SISTEMA DE GESTIÒN DE SEGURIDAD DE LA INFORMACIÒN

ISO/IEC 27001:2013

"Las organizaciones gastan millones de dólares en firewalls y dispositivos de seguridad, pero tiran el dinero porque ninguna de estas medidas cubre el eslabón más débil de la cadena de seguridad: la gente que usa y administra los equipos"

Kevin Mitnick

ESTRUCTURA DE LA NTC ISO/IEC 27001:2013

- ¿Qué es la ISO?
- La nueva estructura ISO 27001:2013.
- Nuevos conceptos.
- La ISO 27002:2013.
- Conclusiones

I. ¿QUÉ ES LA ISO?

International Organization for Standardization

LA ISO Y SUS PRINCIPIOS DE GESTIÓN

- **Trabaja en función a 8 principios de gestión:**

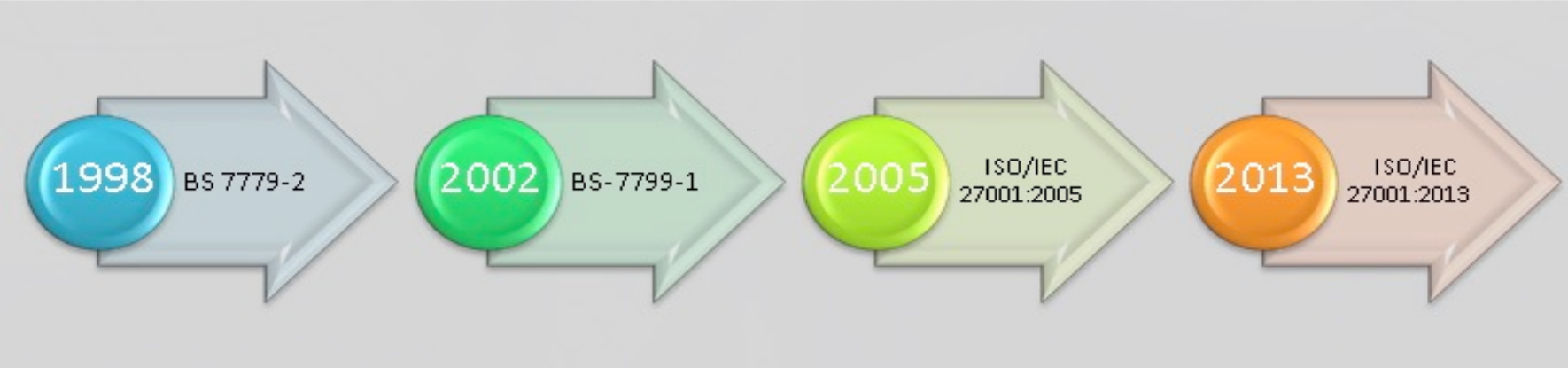
1. **Orientación al cliente.**
2. **Liderazgo.**
3. **Participación del personal.**
4. **Enfoque de procesos.**
5. **Enfoque de sistemas de gestión.**
6. **Mejora Continua.**
7. **Enfoque de mejora continua.**
8. **Relación mutuamente beneficiosa con el proveedor.**

