UNIVERSIDAD SERGIO ARBOLEDA | Colsubsidio

Diplomado de Ciberseguridad y Gestión de Seguridad de la Información

Módulo 4:

Implementación y Gestión en el Estándar ISO 27001

Sesión 2:

Aplicación práctica: diseño inicial de un SGSI y planificación de controles

OBJETIVO DE LA SESIÓN:

Aplicar los conceptos de ISO/IEC 27001:2022 diseñando un esquema inicial de SGSI y comprendiendo cómo se definen los controles según los riesgos.

Fases de implementación de un SGSI

Fase	Explicación
1. Diagnóstico inicial	Analizar la situación actual (brechas frente a ISO 27001).
2. Alcance y política	Definir los límites del SGSI y la política general de seguridad.
3. Análisis de riesgos	Identificar activos, amenazas, vulnerabilidades, impactos y probabilidad.
4. Tratamiento de riesgos	Seleccionar controles del Anexo A u otros que mitiguen riesgos.
5. Implementación	Poner en marcha controles y procedimientos.
6. Monitoreo y medición	Revisar efectividad (auditorías, indicadores).
7. Mejora continua	Corregir, ajustar y fortalecer el SGSI.

Fases de implementación de un SGSI

Fase 1. Diagnóstico inicial

¿Qué es?

Evaluar la situación actual de la organización respecto a la seguridad de la información.

Objetivo:

Identificar brechas frente a los requisitos de la norma ISO 27001 y las prácticas actuales de seguridad.

Ejemplo práctico

Una clínica desea implementar ISO 27001. Descubre que:

- No tiene política de seguridad formal.
- No realiza backups fuera del edificio.
- Los usuarios usan la misma contraseña para todo.

Fase 1. Diagnóstico inicial

Ejercicio práctico

Instrucción: Haz un diagnóstico inicial individual sobre tu universidad o trabajo:

- ¿Existen políticas de seguridad?
- ¿Qué controles de seguridad física y lógica reconoces?
- ¿Cuáles crees que son sus principales debilidades?

Formato sugerido – Diagnóstico inicial

Área evaluada	Situación actual	Brecha identificada	Acción recomendada
Ej. Backups	Backups diarios en disco local	No existen copias externas o en nube	Implementar backups en nube semanalmente

Área evaluada	Situación actual	Brecha identificada	Acción recomendada
Políticas de seguridad	Existen políticas de uso aceptable y de protección de datos (Habeas Data).	Bajo conocimiento por parte de estudiantes y personal.	Realizar campañas de socialización y capacitaciones periódicas.
Seguridad física	Acceso con carnet, cámaras de videovigilancia, guardias en turnos.	Algunos laboratorios y oficinas quedan sin supervisión en ciertos horarios.	Implementar rondas de seguridad adicionales y control de acceso más estricto.
Seguridad lógica (TI)	Acceso con usuario/contraseña y antivirus en equipos institucionales.	Contraseñas débiles y ausencia de doble factor de autenticación.	Establecer políticas de contraseñas fuertes y habilitar autenticación multifactor.
Gestión de incidentes	No existe un canal claro de reporte de incidentes de seguridad.	Incidentes (phishing, malware) pueden pasar desapercibidos o sin atención adecuada.	Crear un buzón o sistema de tickets para reportar incidentes y designar responsables.
Concienciación del usuario	Algunos usuarios instalan software sin autorización o comparten contraseñas.	Riesgo de malware y fuga de información.	Realizar talleres de ciberseguridad y controles técnicos que restrinjan instalaciones.

Fases de implementación de un SGSI

Fase 2. Definición del alcance y política

¿Qué es?

- **Alcance:** procesos, departamentos, sistemas y ubicaciones cubiertas por el SGSI.
- **Política:** declaración de la alta dirección sobre su compromiso con la seguridad de la información.

Ejemplo práctico

- **Alcance:** "SGSI para el procesamiento, almacenamiento y transmisión de información de pacientes en la sede principal."
- **Política (resumen):** "La Clínica Salud Segura declara su compromiso de proteger la información de pacientes y empleados, cumpliendo la ley y mejorando continuamente su SGSI."

