




Fundamentos de un SGSI II

8 Fases de Implementación del SGSI

- 4.-Implementar controles de seguridad:
 - Aplicar las medidas necesarias para mitigar los riesgos identificados, basándose en las mejores prácticas y normativas aplicables.
 - ISO 27002: <https://es.isms.online/iso-27002/>
 - ENS <https://www.ccn-cert.cni.es/es/informes.html>



Centro
Criptológico
Nacional

CCN-CERT

INCIDENTES

RNS

GUÍAS

INFORMES

FORMACIÓN

SOLUCIONES

ENS

SEGURIDAD AL DÍA

COMUNICACIÓN

REGISTRO





















documentos elaborados por el grupo de expertos del CCN-CERT con distinta temática y complejidad para ofrecer una visión actualizada del estado de la ciberseguridad. Nos encontramos con cuatro tipologías:

- Abstracts:** información relevante y condensada sobre tecnologías o procedimientos seguros
- Amenazas:** estudios sobre las distintas ciberamenazas y sus características en un período de tiempo
- Buenas Prácticas:** conjunto de acciones y consejos sobre las acciones más comunes en materia de ciberseguridad
- Código Dañino:** análisis pormenorizado de un malware o familia de malware.

Total: 403 documentos

Mostrar: 20

Pág. 1 de 10

Documento	Categoría	Publicado desde	Actualizado desde
 CCN-CERT BP/22 Recomendaciones de seguridad para Oracle Database 19C 	Buenas Prácticas	May 2022	May 2024
 CCN-CERT BP/22 Security recommendations for Oracle Database 19C 	Buenas Prácticas	May 2022	May 2024
 CCN-CERT BP/22 Recommandations de sécurité pour la base de données Oracle 19C 	Buenas Prácticas	May 2022	May 2024
 CCN-CERT BP/23 Security recommendations for DB2 databases 	Buenas Prácticas	Oct 2021	May 2024
 CCN-CERT BP/24 Recomendaciones de seguridad en bases de datos 	Buenas Prácticas	Dic 2021	May 2024
 CCN-CERT BP/26 Recommandations de sécurité pour Microsoft Edge 	Buenas Prácticas	Jun 2022	May 2024
 CCN-CERT BP/31 Recomendaciones de Protección del Dato en la Nube: Soberanía Digital 	Buenas Prácticas	May 2024	May 2024
 CCN-CERT BP/32 MacOS Operating System Security Recommendations 	Buenas Prácticas	May 2024	May 2024
 CCN-CERT BP/27 Recomendaciones de seguridad en Kubernetes 	Buenas Prácticas	Sep 2022	May 2024
 CCN-CERT BP/27 Recommandations de sécurité de Kubernetes 	Buenas Prácticas	Sep 2022	May 2024

