WEBINAR:

¿Cómo conseguir elaborar un sistema robusto en materia de ciberseguridad y proteger a todos los usuarios de tecnologías digitales?

- ✓ Seguridad de la información ISO 27001
- ✓ Ciberseguridad ISO 27110
- ✓ Protección de la privacidad ISO 27701

Martes, 19 DE MARZO de 2024, a las 9:00h.

ORGANIZA:

Cofinanciado por la Unión Europea

Ministerio de Hacienda

Fondos Europeos

Gobierno de Canarias

Consejería de Universidades, Ciencia e Innovación y Cultura

Agencia Canaria de Investigación, Innovación y Sociedad de la Información

RedCIDE INNOVACIÓN

ASINCA

COLABORA:

DMS DAS MANAGEMENT SOLUTIONS

Título de la jornada ¿Cómo conseguir elaborar un sistema robusto en materia de ciberseguridad y proteger a todos los usuarios de tecnologías digitales? Seguridad de la Información ISO 27001. Ciberseguridad y Protección de la Privacidad ISO 27110 e ISO 27701.

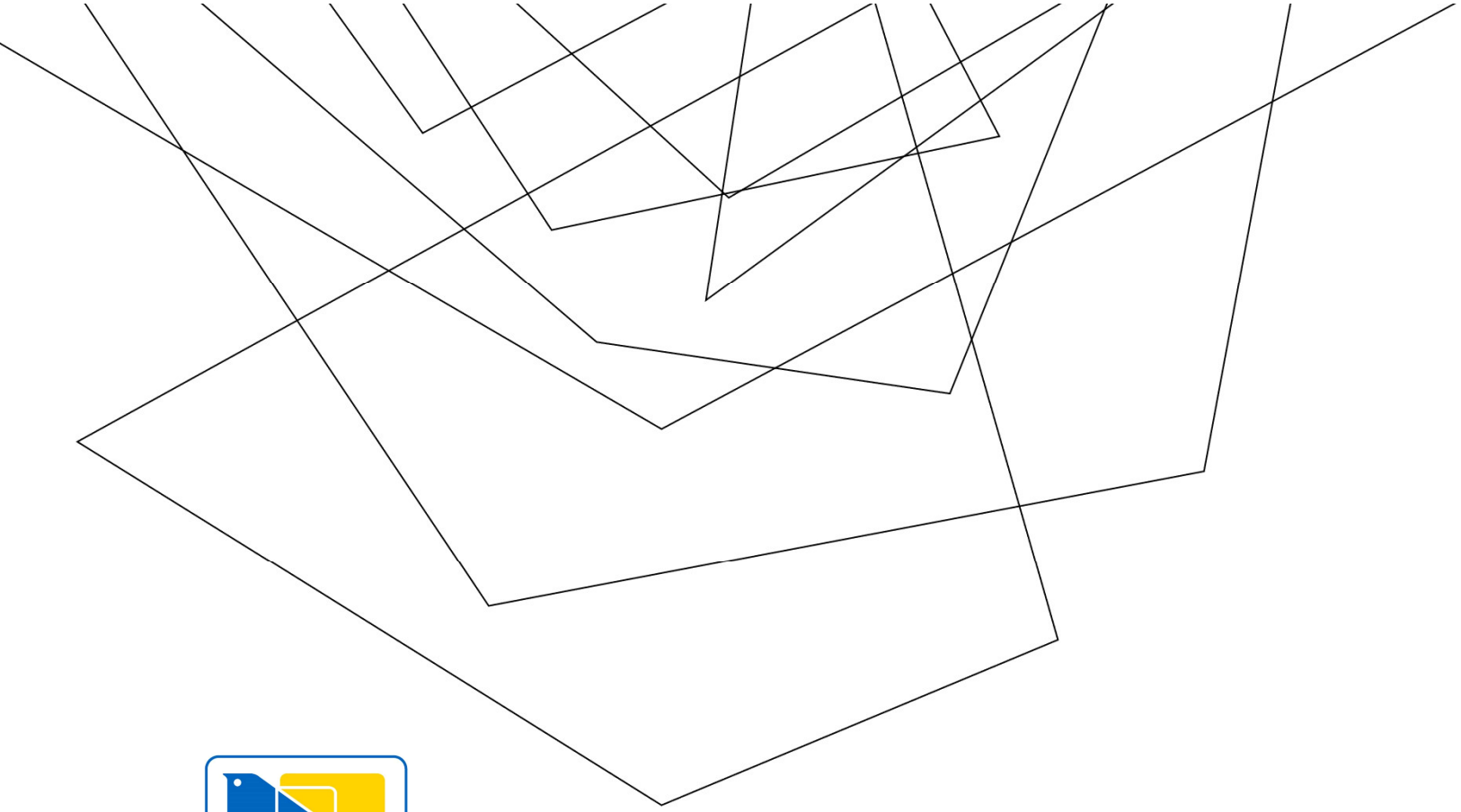
Objetivo Informar a los asistentes sobre las obligaciones y responsabilidades penales que impone la actual normativa y la conveniencia de disponer de sistemas de gestión de cumplimiento normativo

Contenido

- **Seguridad de la Información- ISO 27001.** Los Sistemas de Gestión de Seguridad de la Información (SGSI) son el medio más eficaz de minimizar los riesgos, al asegurar que se identifican y valoran los procesos de negocio y/o servicios de TI, activos y sus riesgos, considerando el impacto para la organización, y se adoptan los controles y procedimientos más eficaces y coherentes con la estrategia de negocio, considerando la mejora continua.
- **Protección de la Privacidad. ISO 27701.** Esta norma de seguridad de la información recientemente publicada proporciona orientación para las organizaciones que buscan establecer sistemas para apoyar el cumplimiento del RGPD y otros requisitos de privacidad de datos.
- **Ciberseguridad en las Organizaciones**, nueva ISO 27110 para la mejora de la Ciberseguridad en las organizaciones. Esta norma está dirigida a conseguir elaborar un sistema robusto en materia de ciberseguridad y proteger a todos los usuarios de tecnologías digitales.

Dirigido a: responsables de cumplimiento normativo, de sistemas de gestión, CIO, RRHH y a todas las personas interesadas en la materia.

Ponente: José María Pérez Carmona, consultor-auditor de sistemas de gestión.



SEGURIDAD DE LA INFORMACIÓN - ISO 27001

José María Pérez Carmona

Socio – Director de Proyectos en DAS MANAGEMENT


Seguridad de la información, ciberseguridad y privacidad
ISO/IEC 27001
ISO/IEC 27001 especifica los requisitos para implementar y mantener un sistema de gestión de seguridad de la información (SGSI) eficaz.
Las organizaciones que obtienen la certificación ISO/IEC 27001 fortalecen su capacidad para protegerse contra los ciberataques y ayudan a prevenir el acceso no deseado a información sensible o confidencial.