Fase 2. Definición del alcance y política

Ejercicio práctico

Redacta una política corta de seguridad de la información para tu emprendimiento o proyecto académico, incluyendo:

- Propósito
- Alcance
- Compromiso general

Formato sugerido – Política de seguridad

Elemento	Contenido
Propósito	¿Por qué existe esta política?
Alcance	¿A quiénes y qué procesos aplica?
Compromiso	Declaración de alta dirección sobre seguridad y mejora continua.

Política corta de seguridad de la información – Empresa de Biotecnología

Elemento	Contenido
Propósito	Proteger la confidencialidad, integridad y disponibilidad de la información generada en procesos de investigación, desarrollo de bioproductos y gestión de datos de laboratorio, garantizando el cumplimiento normativo (ISO 27001, Habeas Data, GDPR) y la confianza de clientes y aliados.
Alcance	Aplica a todos los empleados, investigadores, contratistas y estudiantes vinculados al emprendimiento, así como a los procesos de gestión de datos experimentales, propiedad intelectual, información de pacientes en proyectos clínicos y sistemas de TI utilizados en la operación.
Compromiso	La alta dirección se compromete a establecer, mantener y mejorar continuamente un Sistema de Gestión de Seguridad de la Información (SGSI), asignando los recursos necesarios para implementar controles adecuados, cumplir con la normativa vigente, y fomentar la cultura de seguridad entre todos los colaboradores.

Fases de implementación de un SGSI

Fase 3. Análisis y evaluación de riesgos

¿Qué es?: Identificar, evaluar y priorizar los riesgos que pueden afectar los activos de información.
Objetivo: Decidir qué riesgos son aceptables y cuáles necesitan tratamiento.

Ejemplo práctico
Activo: Historias clínicas digitales
Amenaza: Ransomware
Vulnerabilidad: Usuarios sin capacitación, no hay backups externos
Impacto: Muy alto
Probabilidad: Media
Riesgo: Alto
Tratamiento: Implementar backups en nube, capacitación en phishing, antivirus actualizado.

Ejercicio práctico
Realiza un análisis de riesgos de tu dispositivo móvil:
1. Identifica un activo (fotos, documentos, apps bancarias).
2. Menciona una amenaza.
3. Determina vulnerabilidad, impacto y probabilidad.
4. Propón un control.

Formato sugerido – Análisis de riesgos

Activo	Amenaza	Vulnerabilidad	Impacto	Probabilidad	Nivel de riesgo	Control propuesto

Fases de implementación de un SGSI

Fase 4. Tratamiento de riesgos

¿Qué es?: Elegir e implementar controles para reducir riesgos a niveles aceptables.
Opciones de tratamiento (ISO 27001):

- Evitar el riesgo
- Reducirlo con controles
- Transferirlo (ej. seguros)
- Aceptarlo

Ejemplo práctico

- **Riesgo:** Filtración de contraseñas
- **Control:** Implementar MFA (autenticación multifactor)

Ejercicio práctico

Selecciona un control para cada amenaza identificada en el ejercicio anterior. Justifica por qué es la mejor opción.

Formato sugerido – Plan de tratamiento de riesgos

Riesgo	Control seleccionado	Responsable	Fecha estimada de implementación

Fases de implementación de un SGSI

Fase 5. Implementación

¿Qué es?: Poner en práctica los controles, políticas y procedimientos definidos.
Incluye:

- Capacitación a usuarios
- Configuración de sistemas
- Creación de procedimientos escritos

Ejemplo práctico
Implementar backups automáticos en nube, configurar MFA en correos corporativos y realizar inducción de seguridad digital a los empleados.

Ejercicio práctico
Diseña un plan de implementación breve para los controles propuestos en tu análisis anterior.

Formato sugerido – Plan de implementación

Control	Actividades	Responsable	Recursos requeridos	Fecha estimada

Fases de implementación de un SGSI

Fase 6. Monitoreo y medición

¿Qué es?: Evaluar si los controles implementados son efectivos y cumplen los objetivos de seguridad.

Incluye:

- Auditorías internas
- Indicadores de desempeño (KPIs)
- Revisión de incidentes y hallazgos

Ejemplo práctico

- Auditoría anual del SGSI
- Revisión mensual de logs de acceso
- Indicador: % de usuarios capacitados en phishing

Fase 6. Monitoreo y medición

Ejercicio práctico

Propón dos indicadores para monitorear la efectividad de un SGSI en una empresa de servicios en línea.