CERTIFICADOS ISO/IEC 27001 EMITIDOS A NIVEL MUNDIAL

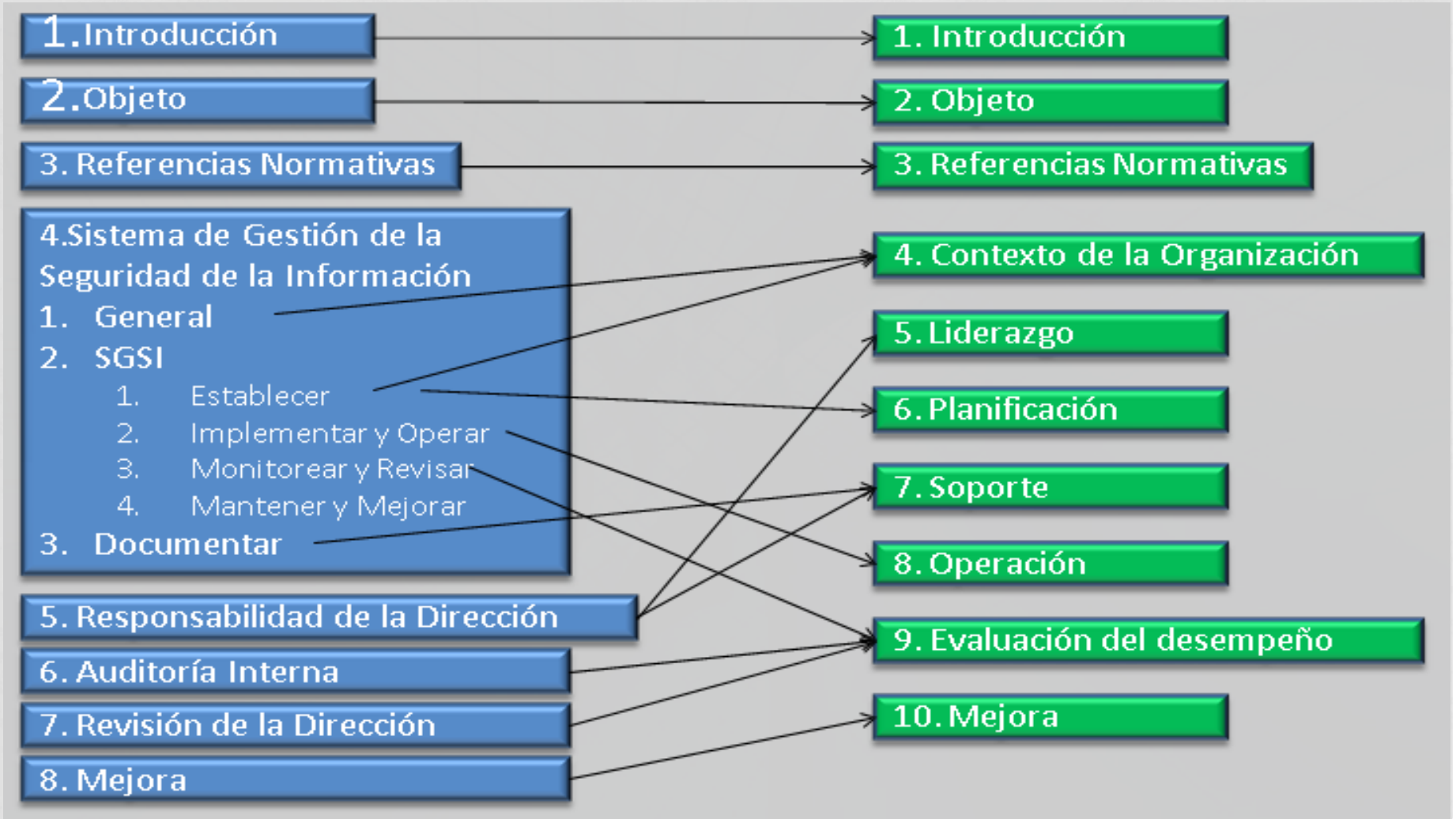
- Del informe de la ISO se desprende que el número de certificados ISO/IEC 27001 mantenidos a nivel mundial a fines del **2015** asciende a **27.536**, lo cual representa un **20%** de crecimiento respecto del 2014.

Del total de certificados emitidos,
un 44% se encuentran en el este de Asia y Pacífico,
un 38% en Europa,
un 9% en Asia Central y Sur,
un 5% en Norte América,
un 2 % en el Medio oriente,
un **1% en América Central y del Sur**
un 0.5% en África.