EVOLUCIÓN

ISO/IEC 27002:2022

ISO/IEC 27001:2022

PRINCIPALES ACTUALIZACIONES EN ISO 27001:2022

1. En cuanto a la estructura de alto nivel (Anexo SL), las cláusulas del 4 al 10 no han tenido variación alguna.

ANEXO SL ESTRUCTURA DE ALTO NIVEL	CLAUSULAS DEL ANEXO SL QUE NO VARIAN EN ISO 27001:2022
1. Alcance 2. Referencias Normativas 3. Términos y definiciones 4. Contexto de la organización 5. Liderazgo 6. Planificación 7. Soporte 8. Operación 9. Evaluación del desempeño 10. Mejora	4. Contexto de la organización 5. Liderazgo 6. Planificación 7. Soporte 8. Operación 9. Evaluación del desempeño 10. Mejora

ANEXO A: ISO 27001: 2017

14 dominios,114 controles

*A.5 Políticas de Seguridad de la Información
*A.6 Organización de la Seguridad de la Información
*A.7 Seguridad relativa a los recursos humanos
*A.8 Gestión de Activos
*A.9 control de Acceso
*A.10 Criptografía
*A.11 Seguridad Física y del entorno
*A.12 Seguridad de las operaciones

Anexo A: ISO 27001: 2022

4 dominios, 93 controles

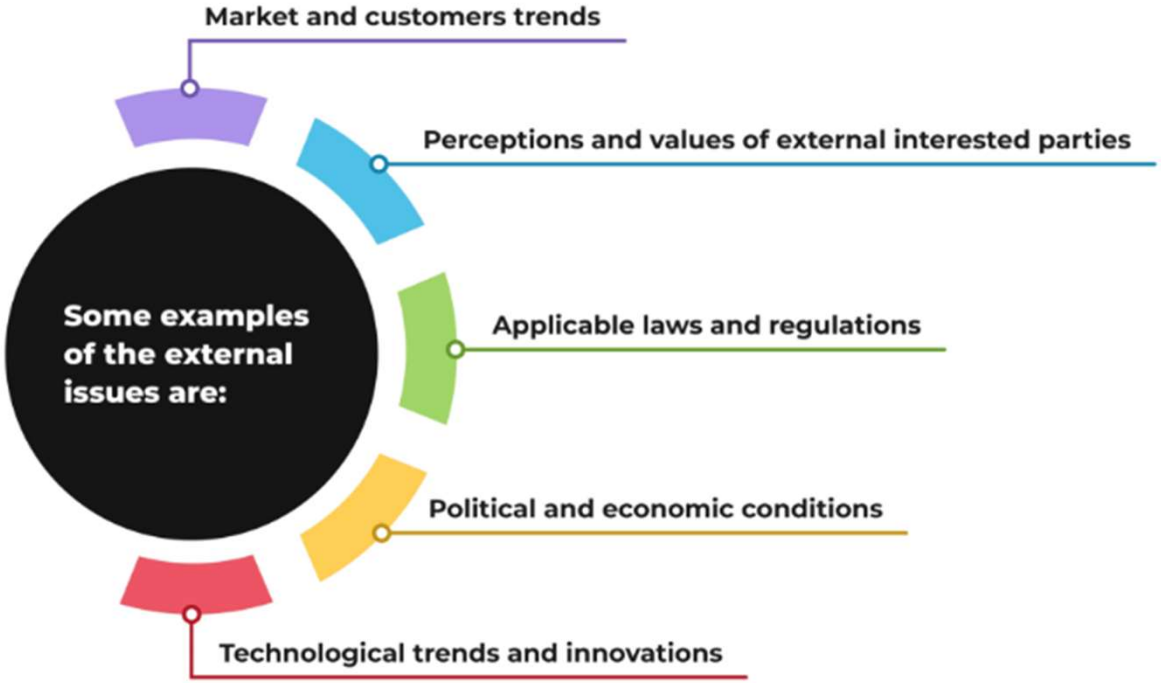
*A.5 Controles Organizacionales
*A.6 Controles de Personas
*A.7 Controles Físicos
*A.8 Controles Tecnológicos

ISO / IEC 27001: 2022 se publicó el 25 de octubre 2022, reemplazando la versión 2013

Las organizaciones certificadas según ISO/IEC 27001:2013 deben completar antes de tres años la transición a la versión 2022

A partir del 31 de octubre de 2023, las auditorías de certificación iniciales solo están permitidas de acuerdo con ISO/IEC 27001:2022.


Estructura de ISO 27001
Evaluación y tratamiento de riesgos
Implementación de medidas de seguridad


Market and customers trends
Perceptions and values of external interested parties
Some examples of the external issues are:
Applicable laws and regulations
Political and economic conditions
Technological trends and innovations

Al definir cómo implementar un Sistema de Gestión de Seguridad de la Información, las reglas requeridas se pueden escribir en forma de políticas, procedimientos y otros tipos de documentos, o se pueden implementar en forma de procesos y tecnologías establecidos que no están documentados. **La norma ISO 27001 define qué documentos son obligatorios**, es decir, cuáles deben existir como mínimo.

Lo que se debe documentar	Referencia ISO 27001	Por lo general, se documenta a través de
Ámbito de aplicación del SGSI	Cláusula 4.3	Documento de alcance del SGSI
Política de seguridad de la información	Cláusula 5.2	Política de Seguridad de la Información
Evaluación de riesgos y proceso de tratamiento de riesgos	Cláusula 6.1.2	Evaluación de riesgos y metodología de tratamiento
Declaración de aplicabilidad	Cláusula 6.1.3 d)	Declaración de aplicabilidad
Plan de tratamiento de riesgos	Cláusulas 6.1.3 e, 6.2 y 8.3	Plan de tratamiento de riesgos
Objetivos de seguridad de la información	Cláusula 6.2	Lista de objetivos de seguridad
Informe de evaluación de riesgos y tratamiento	Cláusulas 8.2 y 8.3	Informe de Evaluación de Riesgos y Tratamiento
Inventario de activos	Control A.5.9*	Inventario de activos, o lista de activos en el registro de riesgos
Uso aceptable de los activos	Control A.5.10*	Política de seguridad informática
Procedimiento de respuesta a incidentes	Control A.5.26*	Procedimiento de gestión de incidencias
Requisitos legales, reglamentarios y contractuales	Control A.5.31*	Lista de requisitos legales, reglamentarios y contractuales
Procedimientos operativos de seguridad para la gestión de TI	Control A.5.37*	Procedimientos de seguridad para el departamento de TI
Definición de roles y responsabilidades de seguridad	Controles A.6.2 y A.6.6*	Acuerdos, acuerdos de confidencialidad y especificación de responsabilidades en cada política y procedimiento de seguridad
Definición de configuraciones de seguridad	Control A.8.9*	Procedimientos de seguridad para el departamento de TI
Principios de ingeniería de sistemas seguros	Control A.8.27*	Política de Desarrollo Seguro

Registros ISO 27001 que son obligatorios

Lo que se debe registrar	Referencia ISO 27001	Por lo general, se graba a través de
Capacitaciones, habilidades, experiencia y calificaciones	Cláusula 7.2	Certificados de formación y CV
Seguimiento y resultados de medición	Cláusula 9.1	Informe de medición
Programa de auditoría interna	Cláusula 9.2	Programa de Auditoría Interna
Resultados de las auditorías internas	Cláusula 9.2	Informe de Auditoría Interna
Resultados de la revisión por la dirección	Cláusula 9.3	Actas de Revisión por la Dirección
Resultados de las acciones correctivas	Cláusula 10.2	Formulario de Acción Correctiva
Registros de actividades de usuario, excepciones y eventos de seguridad	Control A.8.15*	Registros automáticos en sistemas de información

Un ejemplo de SGSI: Implementación de varios controles para un activo

Tomemos una computadora portátil como ejemplo: puede disminuir el riesgo de los datos en esta computadora portátil aplicando varios controles diferentes, por ejemplo:

- Escriba un procedimiento que indique que no puede dejar la computadora portátil en el automóvil.
- Proteja su computadora portátil con una contraseña, de modo que si se la roban, será más difícil que alguien acceda a su información.
- Cifre su disco: este es un nivel aún más alto de protección de la información.
- Pida a sus empleados que firmen una declaración que los obligue a pagar por cualquier daño que ocurra en caso de que ocurra un incidente de este tipo.
- Capacite y concientice a sus empleados de que existen riesgos de seguridad si dejan sus computadoras portátiles en sus automóviles.

