones para una rápida comprensión del funcionamiento del cuestionario automático de autoevaluación ISO 27001. Adicionalmente, se explica cómo proceder si se desea descargar un PDF con los resultados obtenidos.

Procedimiento

En primer lugar la persona responsable debe de rellenar la información competente a la empresa y a quién está realizando la auditoría.

Información general de la auditoría	
Fecha de la auditoría	01/01/2024

Información general de la empresa	
Nombre de la empresa	
CIF	
Dirección	

Información general del responsable de auditoría	
Nombre completo	
DNI	
Cargo	

Para ello debe de acceder al apartado "información General" al cuál se puede acceder a través del siguiente botón:

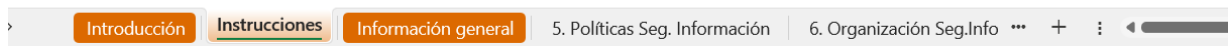


Ilustración 6. Hoja "Instrucciones". Fuente: Elaboración propia

3.1.3. Información General

En esta hoja se recopila la siguiente información clave para el informe de auditoría:

- Fecha y datos principales de la auditoría
- Datos de la empresa auditada
- Datos del responsable de la auditoría (nombre, cargo en la empresa...)



Información general

Información general de la auditoría

Fecha de la auditoría	01/01/2024
-----------------------	------------

Información general de la empresa

Nombre de la empresa	
CIF	
Dirección	

Información general del responsable de auditoría

Nombre completo	
DNI	
Cargo	

Comenzar formulario

Introducción
Instrucciones
Información general
5. Políticas Seg. Información
6. Organización Seg.Info
... + : ◀

Ilustración 7. Hoja "Información General". Fuente: Elaboración propia

3.1.4. Formulario

A continuación se encuentran las hojas correspondientes al formulario que usará la herramienta para producir los resultados de la autoevaluación. Se trata de las hojas comprendidas entre “5. Políticas Seg. Información” y “18. Cumplimiento”. Cada una de estas hojas se corresponde con uno de los dominios o categorías y se estructuran en base a los objetivos de control y los controles que componen cada apartado. Se describen en mayor profundidad a continuación:

3.1.4.1. Formulario: “5. Políticas Seg. Información”

Esta hoja se estructura en base al dominio “5. Políticas de Seguridad de la información” y busca completar el siguiente objetivo de control:

- Proporcionar orientación y apoyo a la gestión de la seguridad de la información de acuerdo con los requisitos del negocio, las leyes y normativa pertinentes.



5. Políticas de seguridad de la información

5.1. Directrices de gestión de la seguridad de la información			
ID Control	Objetivo del control	Control	SI - NO - N/A
A.5.1.1	Políticas de la seguridad de la información	Existe un conjunto de políticas para la seguridad de la información definido, aprobado por la dirección, publicado y comunicado a los empleados y partes externas relevantes.	
A.5.1.2	Revisión de las políticas de la seguridad de la información	Se realizan revisiones periódicas de las políticas de seguridad de la información o siempre que se realicen cambios significativos.	

Siguiente

Ilustración 8. Hoja "5. Políticas de seguridad de la información". Fuente: Elaboración propia

3.1.4.2. Formulario: "6. Organización Seg. Info"

Esta se hoja estructura en base al dominio "Organización de la seguridad de la información" y busca cubrir los siguientes objetivos de control:

- Establecer un marco de gestión para iniciar y controlar la implementación y operación de la seguridad de la información dentro de la organización.
- Garantizar la seguridad en el teletrabajo y en el uso de dispositivos móviles

6. Organización de la seguridad de la información

6.1. Organización interna			
ID Control	Objetivo del control	Control	SI - NO - N/A
A.6.1.1	Roles y responsabilidades en seguridad de la información	Todas las responsabilidades en seguridad de la información se encuentran correctamente definidas y asignadas.	NO
A.6.1.2	Segregación de tareas	Las funciones y áreas de responsabilidad se encuentran definidas siguiendo una adecuada segregación de funciones a fin de imposibilitar modificaciones no autorizadas o no intencionadas así como usos indebidos de los activos de la organización.	NO
A.6.1.3	Contacto con las autoridades	Se mantienen contactos apropiados con las autoridades pertinentes.	NO
A.6.1.4	Contacto con grupos de interés especial	Se mantienen contactos apropiados con grupos de interés especial, u otros foros y asociaciones profesionales especializados en seguridad.	NO
A.6.1.5	Seguridad de la información en la gestión de proyectos	La seguridad de la información se trata dentro de la gestión de proyectos, independientemente de la naturaleza del proyecto.	NO

6.2. Los dispositivos móviles y teletrabajo			
ID Control	Objetivo del control	Control	SI - NO - N/A
A.6.2.1	Política de dispositivos móviles	Existen una política y unas medidas de seguridad adecuadas para la protección contra los riesgos de la utilización de dispositivos móviles.	N/A
A.6.2.2	Teletrabajo	Existen una política y unas medidas de seguridad adecuadas para proteger la información accedida, tratada o almacenada en emplazamientos de teletrabajo.	N/A

Anterior

Siguiente

Ilustración 9. Hoja "Organización Seg. Información". Fuente: Elaboración propia

3.1.4.3. Formulario: “7. Seguridad relativa a los recursos humanos”

Esta se hoja estructura en base al dominio “7. Seguridad relativa a los recursos humanos” y se estructura en base a los siguientes objetivos de control:

- Asegurar que los empleados y contratistas entiendan sus responsabilidades y son adecuados para las funciones para las que se consideran.

- Asegurar que los empleados y contratistas conozcan y cumplan con sus responsabilidades en seguridad de la información.

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

7. Seguridad relativa a los recursos humanos

7.1. Antes del empleo			
ID Control	Objetivo del control	Control	SI - NO - NA
A.7.1.1	Investigación de antecedentes	Se realiza una comprobación de los antecedentes de todos los candidatos al puesto de trabajo de acuerdo con las leyes, normativa y códigos éticos que sean de aplicación siendo dicha comprobación proporcional a las necesidades del negocio, la clasificación de la información a la que se accede y los riesgos percibidos	SI
A.7.1.2	Términos y condiciones del empleo	En base a las obligaciones contractuales, los empleados y contratistas establecen los términos y condiciones en su contrato de trabajo en lo que respecta a la seguridad de la información, tanto hacia el empleado como hacia la organización.	SI

7.2. Durante el empleo			
ID Control	Objetivo del control	Control	SI - NO - NA
A.7.2.1	Responsabilidades de gestión	La dirección exige a los empleados y contratistas, que apliquen la seguridad de la información de acuerdo con las políticas y procedimientos establecidos en la organización.	NO
A.7.2.2	Concienciación, educación y capacitación en seguridad de	Todos los empleados de la organización y, cuando corresponda, los contratistas, reciben una adecuada educación, concienciación y capacitación con actualizaciones periódicas sobre las políticas.	NO
A.7.2.3	Proceso disciplinario	Existe un proceso disciplinario formal que haya sido comunicado a los empleados, que recoja las acciones a tomar ante aquellos que hayan provocado alguna brecha de seguridad.	NO

7.3. Finalización del empleo o cambio en el puesto de trabajo			
ID Control	Objetivo del control	Control	SI - NO - NA
A.7.3.1	Responsabilidades ante la finalización o cambio	Las responsabilidades en seguridad de la información y obligaciones que siguen vigentes después del cambio o finalización del empleo se encuentran correctamente definidas y comunicadas al empleado o contratista y son de obligado cumplimiento.	NA

Anterior

Siguiente

Ilustración 10. Hoja “7. Seguridad relativa a los recursos humanos”. Fuente: Elaboración propia

3.1.4.4. Formulario: "8. Gestión de activos"

Esta hoja se estructura en base al dominio "8. Gestión de activos" y se estructura en base a los siguientes objetivos de control:

- Identificar los activos de la organización y definir las responsabilidades de protección adecuadas.
- Asegurar que la información reciba un nivel adecuado de protección de acuerdo con su importancia para la organización.
- Evitar la revelación, modificación, eliminación o destrucción no autorizadas de la información almacenada en soportes.

8. Gestión de activos

8.1. Responsabilidad sobre los activos			
ID Control	Objetivo del control	Control	SI - NO - N/A
A.8.1.1	Inventario de activos	La información y otros activos asociados a la información y a los recursos para el tratamiento de la información se encuentran claramente identificados y se mantiene un inventario de estos.	SI
A.8.1.2	Propiedad de los activos	Todos los activos que figuran en el inventario tienen un propietario	SI
A.8.1.3	Uso aceptable de los activos	Se han identificado, documentado e implementado las reglas de uso aceptable de la información y de los activos asociados con los recursos para el tratamiento de la información.	SI
A.8.1.4	Devolución de activos	Todos los empleados y terceras partes devuelven todos los activos de la organización que estén en su poder al finalizar su empleo, contrato o acuerdo.	SI

8.2. Clasificación de la información			
ID Control	Objetivo del control	Control	SI - NO - N/A
A.8.2.1	Clasificación de la información	La información se encuentra clasificada en términos de la importancia de su revelación frente a requisitos legales, valor, sensibilidad y criticidad ante revelación o modificación no autorizadas	NO
A.8.2.2	Etiquetado de la información	Se ha desarrollado e implementado un conjunto adecuado de procedimientos para etiquetar la información, de acuerdo con el esquema de clasificación adoptado por la organización.	NO
A.8.2.3	Manipulado de la información	Se ha desarrollado e implementado un conjunto adecuado de procedimientos para la manipulación de la información, de acuerdo con el esquema de clasificación adoptado por la organización.	NO

8.3. Manipulación de los soportes			
ID Control	Objetivo del control	Control	SI - NO - N/A
A.8.3.1	Gestión de soportes extraíbles	Se encuentran implementados procedimientos para la gestión de los soportes extraíbles, de acuerdo con el esquema de clasificación adoptado por la organización.	N/A
A.8.3.2	Eliminación de soportes	Los soportes se han eliminados de forma segura cuando ya no vayan a ser necesarios, mediante procedimientos formales.	N/A
A.8.3.3	Soportes físicos en tránsito	Durante el transporte fuera de los límites físicos de la organización, los soportes que contengan información se encuentran protegidos contra accesos no autorizados, usos indebidos o deterioro.	N/A

Anterior

Siguiente

Ilustración 11. Hoja "8. Gestión de activos". Fuente: Elaboración propia



3.1.4.5. Formulario: "9. Control de acceso"

Esta hoja se estructura en base al dominio "9. Control de acceso" y se estructura en base a los siguientes objetivos de control:

- Limitar el acceso a los recursos de tratamiento de la información y a la información.
- Garantizar el acceso de usuarios autorizados y evitar el acceso no autorizado a los sistemas y servicios.
- Para que los usuarios se hagan responsables de salvaguardar su información de autenticación.
- Prevenir el acceso no autorizado a los sistemas y aplicaciones.