EVOLUCIÓN NTC ISO/IEC 27001:2013



ISO 27001:2005 Y LA 27001:2013



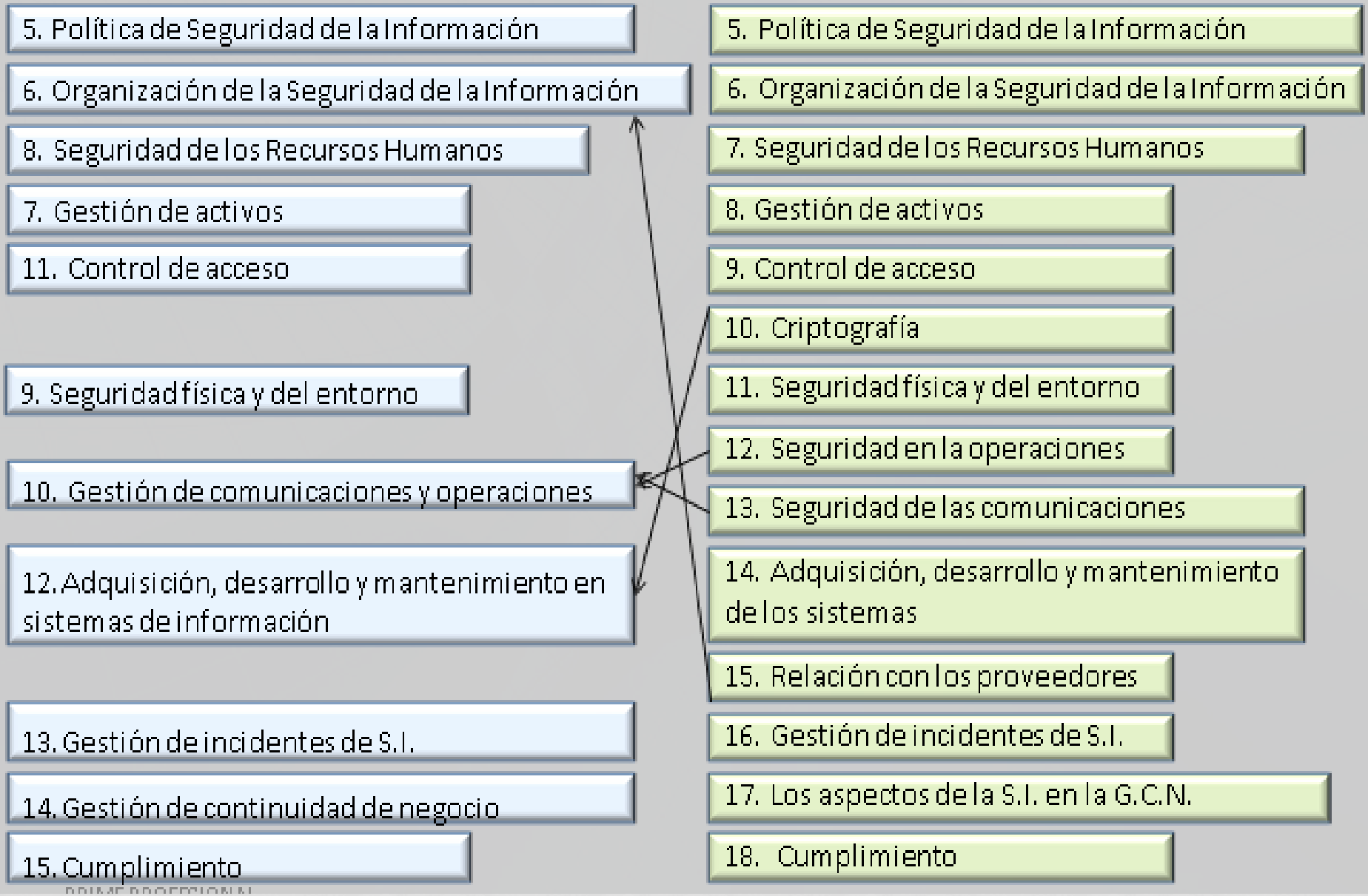
VENTAJAS Y DESVENTAJAS

VENTAJAS	DESVENTAJAS
Facilita la integración de los sistemas de gestión, debido a que es una estructura de alto nivel, donde los términos y definiciones ayudan a implementar.	Es una abstracción y es un nivel alto, no es tan detallado.
Todas las definiciones vienen del estándar ISO 27000 y las inconsistencias se han removido.	Los requisitos son un tanto mas difícil para interpretar, debido a los nuevos conceptos.
Los riesgos en la seguridad de la información en su conjunto deben ser abordados.	No se menciona el enfoque PDCA.
Los documentos requeridos están claramente establecidos, hace referencia al tamaño y complejidad.	No se menciona las políticas del SGSI.
Menciona que las acciones preventivas no van.	No hay una descripción detallada de la identificación del riesgo.