Ahora, proteger una computadora portátil puede parecer simple, pero el problema crece cuando tiene cientos de computadoras portátiles, docenas de servidores, una multitud de software, muchos empleados, etc. Con tantos datos y usuarios, sería extremadamente difícil gestionar todos los controles (salvaguardas) sin algún tipo de sistema, y ese sistema es el SGSI. Un sistema de gestión de seguridad de la información es un marco que explica cómo gestionar un sistema de seguridad tan complejo.


1 | Identify stakeholders and their expectations
2 | Identify which risks exist for the information
3 | Implement all the controls and other risk treatment methods
ISMS
IMPLEMENTATION
STEPS
4 | Continuously measure
5 | Make continuous improvement

¿Quiénes son las partes interesadas y cómo puede identificarlas según las normas ISO 27001 e ISO 22301?


employees
clients
shareholders / owners of the business
employee families
Interested parties could include
government agencies / regulators
media
emergency services (e.g., firefighters, police, ambulance, etc.)
suppliers and partners

Normas de apoyo a la norma ISO 27001

La norma ISO/IEC 27002 proporciona directrices para la implementación de los controles enumerados en el Anexo A de la norma ISO 27001. Puede ser muy útil, ya que proporciona detalles sobre cómo implementar estos controles.

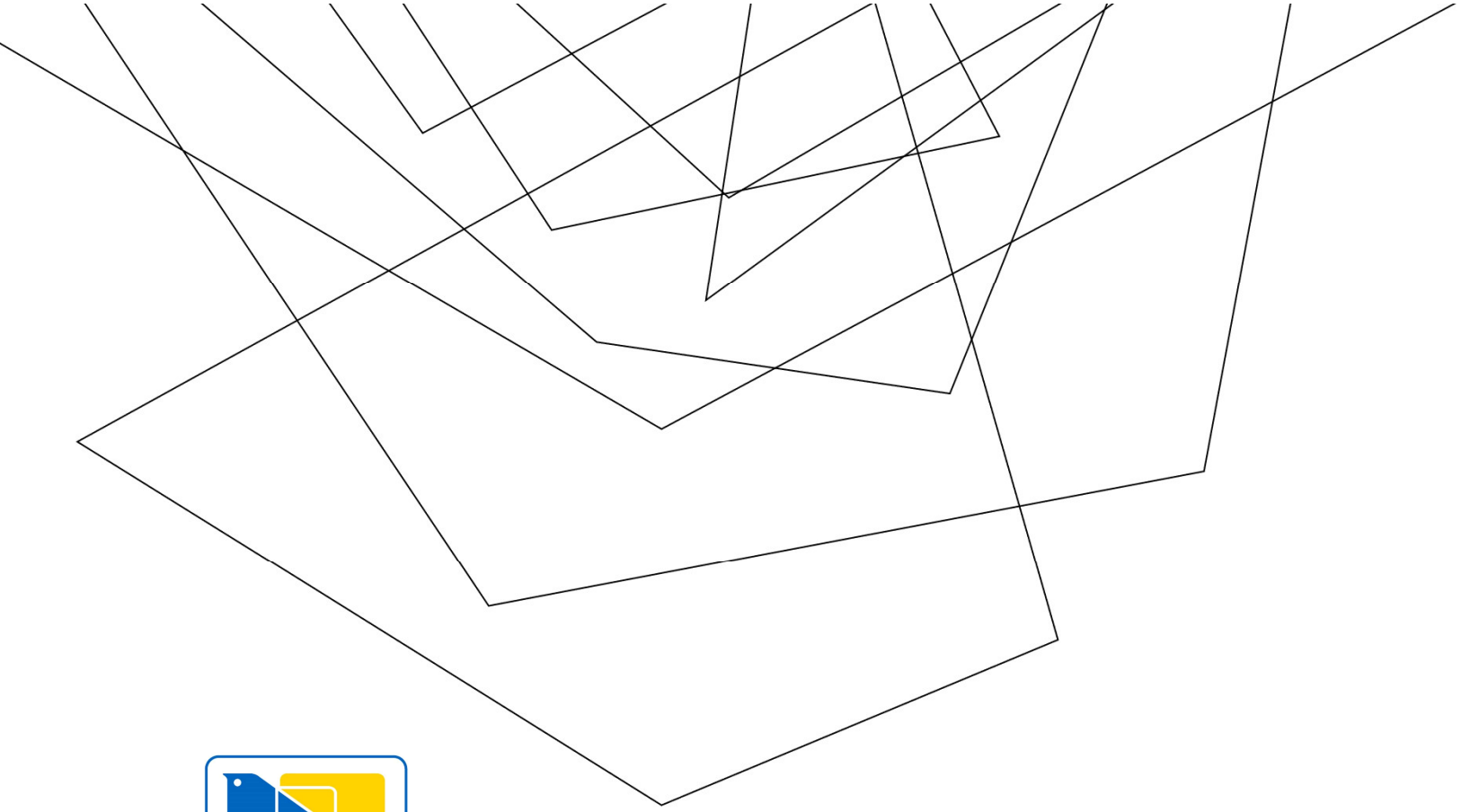
La norma ISO/IEC 27004 proporciona directrices para la medición de la seguridad de la información: encaja bien con la norma ISO 27001, ya que explica cómo determinar si el SGSI ha alcanzado sus objetivos.

La norma ISO/IEC 27005 proporciona directrices para la gestión de riesgos de seguridad de la información. Es un muy buen complemento de la norma ISO 27001, ya que proporciona detalles sobre cómo realizar la evaluación y el tratamiento de riesgos, probablemente la etapa más difícil de la implementación.

La norma ISO/IEC 27017 proporciona directrices para la seguridad de la información en entornos de nube. Se trata de un código de prácticas basado en la norma ISO/IEC 27002 para servicios en la nube.

La norma ISO/IEC 27018 proporciona directrices para la protección de la privacidad en entornos de nube. Es un código de prácticas basado en la norma ISO/IEC 27002 para la protección de la información de identificación personal (PII) en nubes públicas que actúan como procesadores de PII.

La norma ISO/IEC 27031 proporciona directrices sobre lo que hay que tener en cuenta a la hora de desarrollar la continuidad de las actividades de las tecnologías de la información y la comunicación (TIC). Esta norma es un gran vínculo entre la seguridad de la información y las prácticas de continuidad del negocio.



CHECKLIST PARA IMPLEMENTAR EL ESTÁNDAR ISO 27001

José María Pérez Carmona

Socio – Director de Proyectos en DAS MANAGEMENT

Los 20 pasos de la checklist para implementar el estándar ISO 27001

La **aplicación de la norma ISO 27001** supone una inversión importante de tiempo, esfuerzo y recursos: si intentas hacer demasiado de una vez, te sentirás abrumado. Por eso, la mejor forma de abordar esta tarea es dividirla en conjuntos de trabajo más pequeños y factibles.