Indicador	Meta	Frecuencia de medición	Responsable

Indicador	Fórmula	Meta	Frecuencia de medición	Responsable
Tasa de incidentes de seguridad reportados	(N° de incidentes de seguridad detectados en el periodo / N° total de usuarios o servicios) × 100	< 1% de incidentes por cada 1.000 usuarios	Mensual	Oficial de Seguridad de la Información (CISO)
Cumplimiento en actualizaciones de seguridad	(N° de sistemas actualizados con parches críticos / N° total de sistemas identificados) × 100	≥ 95% de sistemas parchados en ≤ 30 días	Trimestral	Equipo de TI / Seguridad
Nivel de capacitación en seguridad del personal	(N° de empleados capacitados / N° total de empleados) × 100	100% del personal capacitado al menos 1 vez al año	Semestral	Recursos Humanos + Seguridad de la Información
Disponibilidad de servicios críticos	(Tiempo total de disponibilidad / Tiempo total del periodo) × 100	≥ 99,5% de disponibilidad	Mensual	Equipo de Infraestructura / Operaciones

Disponibilidad de servicios críticos

Calcule la disponibilidad porcentual del servicio de aplicación web de un banco si estuvo fuera de servicio 30 horas durante los meses de mayo, junio y julio y la frecuencia de medición es trimestral. Y definir si estamos cumpliendo con el 99,95 % de disponibilidad.

$$\%\text{Disponibilidad} = (\text{Tiempo total de disponibilidad} / \text{Tiempo total del periodo}) \times 100$$

$$3\ meses = 90 * 24 = 2160$$

$$No\ disponible = 30 \rightarrow \text{Tiempo total de disponibilidad} = 2160 - 30 = 2130$$

$$\%\text{Disponibilidad} = (2130 / 2160) \times 100 = 98{,}61\%$$

$$3\ meses = 92 * 24 = 2208$$

$$No\ disponible = 30 \rightarrow \text{Tiempo total de disponibilidad} = 2208 - 30 = 2178$$

$$\%\text{Disponibilidad} = (2178 / 2208) \times 100 = 98{,}64\%$$

Fases de implementación de un SGSI

Fase 7. Mejora continua

¿Qué es?: Actualizar y fortalecer el SGSI a partir de hallazgos, incidentes, auditorías y cambios en el entorno.

Ejemplo práctico
Después de un simulacro de phishing donde 40% de usuarios cayeron, la empresa:

- Actualiza su capacitación con ejemplos más realistas
- Implementa simulaciones trimestrales

Fase 7. Mejora continua

Ejercicio práctico

Propón una mejora continua para tu seguridad digital personal.

Formato sugerido – Plan de mejora

Hallazgo	Acción de mejora	Responsable	Fecha límite

Fase 7. Mejora continua

Hallazgo	Acción de mejora	Responsable	Fecha límite
Uso de contraseñas débiles y repetidas	Implementar un gestor de contraseñas y activar la autenticación multifactor (MFA) en todas las cuentas críticas	Usuario	1 mes
Dispositivos sin actualizaciones automáticas	Configurar actualizaciones automáticas en laptop y smartphone para sistema operativo y aplicaciones	Usuario	2 semanas
Copias de seguridad irregulares	Establecer un plan de respaldo mensual en la nube cifrada y en un disco externo	Usuario	1 mes
Uso frecuente de redes WiFi públicas sin protección	Utilizar una VPN confiable en conexiones públicas y evitar el acceso a información sensible en estas redes	Usuario	Inmediato

¿Qué es el ciclo PHVA (PDCA)?

El ciclo **PHVA (Planificar – Hacer – Verificar – Actuar)**, conocido internacionalmente como **PDCA (Plan – Do – Check – Act)**, es un modelo de gestión de calidad y mejora continua desarrollado por **Walter Shewhart** y popularizado por **W. Edwards Deming.**

Es un enfoque **iterativo y sistemático** que permite a las organizaciones planear, implementar, evaluar y mejorar procesos y sistemas de gestión, incluyendo el **Sistema de Gestión de Seguridad de la Información (SGSI) de ISO/IEC 27001:2022.**