ALGUNOS DATOS

ISO 27001:2013	ISO 27001:2005
7 CLAUSULAS: La mas resaltante es el contexto de la organización.	5 CLAUSULAS:
El anexo A tiene 14 categorías de control (del 5 al 18)	El anexo A tiene 11 categorías de control (del 5 al 15)
Menciona a la ISO 31000 en la clausula 6.1 Acciones para la dirección de riesgos y oportunidades	No menciona la ISO 31000 u otro estándar.

ISO 27002:2005 Y LA ISO 27002:2013



ISO 27002:2005 Y LA ISO 27002:2013

Controles eliminados	Controles nuevos
6 .1.2 Coordinador de seguridad de la información	6.1.5 Seguridad de la información en la gestión de proyectos
10.4.2 Control de código móvil	12.6.2 Restricciones en la instalación de software
11.4.2 Autenticación de usuarios en las conexiones externas	14.2.5 Principios en Ingeniería de seguridad de los sistemas
11.4.4 Diagnostico remoto y protección de la configuración de los puertos	14.2.8 Prueba de la seguridad de los sistemas
11.4.6 Control de las conexiones de las redes	17.1.2 Implementar la continuidad de la seguridad de la información
12.2.2 Control en el procesamiento interno	15.1.3 Tecnología de información y comunicación en la cadena de suministro

ISO/IEC 27002:2013. 14 DOMINIOS, 35 OBJETIVOS DE CONTROL Y 114 CONTROLES

5. POLÍTICAS DE SEGURIDAD.

5.1 Directrices de la Dirección en seguridad de la información.
- 5.1.1 Conjunto de políticas para la seguridad de la información.
- 5.1.2 Revisión de las políticas para la seguridad de la información.

6. ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMAC.

6.1 Organización interna.
- 6.1.1 Asignación de responsabilidades para la segur. de la información.
- 6.1.2 Segregación de tareas.
- 6.1.3 Contacto con las autoridades.
- 6.1.4 Contacto con grupos de interés especial.
- 6.1.5 Seguridad de la información en la gestión de proyectos.

6.2 Dispositivos para movilidad y teletrabajo.
- 6.2.1 Política de uso de dispositivos para movilidad.
- 6.2.2 Teletrabajo.

7. SEGURIDAD LIGADA A LOS RECURSOS HUMANOS.

7.1 Antes de la contratación.
- 7.1.1 Investigación de antecedentes.
- 7.1.2 Términos y condiciones de contratación.

7.2 Durante la contratación.
- 7.2.1 Responsabilidades de gestión.
- 7.2.2 Concienciación, educación y capacitación en segur. de la informac.
- 7.2.3 Proceso disciplinario.

7.3 Cese o cambio de puesto de trabajo.
- 7.3.1 Cese o cambio de puesto de trabajo.

8. GESTIÓN DE ACTIVOS.

8.1 Responsabilidad sobre los activos.
- 8.1.1 Inventario de activos.
- 8.1.2 Propiedad de los activos.
- 8.1.3 Uso aceptable de los activos.
- 8.1.4 Devolución de activos.

8.2 Clasificación de la información.
- 8.2.1 Directrices de clasificación.
- 8.2.2 Etiquetado y manipulado de la información.
- 8.2.3 Manipulación de activos.

8.3 Manejo de los soportes de almacenamiento.
- 8.3.1 Gestión de soportes extraíbles.
- 8.3.2 Eliminación de soportes.
- 8.3.3 Soportes físicos en tránsito.