1. Conseguir la aceptación y el apoyo
2. Establecer un órgano de gobernanza
3. Crear una hoja de ruta
4. Definir un ámbito de aplicación
5. Crear una política de seguridad de la información
6. Definir la metodología de evaluación de los riesgos
7. Crear un registro de los riesgos
8. Realizar la evaluación de los riesgos
9. Redactar la declaración de aplicabilidad
10. Redactar el plan de tratamiento de los riesgos
11. Definir cómo medir la eficacia de los controles
12. Implementar los controles de seguridad
13. Crear un programa de formación y concientización
14. Hacer funcionar la checklist de la ISMS
15. Hacer el seguimiento y la medición de la ISMS
16. Crear un inventario con InvGate Insight
17. Realizar auditorías internas
18. Disponer de un plan para auditorías externas
19. Tomar medidas correctivas cuando sea necesario
20. Incorporar la mejora continua

1. Conseguir la aceptación y el apoyo

Como la norma ISO 27001 no es una actividad para hacer una sola vez y desligarse para siempre, necesitarás apoyo. Así que prepara el escenario o fracasarás con el primer obstáculo: consigue el aval de la empresa, de los equipos de asistencia y de tus colegas.

En concreto, debes hacer lo siguiente:

- Recopila información sobre las ventajas de la norma ISO 27001 para poder exponerlas, así como los motivos de por qué es necesaria.
- Identifica a las partes interesadas de tu organización que actuarán como promotores de la iniciativa.
- No te olvides de tu service desk y de los equipos de soporte técnico, que tendrán que estar familiarizados con los requisitos en materia de seguridad de la información.

2. Establecer un órgano de gobernanza

La norma necesita un órgano de gobernanza que la respalde.

Así que en este paso de la checklist para implementar el estándar ISO 27001:

- Designa un director de proyecto que monitoree la implementación de la ISMS.
- Selecciona un equipo para llevar a cabo las actividades de aplicación.
- Aborda la implementación como un proyecto para que cuente con el apoyo y la gobernanza adecuados.

3. Crear una hoja de ruta

Para que la aplicación tenga éxito se requiere una hoja de ruta bien constituida que sirva de guía al equipo.

Para ello:

- Utiliza el ciclo Deming, que consiste en planificar, hacer, comprobar y actuar para reconocer lagunas o desafíos, así como para captar ideas de mejora y corrección.
- Trabaja con tu órgano de gobernanza y el equipo del proyecto para establecer hitos clave.
- Crea criterios de calidad para que tú y tu equipo se aseguren de que todo, en cada etapa, se completó eficazmente, antes de pasar a la siguiente fase.

4. Definir un ámbito de aplicación

Muchas organizaciones muestran problemas con la **implementación de la norma ISO 27001** porque no toman en cuenta su ámbito de aplicación.

Así que en esta fase:

- Comprueba los requisitos del alcance de la norma y compáralos con las necesidades específicas de tu organización.
- Trabaja con tu equipo para determinar qué debe protegerse o asegurarse para que coincida con cualquier otro objetivo estratégico.
- Identifica las dependencias y los puntos de contacto.
- Comprende el impacto completo que tendrá en tu organización; identificando cualquier otro equipo que pudiera verse afectado por tus decisiones en materia de seguridad de la información.

5. Crear una política de seguridad de la información

La creación de una **política de seguridad de la información** es crucial en el proceso de implementación, ya que establece qué está permitido y qué prohibido.

Aquí, los consejos de esta fase de la checklist para implementar el estándar ISO 27001:

- Si cuentas con un equipo de gobernanza, riesgo o cumplimiento, pregunta si existen plantillas que puedas utilizar para que tengan un aspecto coherente con la documentación de políticas, de modo que sea fácil de comprender por el personal.
- Define los requisitos básicos de seguridad de la información de tu organización, y recuerda que los detalles vienen de la mano de los procesos y procedimientos que la sustentarán.
- Incluye una sección de objetivos para establecer qué tipo de seguridad de la información es necesaria.
- Asigna funciones y responsabilidades para garantizar que todos saben a quién corresponde la implementación, el mantenimiento y la elaboración de reportes sobre el rendimiento de la ISMS.

6. Definir la metodología de la evaluación de los riesgos

La gestión del riesgo es un componente clave de la norma. Como tal, resulta fundamental crear una metodología de evaluación sólida para definir las reglas para identificar dichos riesgos, los impactos y sus probabilidades, así como el nivel aceptable para la organización.

Así que haz lo siguiente:

- Codifica la forma en que tu organización gestionará los riesgos de seguridad de la información.
- Crea una matriz para identificar la probabilidad del riesgo y su impacto.
- Identifica escenarios en los que la información, los sistemas o los servicios podrían verse comprometidos.

7. Crear un registro de los riesgos

La checklist para implementar el estándar ISO 217001 también contempla crear un registro de los riesgos para identificar, priorizar y actuar cuando éstos aparezcan.

Los consejos en esta fase son:

- Asegúrate de que sea fácil registrar y gestionar los riesgos.
- Crea resúmenes claros y fáciles de entender de cada riesgo.
- Garantiza que sean visibles la probabilidad y el impacto de cada riesgo.

8. Realizar la evaluación de los riesgos

Una vez que tengas tu registro, es hora de **realizar las evaluaciones de los riesgos de la norma ISO 27001.**

Al efectuarlas:

- Asegúrate de que todos están familiarizados con la metodología de los riesgos definida en los pasos anteriores.
- Identifica las amenazas y vulnerabilidades.
- Evalúa la probabilidad y el impacto de los riesgos.
- Selecciona y prioriza las opciones de tratamiento de los riesgos.
- Aplica los tratamientos elegidos.
- Monitorea y revisa de forma continua todos los riesgos.

9. Redactar la declaración de aplicabilidad

Una vez concluido el proceso de evaluación y tratamiento de los riesgos, comprenderás claramente los controles ISO 27001 Anexo A. El documento de la Declaración de Aplicabilidad o Statement of Applicability (SoA) debe enumerar todos los controles aplicables, proporcionar las razones para su selección u omisión, y describir cómo se implementan en la organización.

Entonces, cuando redactes tu SoA haz lo siguiente:

- Identifica qué controles se aplican en tu organización.
- Describe brevemente cada control aplicable.
- Explica las razones para incluir o excluir controles de la SoA.
- Describe cómo se aplica y gestiona cada control.
- Aporta pruebas de que el control funciona según lo previsto y es eficaz para reducir los riesgos a un nivel aceptable.
- Garantiza que la SoA se revisa y actualiza periódicamente para reflejar los cambios en el Sistema de Gestión de la Seguridad de la Información de la organización y también para avalar que cada control sigue siendo adecuado para su propósito.

10. Redactar el plan de tratamiento de los riesgos

El plan es necesario para reaccionar ante los riesgos que puedan afectar la confidencialidad, integridad y disponibilidad de los activos de información o CIA.

Al momento de crearlo:

- Diseña una respuesta para cada riesgo (Tratamiento de Riesgos).
- Asigna un responsable a cada riesgo identificado.
- Asigna responsables de actividades y mitigación de riesgos.
- Establece fechas objetivo para completar las actividades de tratamiento de riesgos para que puedan ser rastreadas y gestionadas a lo largo del tiempo.

11. Definir cómo medir la eficacia de tus controles

Para medir la eficacia de tus controles, necesitas una directriz sólida. De lo contrario, obtendrás la ISMS de Schrödinger.