Controles

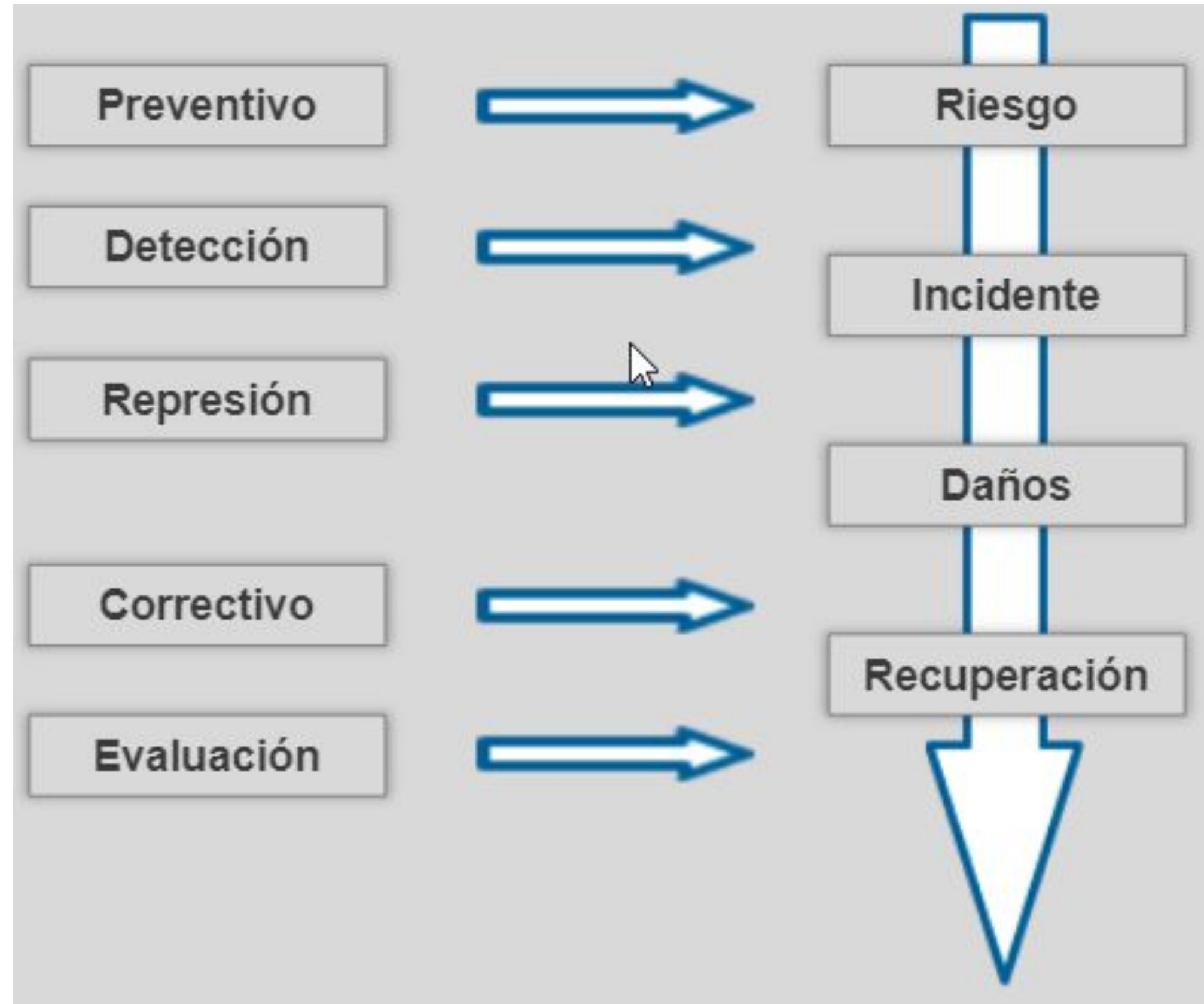
Cláusula 6.1.3 b) c) ISO 27001

- Los objetivos de control y los controles del anexo A deben seleccionarse (o aplicar) como parte de este proceso en la medida en que sirvan para satisfacer los requisitos identificados.
 - Está claro que se deben haber identificado anteriormente TODOS los requisitos de seguridad: normas internas, riesgos a gestionar y obligaciones legales a cumplir.
 - Para algunas organizaciones, la lista del Anexo A puede ser insuficiente, y se recomienda añadir un catálogo adicional de controles: COBIT, ISO 2701x (catálogo sectorial)...

- Factores y restricciones de aplicabilidad:
 - Coste del control. Coste de seguridad versus coste de inseguridad.
 - Disponibilidad del control. Tecnología existente y probada.
 - Implementación y mantenimiento.
 - Controles existentes y planificados.

Categorización de los Controles

- Las medidas de seguridad se categorizan en diferentes etapas desde el potencial de un incidente de seguridad hasta la vuelta a la normalidad.
- Preventivo**, medidas diseñadas para evitar que ocurra un incidente de seguridad. Esto debemos pensarlo antes como posibilidad de que ocurra un incidente.
 - Detección**: Medidas que permiten identificar y detectar incidentes de seguridad cuando ocurren. Servirá en el momento de que tengamos el incidente.
 - Represión**: Acciones tomadas para detener o minimizar el impacto de un incidente en curso. Cuando pensemos que hay algún daño o consecuencia negativa de un incidente.
 - Correctivo**: Son las medidas para corregir los efectos de un incidente y restaurar los sistemas a su estado normal.
 - Evaluación**: Proceso de revisión y análisis post-incidente para evaluar la efectividad de las medidas de seguridad y mejorar futuras respuestas. Este ocurre luego del proceso de restaurar los sistemas y operaciones a su estado normal.