9. Control de acceso

9.1. Requisitos de negocio para el control de acceso			
ID Control	Objetivo del control	Control	SI - NO - N/A
A.9.1.1	Política de control de acceso	Se ha establecido, documentado y revisado una política de control de acceso basada en los requisitos de negocio y de seguridad de la información.	
A.9.1.2	Acceso a las redes y a los servicios de red	Únicamente se proporciona a los usuarios el acceso a las redes y a los servicios en red para cuyo uso hayan sido específicamente autorizados.	

9.2. Gestión de acceso de usuario			
ID Control	Objetivo del control	Control	SI - NO - N/A
A.9.2.1	Registro y baja de usuario	Se encuentra implantado un procedimiento formal de registro y retirada de usuarios que haga posible la asignación de los derechos de acceso.	
A.9.2.2	Provisión de acceso de usuario	Se encuentra implantado un procedimiento formal para asignar o revocar los derechos de acceso para todos los tipos de usuarios de todos los sistemas y servicios.	
A.9.2.3	Gestión de privilegios de acceso	La asignación y el uso de privilegios de acceso se encuentra restringida y controlada	
A.9.2.4	Gestión de la información secreta de autenticación de los usuarios	La asignación de la información secreta de autenticación se encuentra controlada a través de un proceso formal de gestión.	
A.9.2.5	Revisión de los derechos de acceso de usuario	Los propietarios de los activos revisan los derechos de acceso de usuario a intervalos regulares.	
A.9.2.6	Retirada o reasignación de los derechos de acceso	Los derechos de acceso de todos los empleados y terceras partes, a la información y a los recursos de tratamiento de la información son retirados a la finalización del empleo, del contrato o del acuerdo, o ajustados en caso de cambio.	

Ilustración 12. Hoja "9. Control de acceso". Fuente: Elaboración propia

9.3. Responsabilidades del usuario			
ID Control	Objetivo del control	Control	SI - NO - N/A
A.9.3.1	Uso de la información secreta de autenticación	Se requiere a los usuarios que sigan las prácticas de la organización en el uso de la información secreta de autenticación.	

9.4. control de acceso a sistemas y aplicaciones			
ID Control	Objetivo del control	Control	SI - NO - N/A
A.9.4.1	Restricción del acceso a la información	Se restringe el acceso a la información y a las funciones de las aplicaciones, de acuerdo con la política de control de acceso definida.	
A.9.4.2	Procedimientos seguros de inicio de sesión	Cuando así se requiera en la política de control de acceso, el acceso a los sistemas y a las aplicaciones se controla por medio de un procedimiento seguro de inicio de sesión.	
A.9.4.3	Sistema de gestión de contraseñas	Los sistemas para la gestión de contraseñas son interactivos y establecer contraseñas seguras y robustas.	
A.9.4.4	Uso de utilidades con privilegios del sistema	Se restringen y controlan rigurosamente el uso de utilidades que puedan ser capaces de invalidar los controles del sistema y de la aplicación.	
A.9.4.5	Control de acceso al código fuente de los programas	Se restringe el acceso al código fuente de los programas	

Anterior

Siguiente

Ilustración 13. Hoja "9. Control de acceso". Fuente: Elaboración propia

3.1.4.6. Formulario: "10. Criptografía"

Esta hoja se estructura en base al dominio "10. Criptografía" y busca completar el siguiente objetivo de control:

- Garantizar un uso adecuado y eficaz de la criptografía para proteger la confidencialidad, autenticidad y/o integridad de la información.

10. Criptografía

10.1. Controles criptográficos			
ID Control	Objetivo del control	Control	SI - NO - N/A
A.10.1.1	Política de uso de los controles criptográficos	Se ha desarrollado e implementado una política sobre el uso de los controles criptográficos para proteger la información.	
A.10.1.2	Gestión de claves	Se ha desarrollado una política sobre el uso, la protección y la duración de las claves de cifrado a lo largo de todo su ciclo de vida.	

Anterior

Siguiente

Ilustración 14. Hoja "10. Criptografía". Fuente: Elaboración propia

3.1.4.7. Formulario: "11. Seguridad física y del entorno"

Esta hoja se estructura en base al dominio "11. Seguridad física y del entorno" y se estructura en base a los siguientes objetivos de control:

- Prevenir el acceso físico no autorizado, los daños e interferencia a la información de la organización y a los recursos de tratamiento de la información.
- Evitar la pérdida, daño, robo o el compromiso de los activos y la interrupción de las operaciones de la organización.

11. Seguridad física y del entorno

11.1. Áreas seguras			
ID Control	Objetivo del control	Control	SI - NO - N/A
A.11.1.1	Perímetro de seguridad física	Se utilizan perímetros de seguridad para proteger las áreas que contienen información sensible así como los recursos de tratamiento de la información.	SI
A.11.1.2	Controles físicos de entrada	Las áreas seguras se encuentran protegidas mediante controles de entrada adecuados, para asegurar que únicamente se permite el acceso al personal autorizado.	SI
A.11.1.3	Seguridad de oficinas, despachos y recursos	Para las oficinas, despachos y recursos, se ha diseñado y aplicado la seguridad física.	SI
A.11.1.4	Protección contra las amenazas externas y sabotajes	Se debe diseñar y aplicar una protección física contra desastres naturales, ataques provocados por el hombre o accidentes.	SI
A.11.1.5	El trabajo en áreas seguras	Se han diseñado e implementado procedimientos para trabajar en las áreas seguras.	SI
A.11.1.6	Áreas de carga y descarga	Se han controlado los puntos de acceso tales como las áreas de carga y descarga y otros puntos, donde pueda acceder personal no autorizado a las instalaciones, e idóneamente y según la disponibilidad, se han aislado dichos puntos de los recursos de tratamiento de la información para evitar accesos no autorizados.	SI

11.2. Seguridad de los equipos			
ID Control	Objetivo del control	Control	SI - NO - N/A
A.11.2.1	Emplazamiento y protección de equipos	Los equipos se han situado o protegido de forma que se reduzcan los riesgos de las amenazas y los riesgos ambientales así como las oportunidades de que se produzcan accesos no autorizados.	NO
A.11.2.2	Instalaciones de suministro	Los equipos se encuentran protegidos contra fallos de alimentación y otras alteraciones causadas por fallos en las instalaciones de suministro.	NO
A.11.2.3	Seguridad del cableado	El cableado eléctrico y de telecomunicaciones que transmite datos o que sirve de soporte a los servicios de información se encuentra protegido frente a interceptaciones, interferencias o daños.	NO
A.11.2.4	Mantenimiento de los equipos	Los equipos reciben un mantenimiento correcto que asegure su disponibilidad y su integridad continuas.	NO
A.11.2.5	Retirada de materiales propiedad de la empresa	Sin autorización previa, los equipos, la información o el software no se sacan de las instalaciones.	NO
A.11.2.6	Seguridad de los equipos fuera de las instalaciones	Se aplican medidas de seguridad a los equipos situados fuera las instalaciones de la organización, teniendo en cuenta los diferentes riesgos que conlleva trabajar fuera de dichas instalaciones.	NO
A.11.2.7	Reutilización o eliminación segura de equipos	Todos los soportes de almacenamiento deben ser comprobados para confirmar que todo dato sensible y software bajo licencia se ha eliminado de manera segura, antes de deshacerse de ellos.	NO
A.11.2.8	Equipo de usuario desatendido	Los usuarios se aseguran de que el equipo desatendido tiene la protección adecuada.	NO
A.11.2.9	Política de puesto de trabajo despejado y pantalla limpia	Se ha adoptado una política de puesto de trabajo despejado de papeles y medios de almacenamiento desmontables y una política de pantalla limpia para los recursos de tratamiento de la información.	NO

Anterior

Siguiente

Ilustración 15. Hoja 11 "Seguridad física y entorno". Fuente: Elaboración propia



3.1.4.8. Formulario: "12. Seguridad de las operaciones"

Esta hoja se estructura en base al dominio "12. Seguridad de las operaciones" y se estructura en base a los siguientes objetivos de control:

- Asegurar el funcionamiento correcto y seguro de las instalaciones de tratamiento de la información.
- Asegurar que los recursos de tratamiento de información y la información están protegidos contra el malware.
- Evitar la pérdida de datos
- Registrar eventos y generar evidencias.
- Asegurar la integridad del software en explotación.
- Reducir los riesgos resultantes de la explotación de las vulnerabilidades técnicas.
- Minimizar el impacto de las actividades de auditoría en los sistemas operativos.

