ISO/IEC 27002:2005. DOMINIOS, OBJETIVOS DE CONTROL Y CONTROLES

5. POLÍTICA DE SEGURIDAD.
5.1 Política de seguridad de la información.
- 5.1.1 Documento de política de seguridad de la información.
- 5.1.2 Revisión de la política de seguridad de la información.

6. ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMAC.
6.1 Organización interna.
- 6.1.1 Compromiso de la Dirección con la seguridad de la información.
- 6.1.2 Coordinación de la seguridad de la información.
- 6.1.3 Asignación de responsabilidades relativas a la seguridad de la información.
- 6.1.4 Proceso de autorización de recursos para el procesado de la información.
- 6.1.5 Acuerdos de confidencialidad.
- 6.1.6 Contacto con las autoridades.
- 6.1.7 Contacto con grupos de especial interés.
- 6.1.8 Revisión independiente de la seguridad de la información.

6.2 Terceros.
- 6.2.1 Identificación de los riesgos derivados del acceso de terceros.
- 6.2.2 Tratamiento de la seguridad en la relación con los clientes.
- 6.2.3 Tratamiento de la seguridad en contratos con terceros.

7. GESTIÓN DE ACTIVOS.
7.1 Responsabilidad sobre los activos.
- 7.1.1 Inventario de activos.
- 7.1.2 Propiedad de los activos.
- 7.1.3 Uso aceptable de los activos.

7.2 Clasificación de la información.
- 7.2.1 Directrices de clasificación.
- 7.2.2 Etiquetado y manipulado de la información.

8. SEGURIDAD LIGADA A LOS RECURSOS HUMANOS.
8.1 Antes del empleo.
- 8.1.1 Funciones y responsabilidades.
- 8.1.2 Investigación de antecedentes.
- 8.1.3 Términos y condiciones de contratación.

8.2 Durante el empleo.
- 8.2.1 Responsabilidades de la dirección.
- 8.2.2 Concienciación, formación y capacitación en seguridad de la información.
- 8.2.3 Proceso disciplinario.

8.3 Cese del empleo o cambio de puesto de trabajo.
- 8.3.1 Responsabilidad del cese o cambio.
- 8.3.2 Devolución de activos.
- 8.3.3 Retirada de los de derechos de acceso.

9. SEGURIDAD FÍSICA Y AMBIENTAL.
9.1 Áreas seguras.
- 9.1.1 Perímetro de seguridad física.
- 9.1.2 Controles físicos de entrada.
- 9.1.3 Seguridad de oficinas, despachos e instalaciones.
- 9.1.4 Protección contra las amenazas externas y de origen ambiental.
- 9.1.5 Trabajo en áreas seguras.
- 9.1.6 Áreas de acceso público y de carga y descarga.

9.2 Seguridad de los equipos.
- 9.2.1 Emplazamiento y protección de equipos.
- 9.2.2 Instalaciones de suministro.
- 9.2.3 Seguridad del cableado.
- 9.2.4 Mantenimiento de los equipos.
- 9.2.5 Seguridad de los equipos fuera de las instalaciones.
- 9.2.6 Reutilización o retirada segura de equipos.
- 9.2.7 Retirada de materiales propiedad de la empresa.

10. GESTIÓN DE COMUNICACIONES Y OPERACIONES.
10.1 Responsabilidades y procedimientos de operación.
- 10.1.1 Documentación de los procedimientos de operación.
- 10.1.2 Gestión de cambios.
- 10.1.3 Segregación de tareas.
- 10.1.4 Separación de los recursos de desarrollo, prueba y operación.

10.2 Gestión de la provisión de servicios por terceros.
- 10.2.1 Provisión de servicios.
- 10.2.2 Supervisión y revisión de los servicios prestados por terceros.
- 10.2.3 Gestión de cambios en los servicios prestados por terceros.

10.3 Planificación y aceptación del sistema.
- 10.3.1 Gestión de capacidades.
- 10.3.2 Aceptación del sistema.

10.4 Protección contra código malicioso y descargable.
- 10.4.1 Controles contra el código malicioso.
- 10.4.2 Controles contra el código descargado en el cliente.

10.5 Copias de seguridad.
- 10.5.1 Copias de seguridad de la información.

10.6 Gestión de la seguridad de las redes.
- 10.6.1 Controles de red.
- 10.6.2 Seguridad de los servicios de red.

10.7 Manipulación de los soportes.
- 10.7.1 Gestión de soportes extraíbles.
- 10.7.2 Retirada de soportes.
- 10.7.3 Procedimientos de manipulación de la información.
- 10.7.4 Seguridad de la documentación del sistema.

10.8 Intercambio de información.
- 10.8.1 Políticas y procedimientos de intercambio de información.
- 10.8.2 Acuerdos de intercambio.
- 10.8.3 Soportes físicos en tránsito.
- 10.8.4 Mensajería electrónica.
- 10.8.5 Sistemas de información empresariales.

10.9 Servicios de comercio electrónico.
- 10.9.1 Comercio electrónico.
- 10.9.2 Transacciones en línea.
- 10.9.3 Información puesta a disposición pública.