ESTRUCTURA DE LA ISO 27002:2013

- Introducción.
- Cláusula 0: Alcance.
- Cláusula 1: Referencias normativas.
- Cláusula 2: Términos y definiciones.
- Cláusula 3: Estructura de controles.
- Dominios y Controles de Seguridad (Cláusula 4 a 18)
 - Cláusula 4: Contexto organizacional.
 - Cláusula 5: Seguridad de los recursos humanos.
 - Cláusula 6: Gestión de activos.
 - Cláusula 7: Control de acceso.
 - Cláusula 8: Criptografía.
 - Cláusula 9: Seguridad física y ambiental.
 - Cláusula 10: Seguridad en las operaciones.
 - Cláusula 11: Seguridad en las comunicaciones.
 - Cláusula 12: Adquisición, desarrollo y mantenimiento de Sistemas.
 - Cláusula 13: Relación con proveedores.
 - Cláusula 14: Gestión de incidentes de seguridad de la información.
 - Cláusula 15: Continuidad del negocio.
 - Cláusula 16: Cumplimiento

CONTENIDOS DE LA 27002

Actualmente la norma ISO/IEC ISO 27002 es la **mejor “práctica” en uso**, a nivel mundial y referenciada en muchos estándares.

Nos ofrece las siguientes ventajas:

- > **Cobertura consistente** de todos los aspectos de la seguridad.
- > Enfoque a la **prevención** y a la rapidez de respuesta.
- > **Marco de referencia** para estimar el grado de seguridad.
- > **Catálogo mínimo y guía de implantación** de los controles de seguridad para los sistemas de gestión de seguridad certificables: ISO 27001.
- > **Consistencia** con otras normas ISO, y también entre controles de seguridad.

Su **contenido** nos ofrece:

- > Una introducción a los conceptos de gestión de la seguridad (del Apartado 0 al apartado 4).
- > Una definición de 35 objetivos de seguridad [de los apartados de segundo nivel (5.1 al 15.2)].
- > Un catálogo de 114 controles de seguridad (de los números 5.1.1 al 18.2.3).
 - Con especificaciones, guía de implantación y referencias.
 - Cubren aspectos de gestión, aspectos tecnológicos y aspectos jurídicos de la seguridad de la información.

Nueva versión de la ISO 27002:2022

- Un cambio radical con respecto a la versión anterior es la reestructuración de los 14 dominios de controles definidos en ISO 27002:2013 en torno a 4 grandes temas:
 - **Controles Organizacionales (37 controles)**
 - Trata sobre cómo la organización aborda la seguridad de los datos, desde las políticas y procesos que implementa hasta la estructura de su empresa.
 - ¿Tiene su organización un conjunto claro de políticas sobre cómo mantener seguro su SGSI? ¿Están claramente definidas y comunicadas de manera efectiva las funciones y responsabilidades de la seguridad de la información? ¿Están implementados los controles de acceso adecuados?
 - **Controles de Personas (8 controles)**
 - Definen cómo su personal interactúa con los datos y los sistemas de información. Incluyen prácticas como verificaciones de antecedentes de empleados y capacitación en concienciación sobre seguridad.
 - **Controles Físicos (14 controles)**
 - ¿Cómo protegerá los activos de información física? Estos controles incluyen políticas de escritorio limpio, protocolos de almacenamiento y eliminación, sistemas de entrada y acceso, y más.
 - **Controles Tecnológicos (34 controles)**
 - Los controles tecnológicos tratan de mantener una infraestructura de TI segura y en conformidad. Estos controles cubren una variedad de problemas, desde quién puede acceder al código fuente y cómo mantener la seguridad de la red hasta la sincronización de relojes.



DECLARACIÓN DE APLICABILIDAD - SOA

- La “**Declaración de Aplicabilidad**” (**SOA**, por sus siglas en inglés) es un documento clave en la gestión de la seguridad de la información. Este documento detalla los controles de seguridad que una organización ha seleccionado para mitigar los riesgos identificados en su análisis de riesgos.
- Redactar una Declaración de Aplicabilidad (SOA) para ISO 27001 implica varios pasos clave.
- Aquí te dejo una guía básica para ayudarte a empezar:
 - **Identificación y Análisis de Riesgos.**
 - **Definición del Plan de Tratamiento de Riesgos.**
 - **Selección de Controles de Seguridad.**
 - **Documentación de los Controles**
 - **Controles seleccionados**
 - **Controles no seleccionados.**
 - **Redacción del Documento:**
 - **Introducción.**
 - **Alcance.**
 - **Controles seleccionados y no seleccionados.**
 - **Estado de Implementación**
 - **Revisión y Actualización.**
 - **Confidencialidad.**