12. Seguridad de las operaciones			
12.1. Procedimientos y responsabilidades operacionales			
ID Control	Objetivo del control	Control	SI - NO - N/A
A.12.1.1	Documentación de procedimientos operacionales	Se documentan y mantienen procedimientos operacionales y ponerse a disposición de todos los usuarios que los necesiten.	SI
A.12.1.2	Gestión de cambios	Los cambios en la organización, los procesos de negocio, instalaciones de tratamiento de la información y los sistemas que afectan a la seguridad de la información son controlados.	SI
A.12.1.3	Gestión de capacidades	Se debe supervisar y ajustar la utilización de los recursos, así como realizar proyecciones de los requisitos futuros de capacidad, para garantizar el rendimiento	SI
A.12.1.4	Separación de los recursos de desarrollo, prueba y producción	Se separan los recursos de desarrollo, pruebas y operación, para reducir los riesgos de acceso no autorizado o los cambios del sistema en producción.	SI
12.2. Protección contra el software malicioso (malware)			
ID Control	Objetivo del control	Control	SI - NO - N/A
A.12.2.1	Controles contra el código malicioso	Se han implementado los controles de detección, prevención y recuperación que sirvan como protección contra el código malicioso, así como procedimientos adecuados de concienciación al usuario.	NO
12.3. Responsabilidades del usuario			
ID Control	Objetivo del control	Control	SI - NO - N/A
A.12.3.1	Copias de seguridad de la información	Se han realizado copias de seguridad de la información, del software y del sistema y se deben verificar periódicamente de acuerdo a la política de copias de seguridad acordada.	NA

Ilustración 16. Hoja "12. Seguridad de las operaciones". Fuente: Elaboración propia

12.4. Registros y supervisión			
ID Control	Objetivo del control	Control	SI - NO - N/A
A.12.4.1	Registro de eventos	Se han registrado, protegido y revisado periódicamente las actividades de los usuarios, excepciones, fallos y eventos de seguridad de la información.	SI
A.12.4.2	Protección de la información del registro	Los dispositivos de registro y la información del registro se encuentran protegidos contra manipulaciones indebidas y accesos no autorizados.	SI
A.12.4.3	Registros de administración y operación	Se han registrado, protegido y revisado regularmente las actividades del administrador del sistema y del operador del sistema.	SI
A.12.4.4	Sincronización del reloj	Los relojes de todos los sistemas de tratamiento de la información dentro de una organización o de un dominio de seguridad, se encuentran sincronizados con una única fuente de tiempo precisa y acordada.	SI

12.5. Control del software en explotación			
ID Control	Objetivo del control	Control	SI - NO - N/A
A.12.5.1	Instalación del software en explotación	Se han implementado procedimientos para controlar la instalación del software en explotación.	NO

12.6. Gestión de la vulnerabilidad técnica			
ID Control	Objetivo del control	Control	SI - NO - N/A
A.12.6.1	Gestión de las vulnerabilidades técnicas	Se han obtenido información oportuna acerca de las vulnerabilidades técnicas de los sistemas de información utilizados, así como evaluado la exposición de la organización a dichas vulnerabilidades y adoptado las medidas adecuadas para afrontar el riesgo asociado.	N/A
A.12.6.2	Restricción en la instalación de software	Se han establecido y aplicado reglas que rijan la instalación de software por parte de los usuarios.	N/A

12.7. Consideraciones sobre la auditoría de sistemas de información			
ID Control	Objetivo del control	Control	SI - NO - N/A
A.12.7.1	Controles de auditoría de sistemas de información	Los requisitos y las actividades de auditoría que impliquen comprobaciones en los sistemas operativos se encuentran cuidadosamente planificados y acordados para minimizar el riesgo de interrupciones en los procesos de negocio.	SI

Anterior

Siguiente

Ilustración 17. Hoja "12. Seguridad de las operaciones". Fuente: Elaboración propia

3.1.4.9. Formulario: "13. Seguridad de las comunicaciones"

Esta hoja se estructura en base al dominio "13. Seguridad de las comunicaciones" y se estructura en base a los siguientes objetivos de control:

- Asegurar la protección de la información en las redes y los recursos de tratamiento de la información.

- Mantener la seguridad de la información que se transfiere dentro de una organización y con cualquier entidad externa.

13. Seguridad de las comunicaciones

13.1. Gestión de la seguridad de las redes			
ID Control	Objetivo del control	Control	SI - NO - N/A
A.13.1.1	Controles de red	Las redes son gestionadas y controladas para proteger la información en los sistemas y aplicaciones.	
A.13.1.2	Seguridad de los servicios de red	Se identifican los mecanismos de seguridad, los niveles de servicio, y los requisitos de gestión de todos los servicios de red y se incluyen en cualquier acuerdo de servicios de red, tanto si estos servicios se prestan dentro de la organización como si se subcontratan	
A.13.1.3	Segregación en redes	Los grupos de servicios de información, los usuarios y los sistemas de información se encuentran segregados en redes distintas.	

13.2. Intercambio de información			
ID Control	Objetivo del control	Control	SI - NO - N/A
A.13.2.1	Políticas y procedimientos de intercambio de información	Se han establecido políticas, procedimientos y controles formales que protejan el intercambio de información mediante el uso de todo tipo de recursos de comunicación.	
A.13.2.2	Acuerdos de intercambio de información	Se han establecido acuerdos para el intercambio seguro de información del negocio y software entre la organización y terceros.	
A.13.2.3	Mensajería electrónica	La información que sea objeto de mensajería electrónica está adecuadamente protegida.	
A.13.2.4	Acuerdos de confidencialidad o no revelación	Se han identificado, documentado y revisado regularmente los requisitos de los acuerdos de confidencialidad o no revelación.	

Anterior

Siguiente

Ilustración 18. Hoja "13. Seguridad de las comunicaciones". Fuente: Elaboración propia



3.1.4.10. Formulario: “14. Adquisición, desarrollo y mantenimiento de los sistemas de información”

Esta hoja se estructura en base al dominio “14. Adquisición, desarrollo y mantenimiento de los sistemas de información” y se estructura en base a los siguientes objetivos de control:

- Garantizar que la seguridad de la información sea parte integral de los sistemas de información a través de todo el ciclo de vida. Esto también incluye los requisitos para los sistemas de información que proporcionan los servicios a través de redes públicas.
- Garantizar la seguridad de la información que se ha diseñado e implementado en el ciclo de vida de desarrollo de los sistemas de información.
- Asegurar la protección de los datos de prueba.

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

14.1. Requisitos de seguridad en los sistemas de información			
ID Control	Objetivo del control	Control	SI - NO - N/A
A.14.1.1	Análisis de requisitos y especificaciones de seguridad de la información	Los requisitos relacionados con la seguridad de la información se incluyen en los requisitos para los nuevos sistemas de información o mejoras a los sistemas de información existentes.	
A.14.1.2	Asegurar los servicios de aplicaciones en redes públicas	La información involucrada en aplicaciones que pasan a través de redes públicas se encuentra protegida de cualquier actividad fraudulenta, disputa de contrato, revelación y modificación no autorizadas.	
A.14.1.3	Protección de las transacciones de servicios de aplicaciones	La información involucrada en las transacciones de servicios de aplicaciones se encuentra protegida para prevenir la transmisión incompleta, errores de enrutamiento, alteración no autorizada del mensaje, revelación, duplicación, o reproducción de mensajes no autorizadas.	

14.2. Seguridad en el desarrollo y en los procesos de soporte			
ID Control	Objetivo del control	Control	SI - NO - N/A
A.14.2.1	Política de desarrollo seguro	Se establecen y aplican reglas dentro de la organización para el desarrollo de aplicaciones y sistemas.	
A.14.2.2	Procedimiento de control de cambios en sistemas	La implantación de cambios a lo largo del ciclo de vida del desarrollo se ha controlado mediante el uso de procedimientos formales de control de cambios.	
A.14.2.3	Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo	Cuando se modifiquen los sistemas operativos, las aplicaciones de negocio críticas son revisadas y probadas para garantizar que no existen efectos adversos en las operaciones o la seguridad de la organización.	
A.14.2.4	Restricciones a los cambios en los paquetes de software	Se desaconsejan las modificaciones en los paquetes de software, limitándose a los cambios necesarios, y todos los cambios deben ser objeto de un control riguroso.	
A.14.2.5	Principios de ingeniería de sistemas seguros	Principios de ingeniería de sistemas seguros se han establecido, documentado, mantenido y aplicado a todos los esfuerzos de implementación de sistemas de información.	
A.14.2.6	Entorno de desarrollo seguro	Las organizaciones han establecido y protegido adecuadamente los entornos de desarrollo seguro para el desarrollo del sistema y los esfuerzos de integración que cubren todo el ciclo de vida de desarrollo del sistema.	
A.14.2.7	Externalización del desarrollo de software	Los derechos de acceso de todos los empleados y terceras partes, a la información y a los recursos de tratamiento de la información son retirados a la finalización del empleo, del contrato o del acuerdo, o ajustados en caso de cambio.	
A.14.2.8	Pruebas funcionales de seguridad de sistemas	Se llevan a cabo pruebas de la seguridad funcional durante el desarrollo.	
A.14.2.9	Pruebas de aceptación de sistemas	Se han establecido programas de pruebas de aceptación y criterios relacionados para nuevos sistemas de información, actualizaciones y nuevas versiones.	

Ilustración 19. Hoja " 14. Adquisición, desarrollo y mantenimiento de los sistemas de información". Fuente: Elaboración propia



14.3. Datos de prueba			
ID Control	Objetivo del control	Control	SI - NO - N/A
A.14.3.1	Protección de los datos de prueba	Los datos de prueba se seleccionan con cuidado y son protegidos y controlados.	

Anterior

Siguiente

Ilustración 20. Hoja " 14. Adquisición, desarrollo y mantenimiento de los sistemas de información". Fuente: Elaboración propia

3.1.4.11. Formulario: "15. Relación con proveedores"

Esta hoja se estructura en base al dominio "15. Relación con proveedores" y se estructura en base a los siguientes objetivos de control:

- Asegurar la protección de los activos de la organización que sean accesibles a los proveedores.