Así que considera:

- Un plan para medir los objetivos de los controles.
- Crea Indicadores Clave de Rendimiento o KPIs para medir la eficacia de tus controles, como el número de incidentes de seguridad evitados, la reducción de la exposición al riesgo, el porcentaje de personas que completaron la formación adecuada o el índice de cumplimiento de los reglamentos o normas pertinentes.
- Lleva a cabo pruebas periódicas de los controles para identificar debilidades y vulnerabilidades y para determinar qué tan bien funcionan los controles en la práctica.

12. Implementar los controles de seguridad

Esta etapa de la implementación ayuda a los departamentos de IT a controlar los riesgos que podrían afectar la integridad de los activos de información.

En esta fase:

- Asegúrate de que las políticas y procedimientos adecuados respalden tus nuevos controles.
- Cuenta con protocolos para hacer cumplir los nuevos comportamientos y gestionar las excepciones.

13. Crear un programa de formación y concientización

Una **ISO 27001** necesitará formación y un plan de concientización para garantizar que se integren los cambios en los comportamientos y las formas de trabajo.

Por lo tanto:

- Crea contenidos de capacitación y difúndelos entre todos.
- Trabaja con RR.HH. para garantizar que la formación sobre la ISO se encuentra en las actividades de onboarding, y también que se requieren encuentros periódicos de actualización.
- Define las expectativas de los empleados en cuanto a su papel en el mantenimiento de la ISMS.
- Capacita al personal sobre las amenazas comunes a las que se enfrenta tu organización y cómo responder a ellas.

14. Hacer funcionar la checklist de la ISMS

La **checklist de para implementar el estándar ISO 27001** te ayuda a gestionar los riesgos, controles e incidentes de seguridad.

Consta de cuatro secciones principales:

- Planificación de un Programa de Seguridad de la Información.
- Desarrollo de políticas, procedimientos, normas, directrices y documentación.
- Implementación de los controles.
- Medición de las métricas de rendimiento.

17. Realizar auditorías internas

Una excelente manera de prepararse para las auditorías externas y de mantener la transparencia es mediante las auditorías internas.

En ese sentido:

- Asigna recursos internos con las habilidades y competencias necesarias y que estén excluidas del desarrollo y mantenimiento de la ISMS.
- Verifica la conformidad con los requisitos de la norma, el alcance y la SoA.
- Comparte los resultados de la auditoría interna con el órgano de gobernanza de la ISMS y la alta dirección, incluidos los hallazgos, los riesgos y las no conformidades.
- Soluciona todos los problemas identificados antes de proceder con la auditoría externa.

18. Disponer de un plan para las auditorías externas

Este es uno de los pasos finales de la checklist para implementar el estándar ISO 27001, tras haber ejecutado el trabajo duro y realizado la auditoría interna.

Ahora:

- Contrata a un auditor ISO 27001 independiente.
- Realiza una Auditoría de Fase 1 consistente en una revisión exhaustiva de la documentación; y obtén información sobre si estás preparado para pasar a la Auditoría de Fase 2.
- Lleva a cabo la Auditoría de Fase 2 que involucra pruebas realizadas en la ISMS para asegurar el diseño adecuado, la implementación y la funcionalidad en curso, y para evaluar la imparcialidad, la idoneidad y la aplicación efectiva y el funcionamiento de los controles.

19. Tomar medidas correctivas cuando sea necesario

Un plan para gestionar las acciones correctivas incluye:

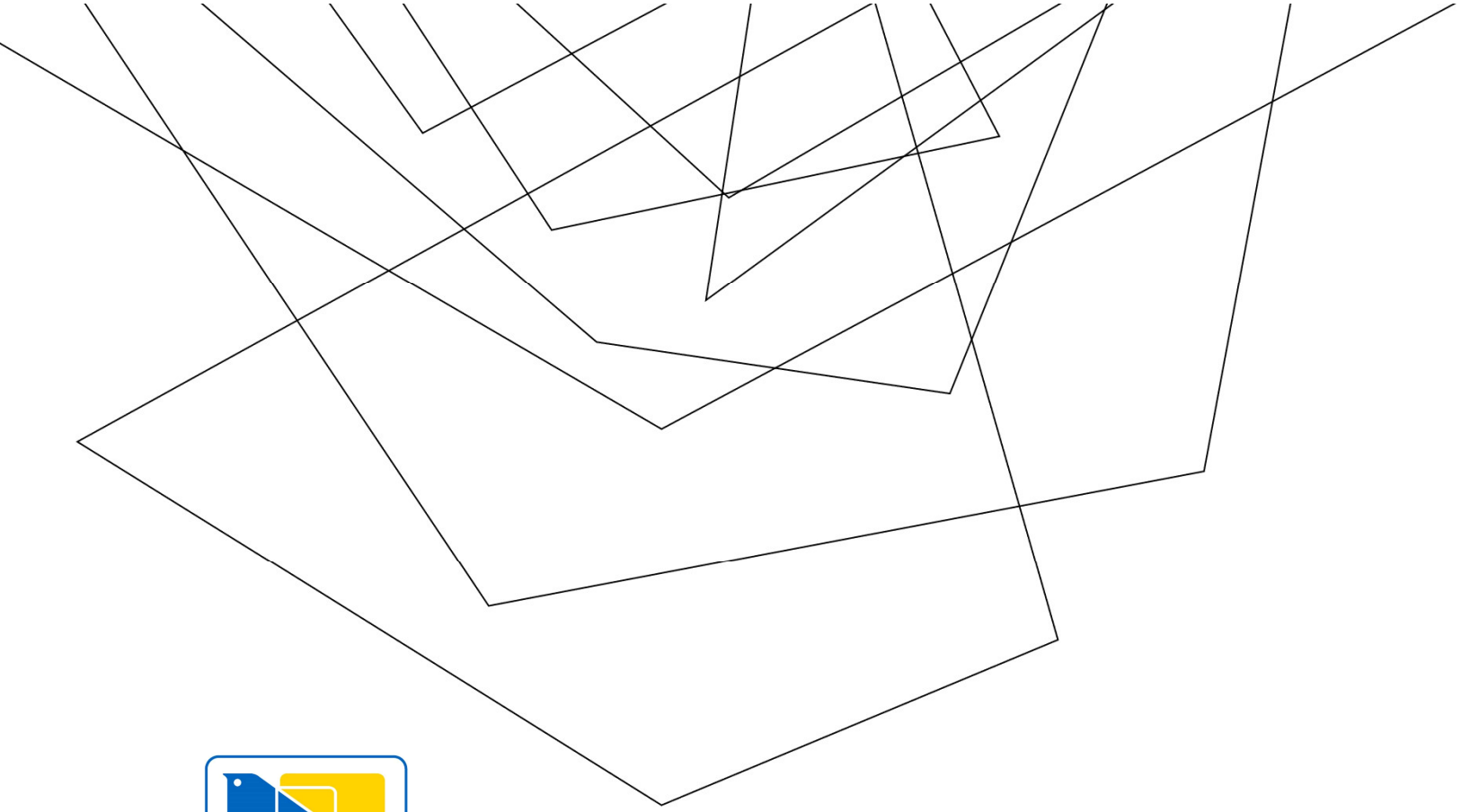
- Asegurarse de que se abordan todos los requisitos de la norma ISO 27001.
- Examinar si la organización y su personal siguen los procesos especificados y documentados.
- Garantizar que la organización cumple los requisitos contractuales con terceros y socios.
- Abordar cualquier no conformidad identificada por el auditor de la norma ISO 27001.
- Revisar la validación formal del auditor tras la resolución de hallazgos y no conformidades.

20. Incorporar la mejora continua

Para cerrar, debes contar con un plan de mejora a lo largo del tiempo.