10.10 Supervisión.
- 10.10.1 Registro de auditorías.
- 10.10.2 Supervisión del uso del sistema.
- 10.10.3 Protección de la información de los registros.
- 10.10.4 Registros de administración y operación.
- 10.10.5 Registro de fallos.
- 10.10.6 Sincronización del reloj.

11. CONTROL DE ACCESO.
11.1 Requisitos de negocio para el control de acceso.
- 11.1.1 Política de control de acceso.

11.2 Gestión de acceso de usuario.
- 11.2.1 Registro de usuario.
- 11.2.2 Gestión de privilegios.
- 11.2.3 Gestión de contraseñas de usuario.
- 11.2.4 Revisión de los derechos de acceso de usuario.

11.3 Responsabilidades de usuario.
- 11.3.1 Uso de contraseña.
- 11.3.2 Equipo de usuario desatendido.
- 11.3.3 Política de puesto de trabajo despejado y pantalla limpia.

11.4 Control de acceso a la red.
- 11.4.1 Política de uso de los servicios en red.
- 11.4.2 Autenticación de usuario para conexiones externas.
- 11.4.3 Identificación de equipos en las redes.
- 11.4.4 Diagnóstico remoto y protección de los puertos de configuración.
- 11.4.5 Segregación de las redes.
- 11.4.6 Control de la conexión a la red.
- 11.4.7 Control de encaminamiento de red.

11.5 Control de acceso al sistema operativo.
- 11.5.1 Procedimientos seguros de inicio de sesión.
- 11.5.2 Identificación y autenticación de usuario.
- 11.5.3 Sistema de gestión de contraseñas.
- 11.5.4 Uso de los recursos del sistema.
- 11.5.5 Desconexión automática de sesión.
- 11.5.6 Limitación del tiempo de conexión.

11.6 Control de acceso a las aplicaciones y a la información.
- 11.6.1 Restricción del acceso a la información.
- 11.6.2 Aislamiento de sistemas sensibles.

11.7 Ordenadores portátiles y teletrabajo.
- 11.7.1 Ordenadores portátiles y comunicaciones móviles.
- 11.7.2 Teletrabajo.

12. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN.
12.1 Requisitos de seguridad de los sistemas de información.
- 12.1.1 Análisis y especificación de los requisitos de seguridad.

12.2 Tratamiento correcto de las aplicaciones.
- 12.2.1 Validación de los datos de entrada.
- 12.2.2 Control del procesamiento interno.
- 12.2.3 Integridad de los mensajes.
- 12.2.4 Validación de los datos de salida.

12.3 Controles criptográficos.
- 12.3.1 Política de uso de los controles criptográficos.
- 12.3.2 Gestión de claves.

12.4 Seguridad de los archivos de sistema.
- 12.4.1 Control del software en explotación.
- 12.4.2 Protección de los datos de prueba del sistema.
- 12.4.3 Control de acceso al código fuente de los programas.

12.5 Seguridad en los procesos de desarrollo y soporte.
- 12.5.1 Procedimientos de control de cambios.
- 12.5.2 Revisión técnica de aplicaciones tras efectuar cambios en el sistema operativo.
- 12.5.3 Restricciones a los cambios en los paquetes de software.
- 12.5.4 Fugas de información.
- 12.5.5 Externalización del desarrollo de software.

12.6 Gestión de la vulnerabilidad técnica.
- 12.6.1 Control de las vulnerabilidades técnicas.

13. GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN
13.1 Notificación de eventos y puntos débiles de la segur. de la información.
- 13.1.1 Notificación de los eventos de seguridad de la información.
- 13.1.2 Notificación de puntos débiles de la seguridad.

13.2 Gestión de incidentes de seguridad de la información y mejoras.
- 13.2.1 Responsabilidades y procedimientos.
- 13.2.2 Aprendizaje de los incidentes de seguridad de la información.
- 13.2.3 Recopilación de evidencias.

14. GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO.
14.1 Aspectos de seguridad de la información en la gestión de la continuidad del negocio.
- 14.1.1 Inclusión de la seguridad de la información en el proceso de gestión de la continuidad del negocio.
- 14.1.2 Continuidad del negocio y evaluación de riesgos.
- 14.1.3 Desarrollo e implantación de planes de continuidad que incluyan la seguridad de la información.
- 14.1.4 Marco de referencia para la planificación de la cont. del negocio.
- 14.1.5 Pruebas, mantenimiento y reevaluación de planes de continuidad.

15. CUMPLIMIENTO.
15.1 Cumplimiento de los requisitos legales.
- 15.1.1 Identificación de la legislación aplicable.
- 15.1.2 Derechos de propiedad intelectual (DPI).
- 15.1.3 Protección de los documentos de la organización.
- 15.1.4 Protección de datos y privacidad de la información personal.
- 15.1.5 Prevención del uso indebido de los recursos de tratamiento de la información.
- 15.1.6 Regulación de los controles criptográficos.

15.2 Cumplimiento de las políticas y normas de segur. y cumplimiento técnico.
- 15.2.1 Cumplimiento de las políticas y normas de seguridad.
- 15.2.2 Comprobación del cumplimiento técnico.

15.3 Consideraciones de las auditorías de los sistemas de información.
- 15.3.1 Controles de auditoría de los sistemas de información.
- 15.3.2 Protección de las herramientas de auditoría de los sist. de inform.