- Mantener un nivel acordado de seguridad y de provisión de servicios en línea con acuerdos con proveedores.

15. Relación con proveedores

15.1 Seguridad en las relaciones con proveedores			
ID Control	Objetivo del control	Control	SI - NO - N/A
A.15.1.1	Política de seguridad de la información en las relaciones con los proveedores	Los requisitos de seguridad de la información para la mitigación de los riesgos asociados con el acceso del proveedor a los activos de la organización se han acordado con el proveedor y han quedado documentados.	
A.15.1.2	Requisitos de seguridad en contratos con terceros	Todos los requisitos relacionados con la seguridad de la información se han establecido y acordado con cada proveedor que puede acceder, tratar, almacenar, comunicar, o proporcionar componentes de la infraestructura de Tecnología de la Información.	
A.15.1.3	Cadena de suministro de tecnología de la información y de las comunicaciones	Los acuerdos con proveedores incluyen requisitos para hacer frente a los riesgos de seguridad de la información relacionados con las tecnologías de la información y las comunicaciones y con la cadena de suministro de productos.	

15.2. Gestión de la provisión de servicios del proveedor			
ID Control	Objetivo del control	Control	SI - NO - N/A
A.15.2.1	Control y revisión de la provisión de servicios del proveedor	Las organizaciones controlan, revisan y auditan regularmente la provisión de servicios del proveedor	
A.15.2.2	Gestión de cambios en la provisión del servicio del proveedor	Segestionan los cambios en la provisión del servicio, incluyendo el mantenimiento y la mejora de las políticas, los procedimientos y controles de seguridad de la información existentes, teniendo en cuenta la criticidad de los procesos y sistemas de negocio afectados así como la reapreciación de los riesgos.	

Anterior

Siguiente

Ilustración 21. Hoja "15. Relación con proveedores". Fuente: Elaboración propia

3.1.4.12. Formulario: "16. Gestión de incidentes de seguridad de la información"

Esta hoja se estructura en base al dominio "16. Gestión de incidentes de seguridad de la información" y se estructura en base a siguiente objetivo de control:

- Asegurar la protección de los activos de la organización que sean accesibles a los proveedores.

16. Gestión de incidentes de seguridad de la información

16.1. Gestión de incidentes de seguridad de la información y mejoras			
ID Control	Objetivo del control	Control	SI - NO - N/A
A.16.1.1	Responsabilidades y procedimientos	Se han establecido las responsabilidades y procedimientos de gestión para garantizar una respuesta rápida, efectiva y adecuada a los incidentes de seguridad de la información.	
A.16.1.2	Notificación de los eventos de seguridad de la información	Los eventos de seguridad de la información se notifican por los canales de gestión adecuados lo antes posible.	
A.16.1.3	Notificación de puntos débiles de la seguridad	Todos los empleados, contratistas, terceras partes usuarias de los sistemas y servicios de información son obligados a anotar y notificar cualquier punto débil que observen o que sospechen que exista, en los sistemas o servicios.	
A.16.1.4	Evaluación y decisión sobre los eventos de seguridad de información	Los eventos de seguridad de la información deben ser evaluados y debe decidirse si se clasifican como incidentes de seguridad de la información.	
A.16.1.5	Respuesta a incidentes de seguridad de la información	Los incidentes de seguridad de la información son respondidos de acuerdo con los procedimientos documentados.	
A.16.1.6	Aprendizaje de los incidentes de seguridad de la información	El conocimiento obtenido a partir del análisis y la resolución de incidentes de seguridad de la información se utiliza para reducir la probabilidad o el impacto de los incidentes en el futuro.	
A.16.1.7	Recopilación de evidencias	La organización ha definido y aplicado procedimientos para la identificación recogida, adquisición y preservación de la información que puede servir de evidencia.	

Anterior

Siguiente

Ilustración 22. Hoja "16. Gestión de incidentes de seguridad de la información ". Fuente: Elaboración propia



3.1.4.13. Formulario: “17. Aspectos de seguridad de la información para la gestión de la continuidad de negocio”

Esta hoja se estructura en base al dominio “17. Aspectos de seguridad de la información para la gestión de la continuidad de negocio” y se estructura en base a los siguientes objetivos de control:

- La continuidad de la seguridad de la información debe formar parte de los sistemas de gestión de la continuidad de negocio de la organización.
- Asegurar la disponibilidad de los recursos de tratamiento de la información.

17. Aspectos de seguridad de la información para la gestión de la continuidad de negocio

17.1 Continuidad de la seguridad de la información			
ID Control	Objetivo del control	Control	SI - NO - N/A
A.17.1.1	Política de seguridad de la información en las relaciones con los proveedores	La organización ha determinado sus necesidades de seguridad de la información y de continuidad para la gestión de la seguridad de la información en situaciones adversas, por ejemplo, durante una crisis o desastre.	
A.17.1.2	Requisitos de seguridad en contratos con terceros	La organización ha establecido, documentado, implementado y mantenido procesos, procedimientos y controles para asegurar el nivel requerido de continuidad de la seguridad de la información durante una situación adversa.	
A.17.1.3	Cadena de suministro de tecnología de la información y de las comunicaciones	La organización ha comprobado los controles establecidos e implementados a intervalos regulares para asegurar que son válidos y eficaces durante situaciones adversas.	

17.2. Redundancias			
ID Control	Objetivo del control	Control	SI - NO - N/A
A.17.2.1	Disponibilidad de los recursos de tratamiento de la información	Los recursos de tratamiento de la información han sido implementados con la redundancia suficiente para satisfacer los requisitos de disponibilidad.	

Anterior

Siguiente

Ilustración 23. Hoja "17. Aspectos de seguridad de la información para la gestión de la continuidad de negocio ".
Fuente: Elaboración propia



3.1.4.14. Formulario: "18. Cumplimiento"

Esta hoja se estructura en base al dominio "18. Cumplimiento" y se estructura en base a los siguientes objetivos de control:

- Evitar incumplimientos de las obligaciones legales, estatutarias, reglamentarias o contractuales relativas a la seguridad de la información o de los requisitos de seguridad.

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

18. Cumplimiento

18.1 Cumplimiento de los requisitos legales y contractuales			
ID Control	Objetivo del control	Control	SI - NO - NA
A.18.1.1	Identificación de la legislación aplicable y de los requisitos	Todos los requisitos pertinentes, tanto legales como regulatorios, estatutarios o contractuales, y el enfoque de la organización para cumplirlos, se han definido de forma explícita, documentado y mantenido actualizados para cada sistema de información de la organización.	SI
A.18.1.2	Derechos de Propiedad Intelectual (DPI)	Se han implementado 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.	SI
A.18.1.3	Protección de los registros de la organización	Los registros se encuentran protegidos contra la pérdida, destrucción, falsificación, revelación o acceso no autorizados de acuerdo con los requisitos legales, regulatorios, contractuales y de negocio.	SI
A.18.1.4	Protección y privacidad de la información de carácter personal	Se ha garantizado la protección y la privacidad de los datos, según se requiera en la legislación y la reglamentación aplicables.	SI
A.18.1.5	Regulación de los controles criptográfico	Los controles criptográficos se utilizan de acuerdo con todos los contratos, leyes y regulaciones pertinentes.	SI

18.2. Revisión de la seguridad de la información			
ID Control	Objetivo del control	Control	SI - NO - NA
A.18.2.1	Revisión independiente de la seguridad de la información	El enfoque de la organización para la gestión de la seguridad de la información y su implantación, es decir, objetivos de control, controles, políticas, procesos y procedimientos para la seguridad de la información, es sometido a una revisión independiente a intervalos planificados o siempre que se produzcan cambios significativos en la implantación de la seguridad.	NO
A.18.2.2	Cumplimiento de las políticas y normas de seguridad	Los directivos se aseguran que todos los procedimientos de seguridad dentro de su área de responsabilidad se realizan correctamente con el fin de cumplir las políticas y normas de seguridad y cualquier otro requisito de seguridad aplicable	NO
A.18.2.3	Comprobación del cumplimiento técnico	Se comprueba periódicamente que los sistemas de información cumplen las políticas y normas de seguridad de la información de la organización	NO

Anterior

Finalizar

Ilustración 24. Hoja "18. Cumplimiento". Fuente: Elaboración propia



3.1.5. Resumen

En esta hoja se facilita el procedimiento y resumen de los resultados obtenidos en el formulario:

Resumen

5. Políticas de seguridad de la información	Nº Si	Nº No	Nº N/A	Resultado
5.1. Directrices de gestión de la seguridad de la información	1	1	0	50,00%
6. Organización de la seguridad de la información	Nº Si	Nº No	Nº N/A	Resultado
6.1. Organización interna	0	5	0	0,00%
6.2. Los dispositivos móviles y teletrabajo	0	0	2	N/A
7. Seguridad relativa a los recursos humanos	Nº Si	Nº No	Nº N/A	Resultado
7.1. Antes del empleo	2	0	0	100,00%
7.2. Durante el empleo	0	3	0	0,00%
7.3. Finalización del empleo o cambio en el puesto de trabajo	0	0	1	N/A
8. Gestión de activos	Nº Si	Nº No	Nº N/A	Resultado
8.1. Responsabilidad sobre los activos	4	0	0	100,00%
8.2. Clasificación de la información	0	3	0	0,00%
8.3. Manipulación de los soportes	0	0	3	N/A
9. Control de acceso	Nº Si	Nº No	Nº N/A	Resultado
9.1. Requisitos de negocio para el control de acceso	2	0	0	100,00%
9.2. Gestión de acceso de usuario	0	6	0	0,00%
9.3. Responsabilidades del usuario	0	0	1	N/A
9.4. control de acceso a sistemas y aplicaciones	5	0	0	100,00%
10. Criptografía	Nº Si	Nº No	Nº N/A	Resultado
10.1. Controles criptográficos	0	2	0	0,00%
11. Seguridad física y del entorno	Nº Si	Nº No	Nº N/A	Resultado
11.1. Áreas seguras	6	0	0	100,00%
11.2. Seguridad de los equipos	0	9	0	0,00%

> ... 16. Gestion de incidentes | 17. Seg. Infor. Contin Negocio | 18. Cumplimiento | **Resumen** | Resultados + : ◀

Ilustración 25. Hoja "Resumen". Fuente: Elaboración propia



3.1.6. Resultados

En esta hoja se facilita el visionado de los resultados obtenidos haciendo uso de la herramienta, así como también se posibilita la obtención de los resultados en formato PDF.