Fases del ciclo PHVA

Fase	Explicación práctica	Ejemplo aplicado a ISO 27001
P – Planificar	Definir objetivos, procesos, recursos y controles necesarios para obtener resultados de acuerdo con la política de seguridad de la información y los requisitos legales y contractuales.	Realizar análisis de riesgos, definir la política de seguridad, establecer objetivos y planes de tratamiento de riesgos.
H – Hacer	Implementar los procesos y controles definidos en la fase de planificación.	Implementar políticas, controles técnicos (MFA, backups) y capacitar usuarios en seguridad.
V – Verificar	Monitorear, medir y evaluar el desempeño de los procesos y controles frente a la política, objetivos y requisitos establecidos.	Realizar auditorías internas, revisar indicadores de desempeño y analizar incidentes de seguridad.
A – Actuar	Tomar acciones para mejorar continuamente el desempeño del SGSI, corrigiendo desviaciones y fortaleciendo procesos.	Actualizar políticas y controles según hallazgos de auditoría, nuevos riesgos o cambios en la organización.

Ejemplo práctico completo en un SGSI

Contexto: Universidad implementa ISO 27001 para proteger datos de estudiantes y docentes.

Planificar (P):

- Define su política de seguridad.
- Realiza análisis de riesgos.
- Establece como objetivo reducir incidentes de phishing en un 80%.

Hacer (H):

- Implementa capacitación en phishing para docentes y administrativos.
- Configura filtros antiphishing en el servidor de correo.
- Aplica MFA en plataforma académica.

Verificar (V):

- Realiza simulaciones de phishing.
- Mide cuántos usuarios caen en los correos simulados.
- Audita la efectividad de los filtros de correo.

Actuar (A):

- Ajusta el contenido de la capacitación para temas donde los usuarios fallaron más.
- Configura reglas adicionales en el servidor de correo para bloquear remitentes falsos.
- Actualiza la política de seguridad con nuevos requisitos.

Importancia del PHVA en ISO/IEC 27001:2022

- **Base del SGSI:** ISO 27001 se construye sobre el ciclo PHVA para garantizar la mejora continua, uno de los principios de todos los sistemas de gestión de la familia ISO.
- **Prevención de riesgos:** Permite no solo responder ante incidentes, sino anticiparse a ellos mediante la revisión y ajuste constante.
- **Evidencia de compromiso:** Demuestra en auditorías que la organización planifica, implementa, revisa y mejora sus procesos, evitando la gestión reactiva y promoviendo una cultura de seguridad.

Checklist de requisitos para la certificación

Requisito ISO 27001	Descripción	Evidencia esperada
Política de Seguridad	Documento aprobado y comunicado a toda la organización	Política firmada y difundida
Alcance del SGSI	Definición clara de qué activos, procesos y áreas cubre	Documento de alcance
Gestión de riesgos	Identificación, análisis y tratamiento de riesgos	Matriz de riesgos actualizada
Roles y responsabilidades	Definidos y comunicados (ej. Oficial de Seguridad)	Organigrama y asignación de funciones
Auditorías internas	Evaluaciones periódicas del SGSI	Reportes de auditoría