Entre los aspectos a tener en cuenta figuran los siguientes:

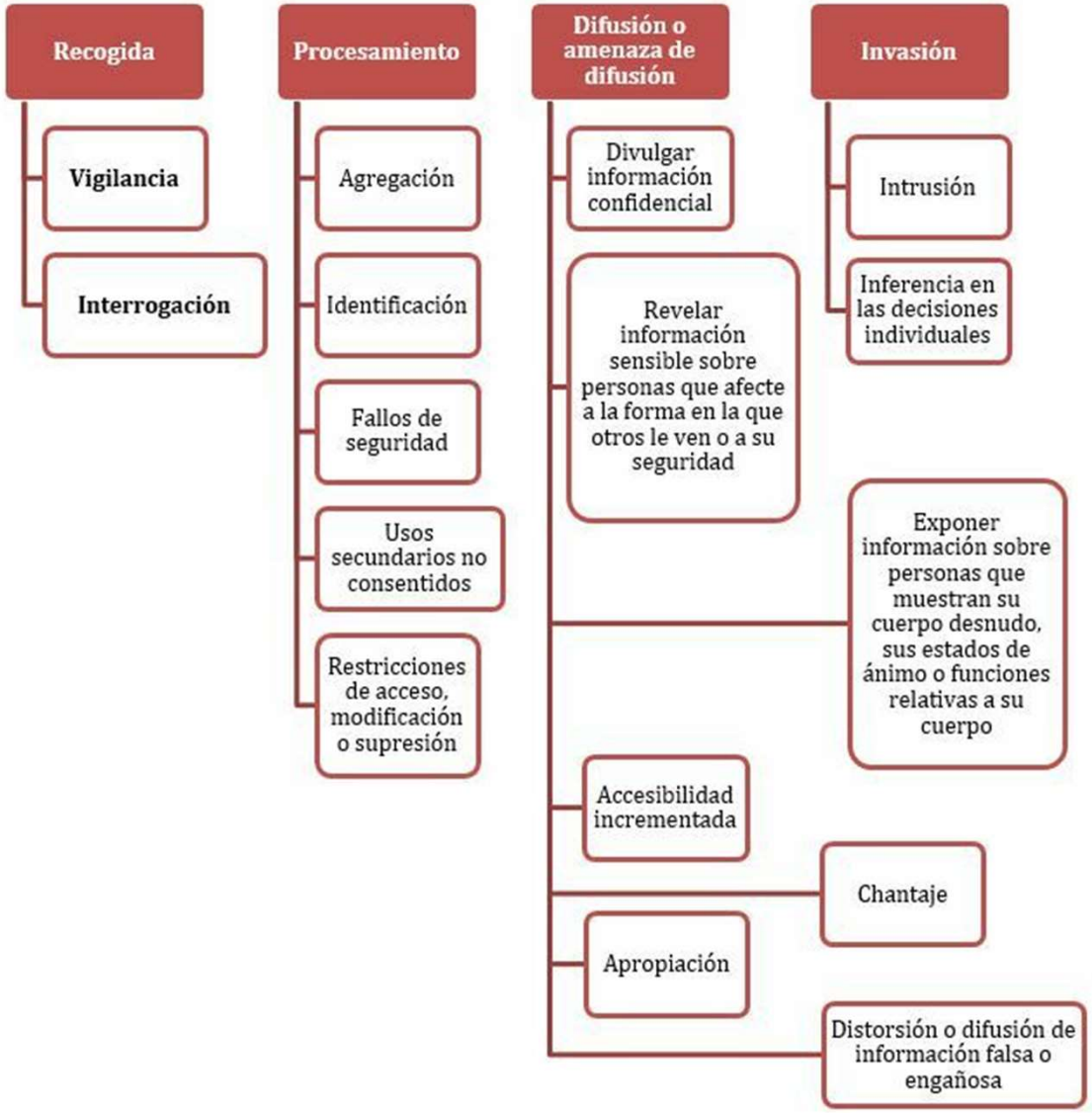
- Planifica revisiones al menos una vez al año para asegurar que tus controles permanecen alineados con las necesidades del negocio y continúan siendo adecuados para su propósito y uso.
- Asegúrate de que la ISMS y sus objetivos siguen siendo adecuados y eficaces.
- Garantiza que la alta dirección permanece informada y actualizada sobre todas las actividades de información críticas.



PROTECCIÓN DE LA PRIVACIDAD. ISO 27701

José María Pérez Carmona

Socio – Director de Proyectos en DAS MANAGEMENT


Recogida
Vigilancia
Interrogación
Procesamiento
Agregación
Identificación
Fallos de seguridad
Usos secundarios no consentidos
Restricciones de acceso, modificación o supresión
Difusión o amenaza de difusión
Divulgar información confidencial
Revelar información sensible sobre personas que afecte a la forma en la que otros le ven o a su seguridad
Exponer información sobre personas que muestran su cuerpo desnudo, sus estados de ánimo o funciones relativas a su cuerpo
Accesibilidad incrementada
Chantaje
Apropiación
Distorsión o difusión de información falsa o engañosa
Invasión
Intrusión
Inferencia en las decisiones individuales

Tanto si tenemos ayuda externa para las tareas técnicas como si tenemos personal en plantilla, la siguiente tabla muestra algunas de las cuestiones que se han de tratar al poner en marcha el PDS para abordar a la vez el RGPD.

Área	
Seguridad de los datos personales (Artículos 5.1.f, 32 y 39)	¿Qué tipos de datos personales se recogen, tratan y almacenan? ¿Son datos especialmente protegidos? ¿Protegemos estos últimos con seudonimización y cifrado? ¿Están documentados los controles y protocolos que aplican a datos personales? ¿Existen controles técnicos y organizativos específicos para cada categoría de datos y tratamiento? ¿Cómo se determinan las pérdidas de confidencialidad, integridad y disponibilidad? ¿Se realiza una evaluación de los riesgos para la privacidad? ¿Se cifran los datos personales en el almacenamiento y cuando se transmiten? ¿Tenemos capacidad de anonimizar y seudonimizar los datos personales?

Notificación de brechas de privacidad (Artículos 33 y 34)	Para cada tratamiento de datos: ¿somos responsables o encargados? Los registros de los tratamientos, los inventarios de datos personales y sus métricas, ¿nos permiten identificar brechas de datos? Si tenemos DPO, ¿está incluido en los planes y procedimientos de gestión de incidentes? En caso de incidente, ¿tenemos controles específicos para mitigar los riesgos de las personas afectadas por brechas de datos personales? ¿Se ha incluido en los planes de respuesta a incidentes la notificación en 72 horas a las autoridades de control?

Gestión de encargados / responsables del tratamiento (Artículo 28)	¿Tenemos los datos y contactos de todos los encargados de tratamiento? Y si somos encargados de los tratamientos de otros ¿tenemos los datos y contactos de los responsables de estos tratamientos? Nuestra evaluación de riesgos, ¿contiene cuestiones sobre las medidas técnicas y organizativas para la protección de privacidad dirigidas a los encargados del tratamiento? ¿Hemos redactado las cláusulas contractuales que incluiremos en los contratos con terceros que vayan a actuar de encargados del tratamiento de datos personales? ¿Hemos revisado los contratos existentes con responsables de tratamiento anteriores para que incluyan estas cláusulas? Para cada tratamiento del que seamos responsables ¿requerimos a los encargados que nos pidan autorización antes de subcontratar a su vez el tratamiento? Para cada tratamiento del que seamos encargados ¿incluyen nuestras políticas de seguridad los requisitos del artículo 32 del RGPD ?