Resultados	
Información general de la auditoría	
Fecha de la auditoría	07/01/2024
Información general de la empresa	
Nombre de la empresa	
CIF	
Dirección	
Información general del responsable de auditoría	
Nombre completo	
DNI	
Cargo	
5. Políticas de seguridad de la información	
5.1. Directrices de gestión de la seguridad de la información	Resultado 50,00%
6. Organización de la seguridad de la información	
6.1. Organización interna	Resultado 0,00%
6.2. Los dispositivos móviles y teletrabajo	Resultado N/A
7. Seguridad relativa a los recursos humanos	
7.1. Antes del empleo	Resultado 100,00%
7.2. Durante el empleo	Resultado 0,00%
7.3. Finalización del empleo o cambio en el puesto de trabajo	Resultado N/A
8. Gestión de activos	
8.1. Responsabilidad sobre los activos	Resultado 100,00%
8.2. Clasificación de la información	Resultado 0,00%
8.3. Manipulación de los soportes	Resultado N/A
9. Control de acceso	
9.1. Requisitos de negocio para el control de acceso	Resultado 100,00%

> ... 16. Gestion de incidentes | 17. Seg. Infor. Contin Negocio | 18. Cumplimiento

Ilustración 26. Hoja "Resultados". Fuente: Elaboración propia



3.2. Funcionamiento y navegación de la herramienta

A continuación, en este subapartado se detallan las instrucciones para una rápida comprensión del funcionamiento del cuestionario automático de autoevaluación ISO 27001. Adicionalmente, se explica cómo proceder si se desea descargar un PDF con los resultados obtenidos. Toda esta información viene recopilada desde un punto de vista más visual y esquemático en la hoja “Instrucciones”, será desde esta hoja desde donde se debe de comenzar a emplear la herramienta.

En primer lugar la persona responsable debe de rellenar la información competente a la empresa y a quién está realizando la autoevaluación. Esto se realizaría dentro de la hoja de “*Información General*”. Para ello, dentro de la propia hoja “Instrucciones” se facilita el botón de acceso a “*Información General*”.

Procedimiento

En primer lugar la persona responsable debe de rellenar la información competente a la empresa y a quién está realizando la auditoría.

Información general de la auditoría	
Fecha de la auditoría	01/01/2024

Información general de la empresa	
Nombre de la empresa	
CIF	
Dirección	

Información general del responsable de auditoría	
Nombre completo	
DNI	
Cargo	

Para ello debe de acceder al apartado “información General” al cuál se puede acceder a través del siguiente botón:



Información General

Ilustración 27. Procedimiento 1. Fuente: Elaboración propia

Una vez rellenada la Información requerida en “*Información General*” ya se podrá comenzar a realizar el formulario a través del botón “*Comenzar Formulario*”.

Información general

Información general de la auditoría

Fecha de la auditoría	01/01/2024
-----------------------	------------

Información general de la empresa

Nombre de la empresa	Empresa A
CIF	1
Dirección	Calle A

Información general del responsable de auditoría

Nombre completo	Pepe
DNI	12345678A
Cargo	CISO

Comenzar formulario

Instrucciones Información general 5. Políticas Seg. Información 6. Organización Seg. Información 7. Se ... +

Ilustración 28. Procedimiento 2. Fuente: Elaboración propia

De cara a una mayor comprensión se detallará a continuación el proceso de cumplimentación del formulario de autoevaluación de la norma ISO 27001 de cara a evitar el surgimiento de cualquier duda referente a este proceso. Para ello, se usará a modo de ejemplo la cumplimentación del objetivo de control "5. Políticas de seguridad de la Información".

Tal y como se puede apreciar en la siguiente imagen para cada objetivo de control recogido en el Anexo A de la norma UNE/ISO 27001:2017 existe un subobjetivo de control "5.1. Directrices de gestión de la seguridad de la información" el cuál a su vez está formado por varios controles, que son el sujeto de análisis del presente cuestionario automático de autoevaluación.

5.1. Directrices de gestión de la seguridad de la información			
ID Control	Objetivo del control	Control	SI - NO - N/A
A.5.1.1	Políticas de la seguridad de la información	Existe un conjunto de políticas para la seguridad de la información definido, aprobado por la dirección, publicado y comunicado a los empleados y partes externas relevantes.	
A.5.1.2	Revisión de las políticas de la seguridad de la información	Se realizan revisiones periódicas de las políticas de seguridad de la información o siempre que se realicen cambios significativos.	

Ilustración 29. Procedimiento 3. Fuente: Elaboración propia

A continuación, para la cumplimentación de cada control, únicamente es necesario seleccionar la celda "SI - NO - N/A" de cada control clicando sobre ella, tras lo cual aparecerá una flecha que indica un listado desplegable con las opciones "SI", "NO" y "N/A". El usuario deberá seleccionar una de estas opciones clicando sobre ella y automáticamente se incorporará la respuesta en la celda.

5.1. Directrices de gestión de la seguridad de la información			
ID Control	Objetivo del control	Control	SI - NO - N/A
A.5.1.1	Políticas de la seguridad de la información	Existe un conjunto de políticas para la seguridad de la información definido, aprobado por la dirección, publicado y comunicado a los empleados y partes externas relevantes.	
A.5.1.2	Revisión de las políticas de la seguridad de la información	Se realizan revisiones periódicas de las políticas de seguridad de la información o siempre que se realicen cambios significativos.	<div style="border: 1px solid black; padding: 2px;"> SI NO N/A </div>

Ilustración 30. Procedimiento 4. Fuente: Elaboración propia

De cara a la realización de la presente explicación de la navegación y funcionamiento de la herramienta se seleccionaron las siguientes opciones para cada control:

5.1. Directrices de gestión de la seguridad de la información			
ID Control	Objetivo del control	Control	SI - NO - N/A
A.5.1.1	Políticas de la seguridad de la información	Existe un conjunto de políticas para la seguridad de la información definido, aprobado por la dirección, publicado y comunicado a los empleados y partes externas relevantes.	SI
A.5.1.2	Revisión de las políticas de la seguridad de la información	Se realizan revisiones periódicas de las políticas de seguridad de la información o siempre que se realicen cambios significativos.	NO

Ilustración 31. Procedimiento 5. Fuente: Elaboración propia

Una vez rellenado adecuadamente el objetivo de control, se deberá de proceder de forma análoga con el resto de objetivos de control. Lo cuál será posible a través de la navegación dentro del formulario facilitada por los botones localizados en la parte inferior de cada hoja del formulario:

5. Políticas de seguridad de la información

5.1. Directrices de gestión de la seguridad de la información			
ID Control	Objetivo del control	Control	SI - NO - N/A
A.5.1.1	Políticas de la seguridad de la información	Existe un conjunto de políticas para la seguridad de la información definido, aprobado por la dirección, publicado y comunicado a los empleados y partes externas relevantes.	SI
A.5.1.2	Revisión de las políticas de la seguridad de la información	Se realizan revisiones periódicas de las políticas de seguridad de la información o siempre que se realicen cambios significativos.	NO

Siguiente

Ilustración 32. Procedimiento 6. Fuente: Elaboración propia

Al igual que sucede con la hoja "5. Políticas de seguridad de la Información" para cada apartado se encuentran alojados en la parte inferior de la hoja los botones responsables de permitir la navegación por la herramienta, tal y como se puede apreciar también en el siguiente apartado a través de los botones "Siguiente" y "Anterior":

6.2. Los dispositivos móviles y teletrabajo			
ID Control	Objetivo del control	Control	SI - NO - N/A
A.6.2.1	Política de dispositivos móviles	Existen una política y unas medidas de seguridad adecuadas para la protección contra los riesgos de la utilización de dispositivos móviles.	N/A
A.6.2.2	Teletrabajo	Existen una política y unas medidas de seguridad adecuadas para proteger la información accedida, tratada o almacenada en emplazamientos de teletrabajo.	N/A

Anterior

Siguiente

Ilustración 33. Procedimiento 7. Fuente: Elaboración propia

Finalmente, se deberá de cumplimentar todos los apartados siendo el último el apartado "18. Cumplimiento", el cual a diferencia del resto en vez de contener un botón "Siguiente" dispone de un botón "Finalizar", el cual ya nos hace saber que hemos finalizado de completar el formulario.