Ejemplo de SOA

Declaración de Aplicabilidad (SOA)

Organización: XYZ Corp
Fecha: 09 de octubre de 2024
Versión: 1.0

Introducción

La presente Declaración de Aplicabilidad (SOA) detalla los controles de seguridad seleccionados por XYZ Corp para mitigar los riesgos identificados en nuestro análisis de riesgos, conforme a la norma ISO/IEC 27001.

Alcance

El alcance del Sistema de Gestión de Seguridad de la Información (SGSI) de XYZ Corp incluye todos los procesos relacionados con el desarrollo, mantenimiento y soporte de nuestros productos de software.

Controles Seleccionados y No Seleccionados

Control	Descripción	Estado	Justificación
A.5.1.1	Políticas para la seguridad de la información	Implementado	Necesario para establecer directrices claras de seguridad.
A.6.1.2	Organización de la seguridad de la información	Implementado	Asegura la asignación de responsabilidades de seguridad.
A.8.1.1	Responsabilidad de los activos	Implementado	Protege los activos de información críticos.
A.9.2.3	Gestión de acceso de usuarios	En proceso	Controla el acceso a la información sensible.
A.12.6.1	Gestión de vulnerabilidades técnicas	No implementado	No aplicable debido a la naturaleza de nuestros sistemas.

Estado de Implementación

- Implementado:** Los controles han sido completamente implementados y están operativos.
- En proceso:** Los controles están en fase de implementación y se espera que estén operativos en los próximos meses.
- No implementado:** Los controles no se han implementado debido a su no aplicabilidad o a la baja prioridad de riesgo.

Revisión y Actualización

Esta SOA será revisada y actualizada anualmente o cuando se produzcan cambios significativos en el entorno de riesgos de la organización.

8 Fases de Implementación del SGSI

• 5.-Capacitar al personal:

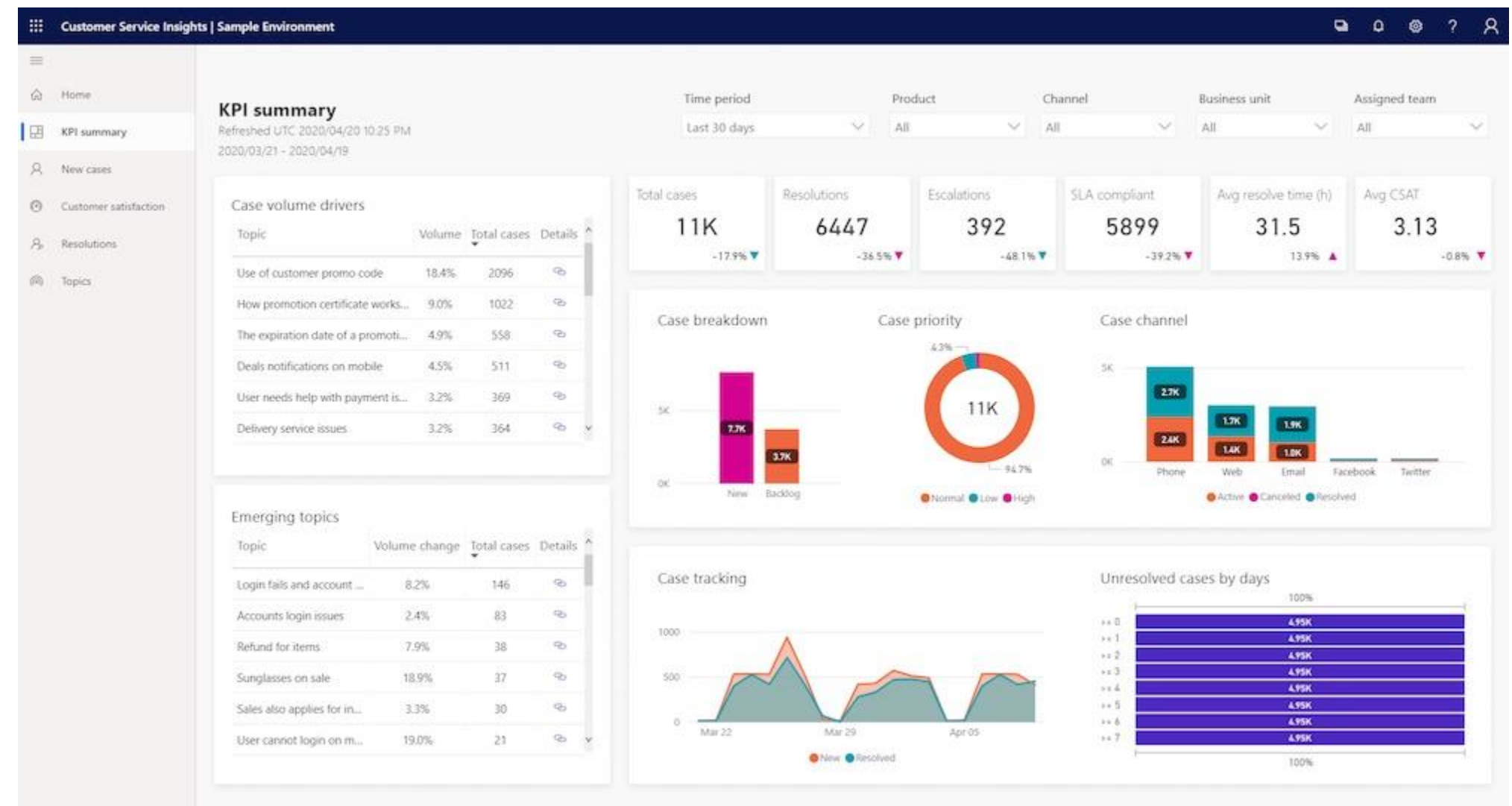
- Asegurar que todos los empleados comprendan sus roles y responsabilidades en relación con la seguridad de la información.
- Brindar capacitación a todo el personal sobre las políticas y procedimientos de seguridad de la información.
- Cuando se implementan las nuevas medidas de protección, al mismo tiempo se deben planificar las sesiones de capacitación y concienciación.
- Promover una cultura de seguridad informática mediante campañas de concientización y sensibilización.
- No es suficiente hacer una solo sesión de capacitación y concienciación. Ya que se incorporan nuevo personal a la organización, los que ya estaban se olvidarán de lo que escucharon, las medidas de protección cambiarán, etc. Es un **proceso continuo**.



8 Fases de Implementación del SGSI

6.-Monitorear y revisar:

- Evaluar continuamente el **SGSI** para identificar áreas de mejora y garantizar que los controles implementados sean efectivos.
- Implementación de indicadores (**KPI**) como, por ejemplo:
 - Dispositivos conectados e Histórico
 - Dispositivos no identificados en redes internas
 - Intentos de Intrusión a la organización.
 - Incidentes de Ciberseguridad.
 - Tiempo medio de detección, contención y de resolución de un ciber incidente.
 - Calificación promedio de seguridad del proveedor.
 - Histórico del parcheo de la plataforma.
 - Gestión de Accesos.
 - Cumplimiento de los controles.



Evaluación Diferencial

- Es una técnica utilizada en la toma de decisiones para comparar los beneficios y/o costos asociados a diferentes opciones.
- Consiste en analizar y comparar 2 situaciones:
 - **Situación inicial o actual o de partida**
 - **Situación deseada**
- Esto es de conformidad con los controles **ISO 27001 (apartado 4 a 10)** y de la **ISO 27002 (anexo A ISO 27001)**
- Algunos ejemplos son:
 - **Escala de 3 Estado.**
 - No aplica
 - No Implementado
 - Implementado
 - **CMM (Modelo de Capacidad y Madurez).**
 - Inexistente
 - Inicial (Initial)
 - Repetible pero intuitivo (Managed)
 - Proceso definido (Defined)
 - Gestionado y Evaluable (Quantitatively Managed)
 - Optimizado (Optimizing)



8 Fases de Implementación del SGSI

- **7.-Realizar auditorías internas:**

- Llevar a cabo auditorías periódicas para verificar el cumplimiento del SGSI con las políticas establecidas y las normativas vigentes.