Artículo 32
UE RGDP
"Seguridad del tratamiento"

=> razón: 83, 74, 75, 76, 77
=> administrative fine: Art. 83 (4) lit a

1. Teniendo en cuenta el estado de la técnica, los costes de aplicación, y la naturaleza, el alcance, el contexto y los fines del tratamiento, así como riesgos de probabilidad y gravedad variables para los derechos y libertades de las personas físicas, el responsable y el encargado del tratamiento aplicarán medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo, que en su caso incluya, entre otros:
=> Artículo: 24

a) la seudonimización y el cifrado de datos personales;
=> Artículo: 4

b) la capacidad de garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento;

c) la capacidad de restaurar la disponibilidad y el acceso a los datos personales de forma rápida en caso de incidente físico o técnico;

d) un proceso de verificación, evaluación y valoración regulares de la eficacia de las medidas técnicas y organizativas para garantizar la seguridad del tratamiento.

2. Al evaluar la adecuación del nivel de seguridad se tendrán particularmente en cuenta los riesgos que presente el tratamiento de datos, en particular como consecuencia de la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos.
=> razón: 75

3. La adhesión a un código de conducta aprobado a tenor del artículo 40 o a un mecanismo de certificación aprobado a tenor del artículo 42 podrá servir de elemento para demostrar el cumplimiento de los requisitos establecidos en el apartado 1 del presente artículo.

4. El responsable y el encargado del tratamiento tomarán medidas para garantizar que cualquier persona que actúe bajo la autoridad del responsable o del encargado y tenga acceso a datos personales solo pueda tratar dichos datos siguiendo instrucciones del responsable, salvo que esté obligada a ello en virtud del Derecho de la Unión o de los Estados miembros.

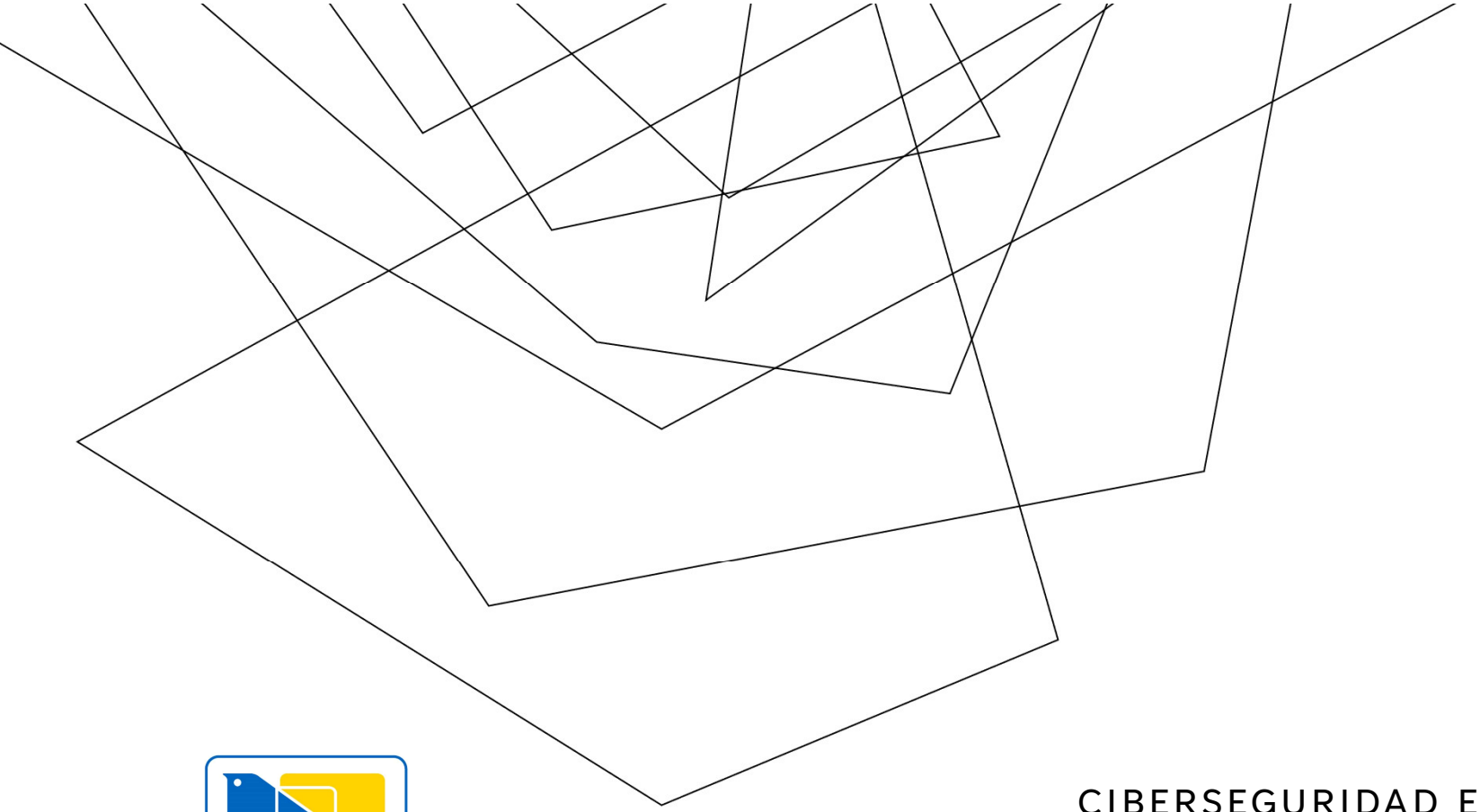
Registro de actividades de tratamiento (Artículo 30)	Para cada tratamiento sabemos: ¿qué tipo de datos personales recogemos? ¿cómo y desde dónde se recogen los datos? ¿cómo y dónde se realiza cada parte del tratamiento? ¿cómo y a dónde se transfieren? ¿cómo y dónde se almacenan, protegen y borran? ¿qué políticas de retención y destrucción tenemos en marcha? ¿se siguen y revisan?

Privacidad por diseño y por defecto (Artículo 25)	Qué datos personales son necesarios para cada tratamiento que gestionamos como responsables o encargados? Nuestras políticas actuales, ¿limitan la cantidad de datos personales que se pueden recoger, bien sea por diseño de los formularios o por otras medidas de seguridad? Si contratamos un equipo de desarrollo o adquirimos nuevas aplicaciones, ¿incorporan los principios de privacidad en los requisitos de diseño de nuevas aplicaciones?

Derechos de los propietarios de datos (Artículos 12, 13, 14, 15,16 y 17; Razones 63 y 64)	¿Hemos actualizado nuestros protocolos para informar a los propietarios de los datos y para recabar su consentimiento? ¿Tenemos procedimientos para clasificar e inventariar los datos de carácter personal y poder responder a las solicitudes de los usuarios sobre su información personal? Nuestros procedimientos actuales, ¿permiten a los propietarios de los datos acceder de forma segura a los datos personales que tenemos de ellos?, ¿tenemos otros datos personales a los que los propietarios no pueden acceder directamente?, ¿cómo se generan los informes sobre estos últimos y cómo se comunican de forma segura a los propietarios de los datos que lo soliciten? ¿Incluyen en nuestras políticas chequeos u otros procedimientos para revisar y corregir datos personales incorrectos o desactualizados? ¿Tenemos en marcha mecanismos para notificar a los propietarios cuando se modifican o se borran sus datos personales Art. 19 RGPD ? ¿Utilizamos perfilado o toma de decisiones automatizadas basados en datos personales y los tratamos conforme al Art. 22 RGPD ? ¿Tenemos en marcha procedimientos para no retener los datos personales más allá del tiempo necesario para el tratamiento o si el propietario decide ejercer su derecho de supresión? ¿Cómo se ejecutan y revisan estos procedimientos? ¿Disponen los encargados de la seguridad de la información y contactos actualizados sobre los terceros a quienes se transfieren los datos?