18.2. Revisiones de la seguridad de la información			
ID Control	Objetivo del control	Control	SI - NO - N/A
A.18.2.1	Revisión independiente de la seguridad de la información	El enfoque de la organización para la gestión de la seguridad de la información y su implantación, es decir, objetivos de control, controles, políticas, procesos y procedimientos para la seguridad de la información, es sometido a una revisión independiente a intervalos planificados o siempre que se produzcan cambios significativos en la implantación de la seguridad.	NO
A.18.2.2	Cumplimiento de las políticas y normas de seguridad	Los directivos se aseguran que todos los procedimientos de seguridad dentro de su área de responsabilidad se realizan correctamente con el fin de cumplir las políticas y normas de seguridad y cualquier otro requisito de seguridad aplicable	NO
A.18.2.3	Comprobación del cumplimiento técnico	Se comprueba periódicamente que los sistemas de información cumplen las políticas y normas de seguridad de la información de la organización	NO

Anterior

Finalizar

> ... 16. Gestion de incidentes | 17. Seg. Infor. Contin Negocio | **18. Cumplimiento** | Resumen | Resultados

Ilustración 34. Procedimiento 8. Fuente: Elaboración propia



3.3. Análisis y obtención de resultados

Una vez completada toda la información referente a la empresa auditada, fecha de auditoría y el propio formulario de autoevaluación se pasaría a la fase correspondiente al análisis y obtención de resultados el cual se detallará en el presente subapartado.

El proceso de evaluación del formulario es automático, por ello, el usuario no tendrá que realizar ningún paso concreto para obtener los resultados de la auditoría. Para una mejor comprensión y detalle del proceso de evaluación, se ha incluido la hoja “Resumen” donde se puede observar el conteo que realiza la herramienta de las respuestas para cada uno de los objetivos de control y obteniendo en base a ello el resultado final. Se puede apreciar el resultado en las siguientes imágenes:

Resumen				
5. Políticas de seguridad de la información	Nº Si	Nº No	Nº N/A	Resultado
5.1. Directrices de gestión de la seguridad de la información	1	1	0	50,00%
6. Organización de la seguridad de la información	Nº Si	Nº No	Nº N/A	Resultado
6.1. Organización interna	0	5	0	0,00%
6.2. Los dispositivos móviles y teletrabajo	0	0	2	N/A
7. Seguridad relativa a los recursos humanos	Nº Si	Nº No	Nº N/A	Resultado
7.1. Antes del empleo	2	0	0	100,00%
7.2. Durante el empleo	0	3	0	0,00%
7.3. Finalización del empleo o cambio en el puesto de trabajo	0	0	1	N/A
8. Gestión de activos	Nº Si	Nº No	Nº N/A	Resultado
8.1. Responsabilidad sobre los activos	4	0	0	100,00%
8.2. Clasificación de la información	0	3	0	0,00%
8.3. Manipulación de los soportes	0	0	3	N/A
9. Control de acceso	Nº Si	Nº No	Nº N/A	Resultado
9.1. Requisitos de negocio para el control de acceso	2	0	0	100,00%
9.2. Gestión de acceso de usuario	0	6	0	0,00%
9.3. Responsabilidades del usuario	0	0	1	N/A
9.4. control de acceso a sistemas y aplicaciones	5	0	0	100,00%
10. Criptografía	Nº Si	Nº No	Nº N/A	Resultado
10.1. Controles criptográficos	0	2	0	0,00%
11. Seguridad física y del entorno	Nº Si	Nº No	Nº N/A	Resultado
11.1. Areas seguras	6	0	0	100,00%
11.2. Seguridad de los equipos	0	9	0	0,00%
12. Seguridad de las operaciones	Nº Si	Nº No	Nº N/A	Resultado
12.1. Procedimientos y responsabilidades operacionales	4	0	0	100,00%
12.2. Protección contra el software malicioso (malware)	0	1	0	0,00%
12.3. Responsabilidades del usuario	0	0	1	N/A
12.4. Registros y supervisión	4	0	0	100,00%
12.5. Control del software en explotación	0	1	0	0,00%
12.6. Gestión de la vulnerabilidad técnica	0	0	2	N/A
12.7. Consideraciones sobre la auditoría de sistemas de información	1	0	0	100,00%
13. Seguridad de las comunicaciones	Nº Si	Nº No	Nº N/A	Resultado
13.1. Gestión de la seguridad de las redes	0	3	0	0,00%
13.2. Intercambio de información	0	0	4	N/A

Ilustración 35. Análisis y obtención de resultados 1. Fuente: Elaboración propia

14. Adquisición, desarrollo y mantenimiento de los sistemas de información	Nº Si	Nº No	Nº N/A	Resultado
14.1. Requisitos de seguridad en los sistemas de información	3	0	0	100,00%
14.2. Seguridad en el desarrollo y en los procesos de soporte	0	9	0	0,00%
14.3. Datos de prueba	0	0	1	N/A
15. Relación con proveedores	Nº Si	Nº No	Nº N/A	Resultado
15.1 Seguridad en las relaciones con proveedores	3	0	0	100,00%
15.2. Gestión de la provisión de servicios del proveedor	0	2	0	0,00%
16. Gestión de incidentes de seguridad de la información	Nº Si	Nº No	Nº N/A	Resultado
16.1. Gestión de incidentes de seguridad de la información y mejoras	7	0	0	100,00%
17. Aspectos de seguridad de la información para la gestión de la continuidad de	Nº Si	Nº No	Nº N/A	Resultado
17.1 Continuidad de la seguridad de la información	0	3	0	0,00%
17.2. Redundancias	0	0	1	N/A
18. Cumplimiento	Nº Si	Nº No	Nº N/A	Resultado
18.1 Cumplimiento de los requisitos legales y contractuales	5	0	0	100,00%
18.2. Revisiones de la seguridad de la información	0	3	0	0,00%

Volver

Resultados

Ilustración 36. Análisis y obtención de resultados 2. Fuente: Elaboración propia

Tal y como se puede ver en las imágenes anteriores, para obtener la valoración de la empresa para cada apartado, la herramienta realiza un conteo del estatus de cada control que constituyen los diferentes objetivos de control de cada apartado.

Para ello, el valor de estudio se trata del porcentaje de controles que si cumplen la normativa para cada uno de los objetivos de control.

A modo de ejemplo, se facilita el resultado para el apartado de la normativa "5. Políticas de seguridad de la Información" con los datos de la explicación del subapartado de la memoria anterior, los cuáles se vuelven a facilitar para una mayor comprensión por parte del lector.

5. Políticas de seguridad de la información

5.1. Directrices de gestión de la seguridad de la información			
ID Control	Objetivo del control	Control	SI - NO - N/A
A.5.1.1	Políticas de la seguridad de la información	Existe un conjunto de políticas para la seguridad de la información definido, aprobado por la dirección, publicado y comunicado a los empleados y partes externas relevantes.	SI
A.5.1.2	Revisión de las políticas de la seguridad de la información	Se realizan revisiones periódicas de las políticas de seguridad de la información o siempre que se realicen cambios significativos.	NO

Siguiente

Ilustración 37. Análisis y obtención de resultados - Ejemplo 1. Fuente: Elaboración propia

Estos resultados arrojarían la siguiente valoración en la hoja resumen:

5. Políticas de seguridad de la información	Nº Si	Nº No	Nº N/A	Resultado
5.1. Directrices de gestión de la seguridad de la información	1	1	0	50,00%

Ilustración 38. Análisis y obtención de resultados - Ejemplo 2. Fuente: Elaboración propia

Como es fácilmente interpretable, la fórmula para la obtención de los resultados es la siguiente:

$$\text{Resultados}(\%) = \frac{N^{\circ} SI}{N^{\circ} SI + N^{\circ} NO} \times 100$$

Como es lógico y dado la diferente naturaleza de las empresas que pueden realizar el formulario ha sido necesaria la inclusión de una opción de respuesta “N/A” o lo que es lo mismo, que ese control no aplica a la empresa auditada, debiendo por tanto no afectar al resultado final.

Esta situación es contemplada por la aplicación tal y como se puede apreciar en la siguiente imagen en la que se ha establecido que existen objetivos de control que no aplican para la empresa auditada.

12. Seguridad de las operaciones	Nº Si	Nº No	Nº N/A	Resultado
12.1. Procedimientos y responsabilidades operacionales	4	0	0	100,00%
12.2. Protección contra el software malicioso (malware)	0	1	0	0,00%
12.3. Responsabilidades del usuario	0	0	1	N/A
12.4. Registros y supervisión	4	0	0	100,00%
12.5. Control del software en explotación	0	1	0	0,00%
12.6. Gestión de la vulnerabilidad técnica	0	0	2	N/A
12.7. Consideraciones sobre la auditoría de sistemas de información	1	0	0	100,00%

Ilustración 39. Análisis y obtención de resultados - Ejemplo 3. Fuente: Elaboración propia

Para concluir, los resultados obtenidos en la hoja “Resumen” así como la información recopilada en “Información General” son mostradas para su visualización siguiendo una estructura de informe en la hoja “Resultados” tal y como se puede apreciar en la siguiente imagen.