Checklist de requisitos para la certificación

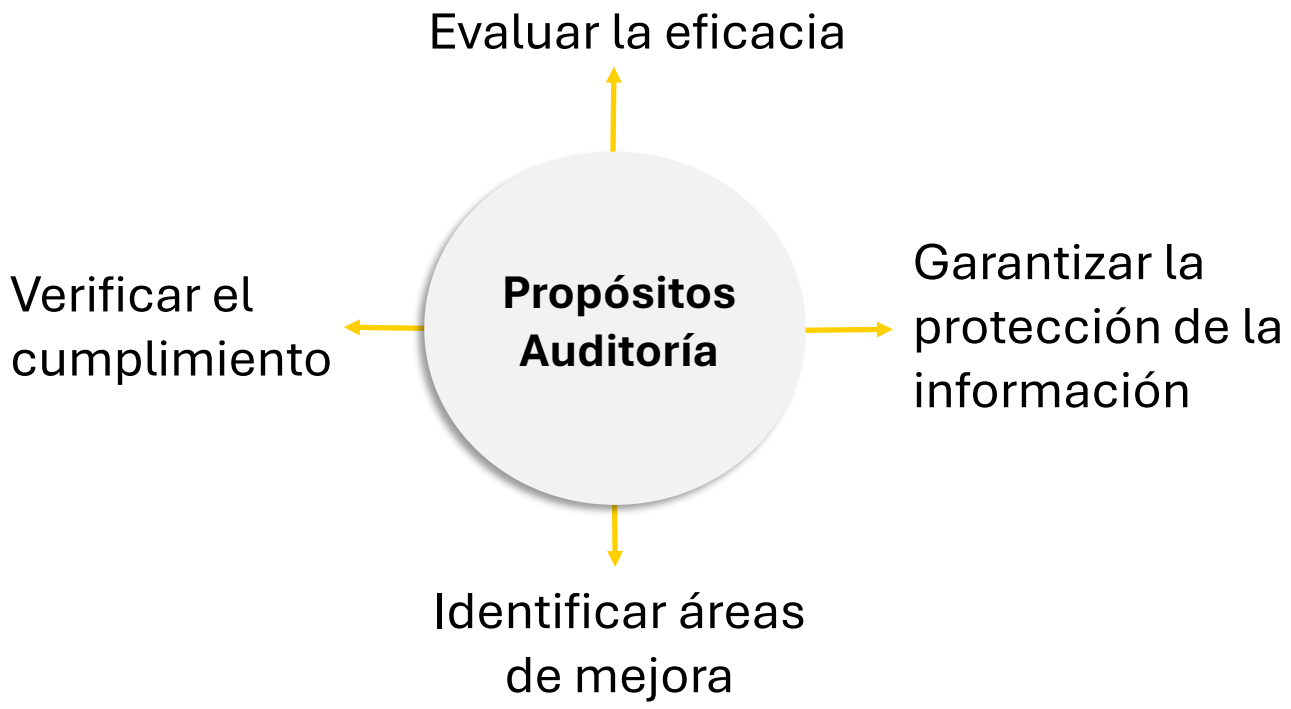
Requisito ISO 27001	Descripción	Evidencia esperada
Controles implementados	Aplicar los controles del Anexo A según riesgos	Políticas, procedimientos, configuraciones
Capacitación y concientización	Programas de formación continua para empleados	Listas de asistencia, materiales de capacitación
Gestión de incidentes	Procedimiento para detectar, responder y aprender	Registro de incidentes
Mejora continua (PHVA)	Ciclo Planear–Hacer–Verificar–Actuar aplicado	Actas de revisión, planes de mejora
Cumplimiento legal	Cumplir GDPR, Habeas Data, leyes locales	Matriz de cumplimiento legal

https://www.british-assessment.co.uk/app/uploads/2023/04/ISO-27001-2022-Checklist-Updated.pdf

Qué es una auditoría ISO 27001?

Una auditoría ISO 27001 es una evaluación sistemática del Sistema de Gestión de Seguridad de la Información (SGSI) de una organización para determinar si cumple con los requisitos de la norma ISO 27001 y si es eficaz para proteger la información.

Este proceso identifica riesgos, no conformidades y oportunidades de mejora, ayudando a la organización a fortalecer su postura de seguridad, reducir costos y garantizar la confidencialidad, integridad y disponibilidad de sus datos.



Auditoría Clínica

Imagina que estás auditando una clínica que quiere certificarse en ISO 27001. Como auditor, revisas documentos, entrevistas a personal y observas prácticas. Encuentras lo siguiente:

- La clínica guarda historias clínicas electrónicas en un servidor local.
- El acceso se hace con usuario y contraseña (pero sin MFA).
- Se hacen copias de seguridad, pero se almacenan en el mismo servidor.
- No existe un registro formal de incidentes de seguridad.
- Hay una política de seguridad, pero no todos los empleados la conocen.

Requisito ISO 27001	Cumple (Sí/No/Parcial)	Evidencia encontrada	Observación
Existe política de seguridad de la información aprobada por la dirección	Sí	Documento firmado 2023	No hay divulgación suficiente
Control de accesos implementado (autenticación robusta)	Parcial	Solo usuario/contraseña	No hay MFA ni gestión de privilegios
Respaldo de la información crítica y almacenamiento seguro	No	Backups en mismo servidor	Crítico: riesgo de pérdida total
Registro y gestión de incidentes de seguridad	No	No se encontraron registros	Implementar sistema de tickets
Concienciación y capacitación en seguridad a empleados	Parcial	Capacitaciones esporádicas	Requiere programa anual documentado

Actividad: Universidad Privada

Imagina que estás auditando una universidad que quiere certificarse en ISO 27001. Como auditor, revisas documentos, entrevistas a personal y observas prácticas. Encuentras lo siguiente:

- La universidad maneja datos personales de estudiantes (nombres, direcciones, notas, información financiera).
- Se detectó que algunos profesores guardan información de bases de datos institucionales en sus laptops personales sin cifrado.
- No hay política clara de control de dispositivos personales.
- La red Wi-Fi institucional no tiene segmentación (estudiantes y administrativos en la misma red).
- El comité directivo firmó la política de seguridad, no hay socialización y no existen auditorías internas previas.
- Solo se realizaron talleres de Seguridad de la Información en 2022

Realiza:

- Marca en el checklist los controles que cumpla o no.
- Define el hallazgo más crítico, por que lo consideras así.
- Propón una acción correctiva.