- **Pasos Clave en una Auditoría SGSI**

- **Planificación:** Definir el alcance y los objetivos de la auditoría, así como el equipo auditor.
- **Revisión Documental:** Evaluar la documentación del SGSI, incluyendo políticas, procedimientos y registros.
- **Evaluación de Riesgos:** Revisar el análisis y la gestión de riesgos para asegurar que se han identificado y mitigado adecuadamente.
- **Verificación de Controles:** Comprobar que los controles de seguridad están implementados y son efectivos.
- **Entrevistas y Observaciones:** Realizar entrevistas con el personal y observar las prácticas diarias para verificar la implementación del SGSI.
- **Informe de Auditoría:** Documentar los hallazgos, incluyendo no conformidades y oportunidades de mejora.

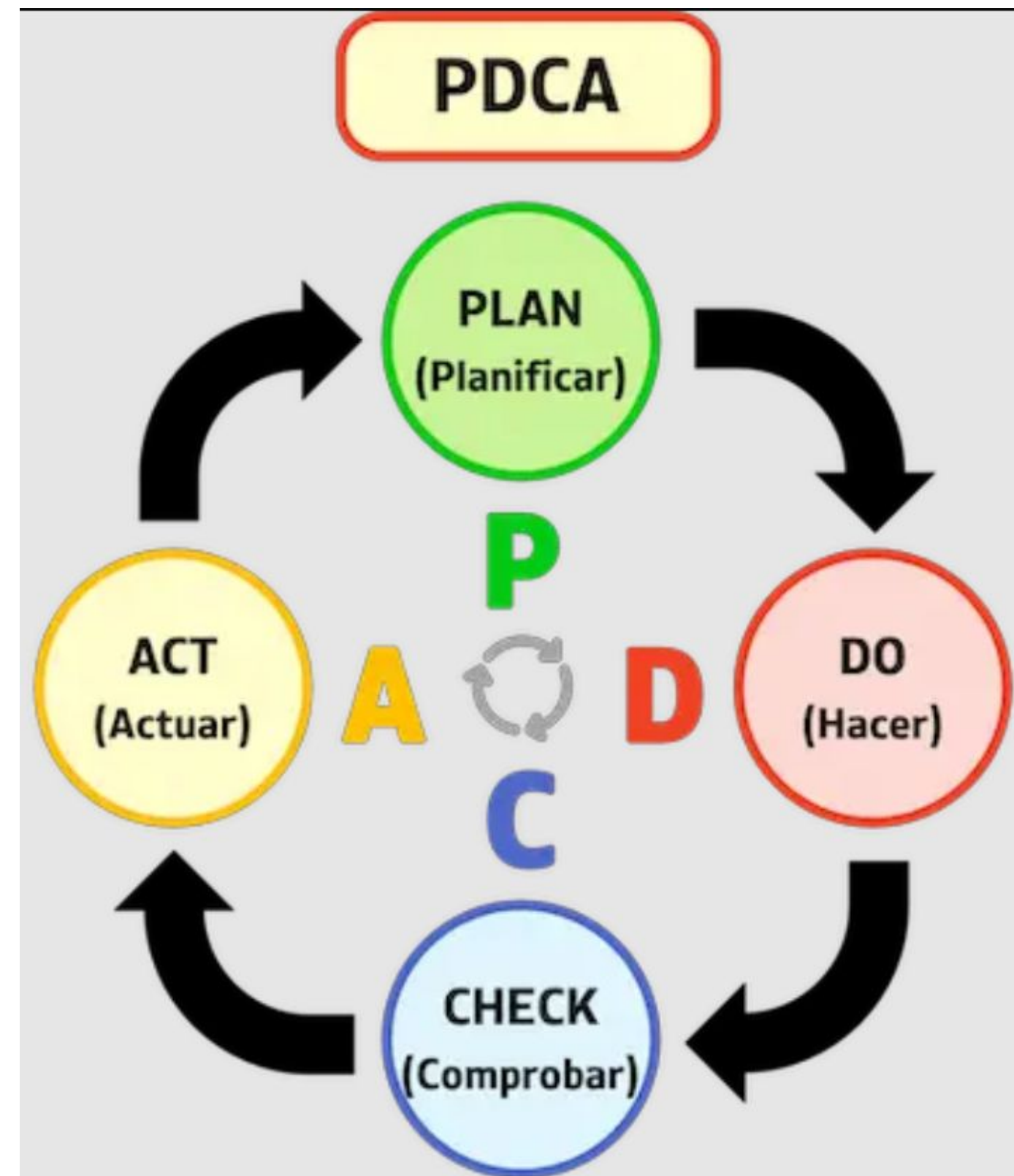


Esta foto de Autor desconocido está bajo licencia [CC BY-SA-NC](#)