Resultados

Información general de la auditoría

Fecha de la auditoría	01/01/2024
-----------------------	------------

Información general de la empresa

Nombre de la empresa	Empresa A
CIF	1
Dirección	Calle A

Información general del responsable de auditoría

Nombre completo	Pepe
DNI	12345678A
Cargo	CISO

5. Políticas de seguridad de la información	Resultado
5.1. Directrices de gestión de la seguridad de la información	50,00%
6. Organización de la seguridad de la información	Resultado
6.1. Organización interna	0,00%
6.2. Los dispositivos móviles y teletrabajo	N/A
7. Seguridad relativa a los recursos humanos	Resultado
7.1. Antes del empleo	100,00%
7.2. Durante el empleo	0,00%
7.3. Finalización del empleo o cambio en el puesto de trabajo	N/A

Ilustración 40. Visionado de resultados 1. Fuente: Elaboración propia

8. Gestión de activos	Resultado
8.1. Responsabilidad sobre los activos	100,00%
8.2. Clasificación de la información	0,00%
8.3. Manipulación de los soportes	N/A
9. Control de acceso	Resultado
9.1. Requisitos de negocio para el control de acceso	100,00%
9.2. Gestión de acceso de usuario	0,00%
9.3. Responsabilidades del usuario	N/A
9.4. control de acceso a sistemas y aplicaciones	100,00%
10. Criptografía	Resultado
10.1. Controles criptográficos	0,00%
11. Seguridad física y del entorno	Resultado
11.1. Areas seguras	100,00%
11.2. Seguridad de los equipos	0,00%
12. Seguridad de las operaciones	Resultado
12.1. Procedimientos y responsabilidades operacionales	100,00%
12.2. Protección contra el software malicioso (malware)	0,00%
12.3. Responsabilidades del usuario	N/A
12.4. Registros y supervisión	100,00%
12.5. Control del software en explotación	0,00%
12.6. Gestión de la vulnerabilidad técnica	N/A
12.7. Consideraciones sobre la auditoría de sistemas de información	100,00%
13. Seguridad de las comunicaciones	Resultado
13.1. Gestión de la seguridad de las redes	0,00%
13.2. Intercambio de información	N/A
14. Adquisición, desarrollo y mantenimiento de los sistemas de información	Resultado
14.1. Requisitos de seguridad en los sistemas de información	100,00%
14.2. Seguridad en el desarrollo y en los procesos de soporte	0,00%
14.3. Datos de prueba	N/A

Ilustración 41. Visionado de resultados 2. Fuente: Elaboración propia



15. Relación con proveedores		Resultado
15.1 Seguridad en las relaciones con proveedores		100,00%
15.2. Gestión de la provisión de servicios del proveedor		0,00%
16. Gestión de incidentes de seguridad de la información		Resultado
16.1. Gestión de incidentes de seguridad de la información y mejoras		100,00%
17. Aspectos de seguridad de la información para la gestión de la continuidad de		Resultado
17.1 Continuidad de la seguridad de la información		0,00%
17.2. Redundancias		N/A
18. Cumplimiento		Resultado
18.1 Cumplimiento de los requisitos legales y contractuales		100,00%
18.2. Revisiones de la seguridad de la información		0,00%

Volver a Resumen

Descargar resultados en PDF

Ilustración 42. Visionado de resultados 3. Fuente: Elaboración propia

Finalmente, tal y como se puede apreciar en la última imagen, se dispone de un botón “*Descargar resultados en PDF*” el cual si se le hace click nos permite obtener un fichero en formato PDF.

Para la elaboración de esta funcionalidad se han utilizado las funciones Macro de Microsoft Excel, más concretamente, se ha implementado una función llamada “*GenerarPDF()*” a través de las funcionalidades proporcionadas por el entorno de desarrollo Microsoft Visual Basic for Applications. Dicha función Macro ha sido asignada al click sobre el botón mencionado anteriormente.

```

Microsoft Visual Basic for Applications
File Edit View Insert Format Debug Run Tools Add-Ins Window Help
Project - VBAProject
Sheet20 (Resumen)
Sheet21 (Resultados)
Sheet3 (Datos)
Sheet4 (Información general)
Sheet5 (BASE)
Sheet6 (5. Políticas Seg. Información)
Sheet7 (6. Organización Seg. Información)
Sheet8 (7. Seguridad relativa a RRHH)
Sheet9 (8. Gestión de activos)
ThisWorkbook
Modules
Module1
Properties - Module1
Module1 Module
Alphabetic Categorized
(Name) Module1

Cuestionario automático de autoevaluación ISO 27001.xlsm - Module1 (Code)
[General] GenerarPDF
Sub GenerarPDF()
    Dim newFileName As String
    newFileName = "Resultados Auditoria ISO 27001"
    FilePath = ActiveWorkbook.Path & _
        Application.PathSeparator & _
        newFileName & ".pdf"

    ActiveSheet.ExportAsFixedFormat _
        Type:=xlTypePDF, _
        FileName:=FilePath, _
        Quality:=xlQualityStandard, _
        IgnorePrintAreas:=False, _
        OpenAfterPublish:=True

End Sub

```

Ilustración 43. Función GenerarPDF(). Fuente: Elaboración propia



El código implementado para la realización de esta función se facilitará en el Anexo 1 al final de la presente memoria de acuerdo con los procedimientos establecidos.



4. Conclusiones

En este apartado final se desarrollarán las conclusiones obtenidas de la realización de este Trabajo Fin de Máster. Adicionalmente, se plantearán posibles mejoras adicionales y posibles futuros trabajos posteriores que continúen con la línea de este trabajo.

En primer lugar, el presente TFM nació fruto de la necesidad de realización de un cuestionario automático de cara a facilitar a empresas públicas o privadas una herramienta de autoevaluación automática del estado de implementación de la norma ISO 27001. De este primer punto surge el primer y gran objetivo que persigue este TFM: la realización de un cuestionario automático el cual proporcionase un mayor grado de conocimiento de las medidas a adoptar o implementar para poder obtener la certificación ISO27001. Facilitando en gran medida por tanto, a la empresa objeto de la auditoría y consecuentemente también a la empresa certificadora.

Para la consecución de este principal objetivo, en un primer lugar fue necesaria la realización de un análisis contextual e histórico que ayudase a comprender las causas y motivaciones que impulsaron el nacimiento y expansión de las normativas regulatorias en materia de Ciberseguridad. Como es lógico, dada la naturaleza del propio trabajo, el principal foco de atención fue la ISO 27001, haciendo hincapié en las diferentes versiones que existen de la norma. Esta última parte, fue sin lugar a duda una de las más importantes de este trabajo, al tener que evaluar cual iba a ser la versión concreta que se iba a utilizar.

Una de las dificultades que se encontraron en la realización de este trabajo fue la falta de accesibilidad para poder acceder a las normativas oficiales, estando el acceso a estas muchas veces sujeto únicamente a su compra en las webs oficiales a un precio elevado.

Finalmente, como ya se ha explicado detalladamente en el capítulo de esta memoria “2. Estado del arte”, se ha escogido la norma *UNE-EN ISO/IEC 27001:2017* al tratarse de una de las opciones más accesibles y que aplica a nuestro territorio, al ser la versión ofrecida por la UNE. Adicionalmente, el estudio de esta normativa posibilitó la consecución del objetivo adicional planteado al inicio de esta memoria correspondiente al aprendizaje y análisis del marco normativo de la ISO 27001.

Una vez finalizada estas primeras etapas de análisis y recopilado de información llegó el turno de enfocarse en la solución propuesta, la cual viene descrita en profundidad en el apartado “3. Solución propuesta” de esta memoria.



A través de Microsoft Excel se ha podido realizar un cuestionario automático con una interfaz sencilla y amigable que incorporan los controles descritos por la norma *UNE-EN ISO/IEC 27001:2017* en su Anexo A. Añadido a esto, haciendo uso de las herramientas automáticas proporcionadas por las funcionalidades Macro de Microsoft Excel se ha realizado una función Macro que hace posible la obtención de los resultados del cuestionario en formato PDF. Uno de los principales objetivos que se plantearon al inicio de este TFM a título personal fueron el aprendizaje de estas herramientas Macro, al gozar de gran utilidad para trabajos con una alta carga de uso de Microsoft Excel como el que actualmente desempeño.

En conclusión, el presente TFM me ha permitido profundizar enormemente en el marco legal que rigen a las organizaciones y empresas en materia de ciberseguridad, completando de esta forma a los conocimientos ya adquiridos en esta materia durante la realización del máster. Adicionalmente, me ha permitido adquirir conocimientos en funcionalidades de Microsoft Excel con las cuales carecía de experiencia previa, todos estos aprendizajes me han proporcionado o perfilado conocimientos que serán de gran utilidad para mi puesto de trabajo como Auditor IT.

4.1. Posibles Mejoras

Debido a la naturaleza del TFM, al tratarse de un trabajo con unos tiempos acotados, en este subapartado se detallarán las posibles mejoras que se han encontrado o planteado durante la realización de este trabajo y no ha sido posible incluirlas por una cuestión de tiempo, estas mejoras pueden dotar a este TFM de una mayor profundidad o utilidad.

El principal punto de mejora sería el planteado en los objetivos adicionales recogidos en el apartado *"1. Introducción"* de esta memoria, concretamente, en el subapartado *"1.2. Objetivos"*. En este subapartado se hacen referencia a objetivos relacionados con el ENS (Esquema Nacional de Seguridad). Tal y como ya se ha detallado anteriormente, este marco normativo es un esquema inspirado en la familia de estándares ISO 27000 y, más concretamente, en la ISO 27001, lo que consecuentemente implica que si una organización ya dispone de la certificación ENS, esta certificación ya garantiza la cumplimentación de gran cantidad de los controles que cubre la ISO 27001.

En vista de esta situación, una de las posibles mejoras sería la incorporación y automatización de esta funcionalidad, es decir, que el cuestionario contemplase esta situación y ocultase o resaltase automáticamente que controles ya se encuentran cubiertos por la certificación ENS y por lo tanto no haría falta preguntar sobre ellos a la persona que estuviese realizando el cuestionario.



Adicionalmente, esta situación se podría extrapolar a otras normativas o estándares actuales como la Ley de protección de datos (LOPD), el Reglamento General de Protección de Datos (RGPD) o las nuevas versiones de la Norma ISO 27001. («¿Qué es el RGPD? | IBM»)

4.2. Posibles Trabajos

Fruto de la realización del presente TFM surgen los posibles futuros nuevos trabajos:

- Incorporación de la herramienta de autoevaluación de la ISO 27001 a una página o solución web para dotarla de una mayor facilidad de difusión y de una mayor visibilidad gráfica.
- Incorporación y automatización del mapeo de los controles de la ISO 27001 al disponer de otras certificaciones orientadas a la ciberseguridad. Este mapeo podría tener un enfoque bidireccional y no solamente teniendo la ISO 27001 como objetivo. Es decir, que el disponer de la certificación ISO 27001 también entrañaría que se están cumpliendo controles de otras certificaciones y no solamente al revés.