Requisito ISO 27001	Cumple	Evidencia encontrada	Observación

Requisito ISO 27001	Cumple	Evidencia encontrada	Observación
Política de seguridad aprobada y comunicada	Parcial	Documento firmado, no difundido	Debe socializarse con estudiantes y docentes
Control de dispositivos personales (BYOD)	No	Profesores usan laptops sin cifrar	Riesgo crítico de fuga de datos
Segmentación de red	No	Una sola red para todos	Exposición innecesaria, riesgo de intrusión
Gestión de datos sensibles (notas, finanzas, salud)	Parcial	Bases de datos protegidas, pero copias locales sin cifrar	Riesgo medio-alto
Auditoría interna regular del SGSI	No	No se han hecho auditorías	Obligatoria para certificación
Capacitación a docentes y administrativos	Parcial	Talleres en 2022, no recurrentes	Requiere capacitaciones anuales

Hallazgos críticos

- Uso de laptops personales sin cifrado: riesgo de pérdida/fuga de datos sensibles
- Falta de segmentación en red Wi-Fi: exposición de sistemas administrativos.
- No hay auditorías internas: incumplimiento de ISO 27001.

Acciones correctivas

- Cifrado obligatorio de dispositivos personales que manejen información institucional.
- Segmentar la red Wi-Fi en al menos dos redes: estudiantes y administrativos.
- Implementar una política BYOD clara (qué se puede almacenar, medidas de seguridad, monitoreo).
- Crear un plan de auditorías internas semestrales del SGSI.
- Capacitación continua a personal y profesores sobre seguridad y protección de datos.

FORO Semana 4

¿Cuál consideras que es el principal beneficio para una organización al implementar ISO 27001?

¿Qué cláusula te pareció más importante y por qué?

FORO Semana 4

Reducción de riesgos

Permite identificar y mitigar amenazas antes de que se materialicen.

Confianza de los clientes

ISO 27001 demuestra compromiso con la seguridad, lo que fortalece la reputación y atrae nuevos clientes.

¿Cuál consideras que es el principal beneficio para una organización al implementar ISO 27001?

Cumplimiento normativo

Ayuda a cumplir con GDPR, Habeas Data o normativas locales.

Eficiencia operativa

El SGSI estandariza procesos y roles, evitando improvisaciones.

FORO Semana 4

¿Qué cláusula te pareció más importante y por qué?

Cláusula 6: Planificación (gestión de riesgos)
Sin gestión de riesgos no se sabe qué proteger ni cómo priorizar.

Cláusula 9: Evaluación del desempeño
Permite medir si el SGSI realmente funciona.

Cláusula 5: Liderazgo
El compromiso de la alta dirección garantiza recursos y cumplimiento.

Cláusula 8: Operación
Gestionar riesgos e implementar controles en la práctica.

Cláusulas principales (requisitos)

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 continua

Referencias

1. Bishop, M. (2003). *Computer Security.*
2. Briceño, E. (2021). *Seguridad De La Información*
3. Kremer, E. Et al. (2019). *Ciberseguridad*
4. Ozkaya, E. (2019). *Cybersecurity: The Beginner's Guide: A comprehensive guide to getting started in cybersecurity*
5. *NORMA TÉCNICA NTC-ISO-IEC COLOMBIANA 27001*
6. *General Data Protection Regulation (GDPR)*
7. LEY ESTATUTARIA 1581 DE 2012. *Link: https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=49981*
8. British-assessment. *(2022). ISO/IEC 27001:2022 Checklist. https://www.british-assessment.co.uk/app/uploads/2023/04/ISO-27001-2022-Checklist-Updated.pdf*
9. SmartSheet. (2022). *Plantillas y listas de verificación gratuitas de la ISO 27001. https://es.smartsheet.com/content/iso-27001-checklist-templates?fl_redir=1*