8 Fases de Implementación del SGSI

- **8.-Mejora continua:**

- Implementar un proceso de mejora continua para adaptar y optimizar el SGSI en función de los cambios en el entorno de amenazas y en la organización misma.
- El **Ciclo Deming**, también conocido como **PDCA** (Planificar, Hacer, Verificar, Actuar), es fundamental en la implementación de un Sistema de Gestión de Seguridad de la Información (SGSI).
 - En la fase de **Planificar**, se establecen los objetivos y se definen las políticas y procesos de seguridad.
 - Durante la fase de **Hacer**, se implementan los controles y se ejecutan las medidas de seguridad diseñadas.
 - En la fase de **Verificar**, se monitorean y evalúan los resultados, asegurando que los controles funcionen como se esperaba.
 - Finalmente, en la fase de **Actuar**, se ajustan y mejoran los controles basándose en las lecciones aprendidas y los cambios en el entorno de seguridad, cerrando así el ciclo para garantizar una gestión continua y eficaz de la seguridad de la información.

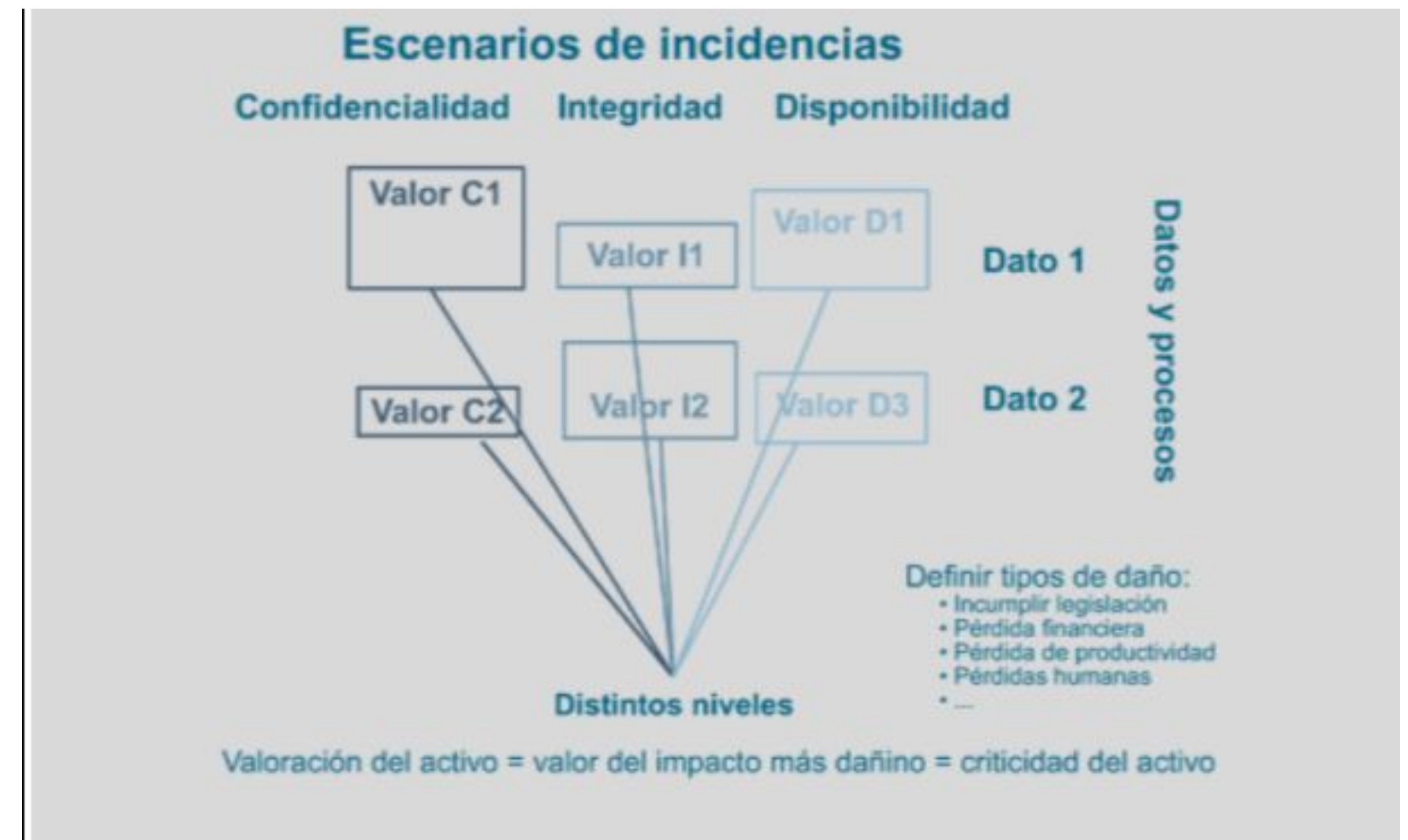


Aplicación del PDCA en ISO 27000.

PDCA	PHVA	Titulo	Cláusulas ISO27001	Objetivo	Entregables
PLAN	Planificar	Diseño del SGSI	4, 5, 6, 7	Definir la política, objetivos, procesos y procedimientos del SGSI relevantes para gestionar el riesgo y mejorar la seguridad de la información, con el fin de obtener resultados acordes con las políticas y objetivos generales de la organización.	Objetivos y controles de seguridad definidos (Declaración de aplicabilidad). Análisis y gestión de riesgos.
DO	Hacer	Implementación y funcionamiento de SGSI	8	Implementar y utilizar la política, controles, procesos y procedimientos del SGSI.	Controles operacionales
CHECK	Verificar	Supervisión revisión del SGSI	9	Evaluar y, en su caso, medir el rendimiento del proceso contra la política, objetivos y la experiencia práctica del SGSI, e informar de los resultados a la dirección para su revisión.	Controles evaluados y eficaces
ACT	Actuar	Mantenimiento y mejora del SGSI	10	Adoptar medidas correctivas en función de los resultados de la auditoría interna del SGSI y de la revisión por parte de la dirección, o de otras informaciones relevantes, para lograr la mejora continua del SGSI.	Mejoras y correcciones