Anexo I

A continuación, se facilita el código de la función GenerarPDF() desarrollada a través de la herramienta Microsoft Visual Dinamics con el objetivo de facilitar los resultados del cuestionario en formato PDF. [TeachEXCEL]

```
Sub GenerarPDF()
```

```
    Dim newFileName As String
```

```
    newFileName = "Resultados Auditoria ISO 27001"
```

```
    FilePath = ActiveWorkbook.Path & _
```

```
        Application.PathSeparator & _
```

```
        newFileName & ".pdf"
```

```
    ActiveSheet.ExportAsFixedFormat _
```

```
        Type:=xlTypePDF, _
```

```
        FileName:=FilePath, _
```

```
        Quality:=xlQualityStandard, _
```

```
        IgnorePrintAreas:=False, _
```

```
        OpenAfterPublish:=True
```

```
End Sub
```



ANEXO OBJETIVOS DE DESARROLLO SOSTENIBLE

Grado de relación del trabajo con los Objetivos de Desarrollo Sostenible (ODS).

Objetivos de Desarrollo Sostenibles	Alto	Medio	Bajo	No Procede
ODS 1. Fin de la pobreza.				X
ODS 2. Hambre cero.				X
ODS 3. Salud y bienestar.				X
ODS 4. Educación de calidad.				X
ODS 5. Igualdad de género.				X
ODS 6. Agua limpia y saneamiento.				X
ODS 7. Energía asequible y no contaminante.				X
ODS 8. Trabajo decente y crecimiento económico.	X			
ODS 9. Industria, innovación e infraestructuras.	X			
ODS 10. Reducción de las desigualdades.				X
ODS 11. Ciudades y comunidades sostenibles.				X
ODS 12. Producción y consumo responsables.				X
ODS 13. Acción por el clima.				X
ODS 14. Vida submarina.				X
ODS 15. Vida de ecosistemas terrestres.				X
ODS 16. Paz, justicia e instituciones sólidas.				X
ODS 17. Alianzas para lograr objetivos.				X



Reflexión sobre la relación del TFG/TFM con los ODS y con el/los ODS más relacionados.

El presente TFM ha sido orientado a una realidad de la actualidad que sufren y afectan tanto las empresas públicas u organizaciones como las privadas. Se trata de la ciberseguridad y el marco normativo que la rige hoy en día ante las innumerables amenazas que sufren estas empresas. Por este mismo motivo, no ha sido directamente creado con el objetivo de tener una estrecha relación con los Objetivos del Desarrollo Sostenible o ODS.

A pesar de todo esto, se puede relacionar este TFM con los siguientes ODS:

ODS 8. Trabajo decente y crecimiento económico

El presente TFM se puede relacionar muy directamente con el ODS 8. Industria innovación e infraestructuras.

A través de la incorporación de los controles necesarios para obtener la certificación ISO 27001 se garantiza el cumplimiento de una gran cantidad de buenas prácticas en materia de ciberseguridad, lo que también conllevaría un gran esfuerzo en materia de procedimientos tanto para el cuidado como para la formación de los trabajadores. No es ningún secreto que una de las principales vías de ataque para los ciber criminales son los propios trabajadores, a través de su ignorancia y errores humanos. Esta certificación garantiza una serie de estándares mínimos referente a los procedimientos de actuación de los propios empleados en su puesto de trabajo, lo que está muy directamente relacionado.

Por otra parte la formación de los empleados en materia de ciberseguridad también se traduce en una menor exposición a ciber ataques, lo que puede suponer un gran ahorro económico para las empresas implicadas.

ODS 9. Industria, innovación e infraestructuras.

El presente TFM se puede relacionar muy directamente con el ODS 8. Industria innovación e infraestructuras.

Como ya hemos visto en el ODS anterior, a través de la incorporación de los controles necesarios para obtener la certificación ISO 27001 se garantiza el cumplimiento de una gran cantidad de buenas prácticas en materia de ciberseguridad, lo que conllevaría una gran innovación e inversión en procedimientos y estructuras que ayudarían a evitar ciber incidentes, que entre otras cosas pueden afectar tremendamente al desarrollo de la actividad económica de la empresa u organización.

Añadido a esto, es una realidad que hoy en día muchas empresas ven a la ciber seguridad como un alto coste anual “poco útil”, ya que en muchas ocasiones se trata



de un gasto o inversión que no es visible a menos que se sufran los ataques o incidentes, es decir, sufre una paradoja: cuanto mejor ciber seguridad se tenga, menos visibilidad e importancia se percibe de esta, puesto que menos incidentes y ataques tenderá a sufrir la empresa y a la inversa, cuanto peor ciber seguridad se tenga más conscientes seremos de la necesidad de esta al sufrir múltiples ataques e incidentes.

Afortunadamente, día a día más empresas evitan caer en este error.



Bibliografía

- ARPANET: El nacimiento de la Internet moderna. [en línea] 2024. [consulta: 10 septiembre 2024]. Disponible en: <https://www.welivesecurity.com/es/we-live-progress/arpamet-nacimiento-internet-moderna/>.
- Asociación Española para la Calidad I AEC. AEC [en línea] 2024. [consulta: 10 septiembre 2024]. Disponible en: <https://www.aec.es/>.
- BASTERO, M., 2024. Historia de Internet: ¿cómo nació y cuál fue su evolución? *Marketing4eCommerce* [en línea] 2024. [consulta: 10 septiembre 2024]. Disponible en: <https://marketing4ecommerce.net/historia-de-internet/>.
- CERT Coordination Center. En: Page Version ID: 1230739997, *Wikipedia* [en línea], 2024. [consulta: 10 septiembre 2024]. Disponible en: https://en.wikipedia.org/w/index.php?title=CERT_Coordination_Center&oldid=1230739997.
- Esquema Nacional de Seguridad (ENS) Certificación - AENOR. [en línea], 2024. [consulta: 10 septiembre 2024]. Disponible en: <https://www.aenor.com/certificacion/tecnologias-de-la-informacion/ens-esquema-nacional>.
- ISO - The ISO Survey. *ISO* [en línea], 2024. [consulta: 10 septiembre 2024]. Disponible en: <https://www.iso.org/the-iso-survey.html>.
- ISO 27001 - Certificado ISO 27001 punto por punto - Presupuesto Online. *Norma ISO 27001* [en línea], 2024. [consulta: 10 septiembre 2024]. Disponible en: <https://www.normaiso27001.es/>.
- ISO 27001:2013 Mejora. [en línea], 2024. [consulta: 10 septiembre 2024]. Disponible en: <https://www.pmg-ssi.com/2014/09/iso-27001-2013-mejora/>.
- ISO/IEC 27001. En: Page Version ID: 162244676, *Wikipedia, la enciclopedia libre* [en línea], 2024. [consulta: 10 septiembre 2024]. Disponible en: https://es.wikipedia.org/w/index.php?title=ISO/IEC_27001&oldid=162244676.
- ISO/IEC 27001 Nueva edición de la Norma: cambios y plazo - RINA.org. [en línea], 2024. [consulta: 10 septiembre 2024]. Disponible en: <https://www.rina.org/es/news/iso-iec-27001>.
- ISO/IEC 27001 y ENS, binomio perfecto para la ciberseguridad | N° 348. [en línea], 2024. [consulta: 10 septiembre 2024]. Disponible en: <https://revista.aenor.com/348/isoiec-27001-y-ens-binomio-perfecto-para-la-ciberseguridad.html>.



ISOWin: La nueva ISO 27001 2013. [en línea], 2024. [consulta: 10 septiembre 2024].
Disponible en: <https://isowin.es/nueva-norma-ISO-27001-2013/>.

Norma ISO 27001: importancia para la seguridad de la información - Think Big
Empresas. [en línea], 2020. [consulta: 10 septiembre 2024]. Disponible en:
<https://web.archive.org/web/20200910184300/https://empresas.blogthinkbig.com/norma-iso-27001-seguridad-informacion/>.

PIB (US\$ a precios actuales) | Data. [en línea], 2024. [consulta: 10 septiembre 2024].
Disponible en:
<https://datos.bancomundial.org/indicador/NY.GDP.MKTP.CD?end=2022&start=2006&view=chart>.

¿Qué es el RGPD? | IBM. [en línea], 2024. [consulta: 10 septiembre 2024]. Disponible
en: <https://www.ibm.com/es-es/cloud/compliance/gdpr-eu>.

SÁNCHEZ, G.R., 2024. El gusano Morris: Un hito en la historia de la ciberseguridad.
Crónica Seguridad [en línea]. [consulta: 10 septiembre 2024]. Disponible en:
<https://cronicaseguridad.com/2024/04/18/el-gusano-morris-un-hito-en-la-historia-de-la-ciberseguridad/>.

SOCIALL, 2022. ENS e ISO 27001: Similitudes, diferencias y ámbitos de aplicación.
RCQUALITY [en línea]. [consulta: 10 septiembre 2024]. Disponible en:
<https://www.rcquality.es/esquema-nacional-seguridad-o-iso-27001/>.

SOLUTIONS, G., 2023. ¿Qué es la norma ISO 27001 y para qué sirve? *GlobalSuite
Solutions* [en línea]. [consulta: 10 septiembre 2024]. Disponible en:
<https://www.globalsuitesolutions.com/es/que-es-la-norma-iso-27001-y-para-que-sirve/>.

UNE-ISO/IEC 17799:2002 Tecnología de la Información. Código de... [en línea], 2024.
[consulta: 10 septiembre 2024]. Disponible en:
<https://www.une.org/encuentra-tu-norma/busca-tu-norma/norma?c=N0028064>.

UNE-ISO/IEC 27001:2007 Tecnología de la información. Técnicas ... [en línea], 2024.
[consulta: 10 septiembre 2024]. Disponible en:
<https://www.une.org/encuentra-tu-norma/busca-tu-norma/norma/?c=N0040067>.