Para cumplir con el RGPD tienes que garantizar los derechos y libertades de las personas desde la misma definición del *tratamiento* de sus datos personales. Para ello:

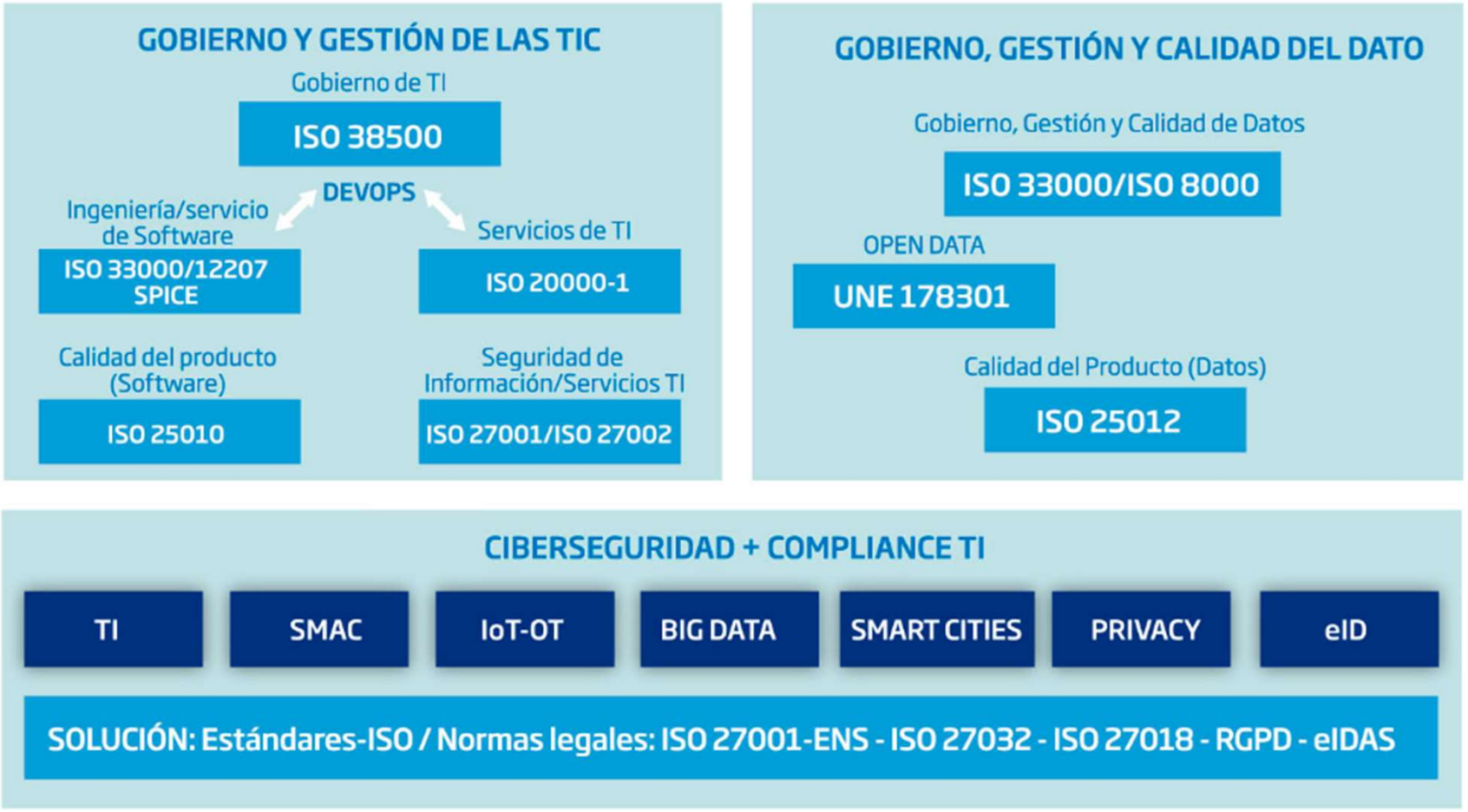
La **Análisos de riesgos** servirá para priorizar también las medidas tecnológicas a implantar. Revisaremos que tenemos los canales tecnológicos, incluidos aquellos canales online (las políticas de privacidad web, las cookies, las apps para móviles), adecuados para: informar, obtener el consentimiento, garantizar los derechos y notificar las posibles brechas de seguridad.



CIBERSEGURIDAD EN LAS ORGANIZACIONES, ISO/IEC TS 27110:2021

José María Pérez Carmona

Socio – Director de Proyectos en DAS MANAGEMENT


GOBIERNO Y GESTIÓN DE LAS TIC
Gobierno de TI
ISO 38500
DEVOPS
Ingeniería/servicio de Software
ISO 33000/12207 SPICE
Servicios de TI
ISO 20000-1
Calidad del producto (Software)
ISO 25010
Seguridad de Información/Servicios TI
ISO 27001/ISO 27002
GOBIERNO, GESTIÓN Y CALIDAD DEL DATO
Gobierno, Gestión y Calidad de Datos
ISO 33000/ISO 8000
OPEN DATA
UNE 178301
Calidad del Producto (Datos)
ISO 25012
CIBERSEGURIDAD + COMPLIANCE TI
TI
SMAC
IoT-OT
BIG DATA
SMART CITIES
PRIVACY
eID
SOLUCIÓN: Estándares-ISO / Normas legales: ISO 27001-ENS - ISO 27032 - ISO 27018 - RGPD - eIDAS


eIDAS-
PSC
(UE 910/2014)
Esquema
Nacional
de Seguridad
(RD 3/2010)
Reglamento
General de
Protección de Datos
RGPD (UE 2016/679)
(ISO 27701)
CIBER
SEGURIDAD
SMAC + IT + IoT + OT
ISO 27001
Ciber
Seguridad Cloud
(Seguridad & Privacidad)
ISO 27001/27017/
27018
Ciber
Seguridad
del Dato
(ISO 25012)
Sistema
de Gestión
de Seguridad de
la Información
ISO 27001/27032
Ciber
Seguridad
Industrial
(ISO 27001/
IEC 62443)

ENLACES A VIDEOS RELACIONADOS:

Políticas de seguridad para la pyme (youtube.com)

CCN

Ciberconsejos - Recomendaciones de Ciberseguridad (youtube.com)

Ciberconsejos - Buenas prácticas en el empleo de tecnología (youtube.com)

Ciberseguridad para la empresa (1/4) (youtube.com)

Ciberseguridad para la empresa (2/4) - YouTube

Ciberseguridad para la empresa (3/4) (youtube.com)

Ciberseguridad para la empresa (4/4) (youtube.com)

ASINCA
ASOCIACION INDUSTRIAL DE CANARIAS

Escanea el código QR para añadir este contacto.

DMS
DAS MANAGEMENT SOLUTIONS

José María Pérez Carmona

Director de Proyectos. Asociado

+34 647434161

josemaria.perezcarmona@das-consultores.com

www.dasmanagementsolutions.com