9. CONTROL DE ACCESOS.

9.1 Requisitos de negocio para el control de accesos.
- 9.1.1 Política de control de accesos.
- 9.1.2 Control de acceso a las redes y servicios asociados.

9.2 Gestión de acceso de usuario.
- 9.2.1 Gestión de altas/bajas en el registro de usuarios.
- 9.2.2 Gestión de los derechos de acceso asignados a usuarios.
- 9.2.3 Gestión de los derechos de acceso con privilegios especiales.
- 9.2.4 Gestión de información confidencial de autenticación de usuarios.
- 9.2.5 Revisión de los derechos de acceso de los usuarios.
- 9.2.6 Retirada o adaptación de los derechos de acceso

9.3 Responsabilidades del usuario.
- 9.3.1 Uso de información confidencial para la autenticación.

9.4 Control de acceso a sistemas y aplicaciones.
- 9.4.1 Restricción del acceso a la información.
- 9.4.2 Procedimientos seguros de inicio de sesión.
- 9.4.3 Gestión de contraseñas de usuario.
- 9.4.4 Uso de herramientas de administración de sistemas.
- 9.4.5 Control de acceso al código fuente de los programas.

10. CIFRADO.

10.1 Controles criptográficos.
- 10.1.1 Política de uso de los controles criptográficos.
- 10.1.2 Gestión de claves.

11. SEGURIDAD FÍSICA Y AMBIENTAL.

11.1 Áreas seguras.
- 11.1.1 Perímetro de seguridad física.
- 11.1.2 Controles físicos de entrada.
- 11.1.3 Seguridad de oficinas, despachos y recursos.
- 11.1.4 Protección contra las amenazas externas y ambientales.
- 11.1.5 El trabajo en áreas seguras.
- 11.1.6 Áreas de acceso público, carga y descarga.

11.2 Seguridad de los equipos.
- 11.2.1 Emplazamiento y protección de equipos.
- 11.2.2 Instalaciones de suministro.
- 11.2.3 Seguridad del cableado.
- 11.2.4 Mantenimiento de los equipos.
- 11.2.5 Salida de activos fuera de las dependencias de la empresa.
- 11.2.6 Seguridad de los equipos y activos fuera de las instalaciones.
- 11.2.7 Reutilización o retirada segura de dispositivos de almacenamiento.
- 11.2.8 Equipo informático de usuario desatendido.
- 11.2.9 Política de puesto de trabajo despejado y bloqueo de pantalla.

12. SEGURIDAD EN LA OPERATIVA.

12.1 Responsabilidades y procedimientos de operación.
- 12.1.1 Documentación de procedimientos de operación.
- 12.1.2 Gestión de cambios.
- 12.1.3 Gestión de capacidades.
- 12.1.4 Separación de entornos de desarrollo, prueba y producción.

12.2 Protección contra código malicioso.
- 12.2.1 Controles contra el código malicioso.

12.3 Copias de seguridad.
- 12.3.1 Copias de seguridad de la información.

12.4 Registro de actividad y supervisión.
- 12.4.1 Registro y gestión de eventos de actividad.
- 12.4.2 Protección de los registros de información.
- 12.4.3 Registros de actividad del administrador y operador del sistema.
- 12.4.4 Sincronización de relojes.

12.5 Control del software en explotación.
- 12.5.1 Instalación del software en sistemas en producción.

12.6 Gestión de la vulnerabilidad técnica.
- 12.6.1 Gestión de las vulnerabilidades técnicas.
- 12.6.2 Restricciones en la instalación de software.

12.7 Consideraciones de las auditorías de los sistemas de información.
- 12.7.1 Controles de auditoría de los sistemas de información.

13. SEGURIDAD EN LAS TELECOMUNICACIONES.

13.1 Gestión de la seguridad en las redes.
- 13.1.1 Controles de red.
- 13.1.2 Mecanismos de seguridad asociados a servicios en red.
- 13.1.3 Segregación de redes.

13.2 Intercambio de información con partes externas.
- 13.2.1 Políticas y procedimientos de intercambio de información.
- 13.2.2 Acuerdos de intercambio.
- 13.2.3 Mensajería electrónica.
- 13.2.4 Acuerdos de confidencialidad y secreto.