Valoración de un Activo

- El impacto generado sobre un activo de información según la norma ISO 27001 es la consecuencia de la materialización de una amenaza.
- Podemos decir que hay diferentes tipos de impacto que son:
 - **Impacto operacional:** que impiden obtener el producto o resultado del servicio al que pertenece el proceso.
 - **Impacto económico:** por costes adicionales, pérdida de ingresos, penalizaciones, etc.
 - **Impacto de reputación:** por pérdida de imagen de marca al no poder prestar el servicio de forma normal a los clientes.
 - **Impacto legal y contractual:** al interrumpir un proceso concreto puede que la organización este incumpliendo algún requisito legal o contractual que pueda tener consecuencias graves.



Valoración de Impacto

- Se consideran tres grupos de impactos, ordenados según las consecuencias que reduzcan el estado de seguridad del activo que haya sido atacado, puede ser directamente e indirectamente.
- Dentro de esto tenemos que el impacto puede ser cualitativo con pérdidas funcionales, cualitativo con pérdidas orgánicas y cuantitativo, si las pérdidas se traducen en dinero más o menos directamente.
- **Cualitativo con pérdidas funcionales:**
 - SA, sub-estado de Autenticación,
 - SC, sub-estado de Confidencialidad,
 - SI, sub-estado de Integridad
 - SD, sub-estado de Disponibilidad.
- **Cualitativo con pérdidas orgánicas:**
 - N1, pérdidas de valor económico.
 - N2, pérdidas indirectas, gastos.
 - N3, pérdidas indirectas, disfuncionalidades tangibles.
 - N4, pérdidas económicas asociadas a la responsabilidad legal.
- **Cuantitativo**
 - L1, pérdidas de fondos patrimoniales intangibles.
 - L2, responsabilidad penal por incumplir las obligaciones legales.
 - L3, Perturbación de la situación política-administrativa de una forma embarazosa.
 - L4, generar daño a las personas.

Valoración de Riesgo



El Riesgo es una función de: la probabilidad de que una amenaza explote una vulnerabilidad y el impacto resultante de dicho evento externo en la organización.