ISO27002.es PATROCINADO POR:

14. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN.

14.1 Requisitos de seguridad de los sistemas de información.
- 14.1.1 Análisis y especificación de los requisitos de seguridad.
- 14.1.2 Seguridad de las comunicaciones en servicios accesibles por redes públicas.
- 14.1.3 Protección de las transacciones por redes telemáticas.

14.2 Seguridad en los procesos de desarrollo y soporte.
- 14.2.1 Política de desarrollo seguro de software.
- 14.2.2 Procedimientos de control de cambios en los sistemas.
- 14.2.3 Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo.
- 14.2.4 Restricciones a los cambios en los paquetes de software.
- 14.2.5 Uso de principios de ingeniería en protección de sistemas.
- 14.2.6 Seguridad en entornos de desarrollo.
- 14.2.7 Externalización del desarrollo de software.
- 14.2.8 Pruebas de funcionalidad durante el desarrollo de los sistemas.
- 14.2.9 Pruebas de aceptación.

14.3 Datos de prueba.
- 14.3.1 Protección de los datos utilizados en pruebas.

15. RELACIONES CON SUMINISTRADORES.

15.1 Seguridad de la información en las relaciones con suministradores.
- 15.1.1 Política de seguridad de la información para suministradores.
- 15.1.2 Tratamiento del riesgo dentro de acuerdos de suministradores.
- 15.1.3 Cadena de suministro en tecnologías de la información y comunicaciones.

15.2 Gestión de la prestación del servicio por suministradores.
- 15.2.1 Supervisión y revisión de los servicios prestados por terceros.
- 15.2.2 Gestión de cambios en los servicios prestados por terceros.

16. GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN.

16.1 Gestión de incidentes de seguridad de la información y mejoras.
- 16.1.1 Responsabilidades y procedimientos.
- 16.1.2 Notificación de los eventos de seguridad de la información.
- 16.1.3 Notificación de puntos débiles de la seguridad.
- 16.1.4 Valoración de eventos de seguridad de la información y toma de decisiones.
- 16.1.5 Respuesta a los incidentes de seguridad.
- 16.1.6 Aprendizaje de los incidentes de seguridad de la información.
- 16.1.7 Recopilación de evidencias.

17. ASPECTOS DE SEGURIDAD DE LA INFORMACION EN LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO.

17.1 Continuidad de la seguridad de la información.
- 17.1.1 Planificación de la continuidad de la seguridad de la información.
- 17.1.2 Implantación de la continuidad de la seguridad de la información.
- 17.1.3 Verificación, revisión y evaluación de la continuidad de la seguridad de la información.

17.2 Redundancias.
- 17.2.1 Disponibilidad de instalaciones para el procesamiento de la información.

18. CUMPLIMIENTO.

18.1 Cumplimiento de los requisitos legales y contractuales.
- 18.1.1 Identificación de la legislación aplicable.
- 18.1.2 Derechos de propiedad intelectual (DPI).
- 18.1.3 Protección de los registros de la organización.
- 18.1.4 Protección de datos y privacidad de la información personal.
- 18.1.5 Regulación de los controles criptográficos.

18.2 Revisiones de la seguridad de la información.
- 18.2.1 Revisión independiente de la seguridad de la información.
- 18.2.2 Cumplimiento de las políticas y normas de seguridad.
- 18.2.3 Comprobación del cumplimiento.

FAMILIA 27000

- Sistemas de Gestión de Seguridad de la Información **27001**
- manual de buenas prácticas **27002**
- Manual para implementar un Sistema de Gestión de Seguridad de la Información **27003**
- Estándar se especifican las técnicas de medida y las métricas que son aplicables SGSI **27004**
- Directrices para la gestión de los Riesgos en la Seguridad de la Información **27005**
- Acreditación de las entidades de auditoría y certificación de Sistema de Gestión de Seguridad de la Información **27006**
- Manual de auditoría de un Sistema de Gestión de Seguridad de la Información **27007**

TALLER