

Quick Search

- Navigate pages | Site Map
- ISO 27002

⊞ 05. Política de Seguridad

⊞ 06. Organización de la Seguridad de Información

⊞ 07. Gestión de Activos

⊞ 08. Seguridad ligada a los Recursos Humanos

⊞ 09. Seguridad Física y del Entorno

⊞ 10. Gestión de Comunicaciones y Operaciones

⊞ 11. Control de Accesos

⊞ 12. Adquisición, Desarrollo y Mantenimiento de Sistemas de Información

⊞ 13. Gestión de Incidentes de Seguridad de la Información

⊞ 14. Gestión de Continuidad del Negocio

⊞ 15. Conformidad

● Objetivos

● Contacto

● Aviso Legal

ISO 27002

Powered by:



Con objeto de mantener las normas relacionadas con la Seguridad de la Información dentro de la serie ISO 2700x, ISO/IEC 27002 sustituye


sólo en la numeración a ISO/IEC 17799:2005, manteniendo intacto su contenido y su relación mediante el Anexo A del estándar ISO 27001.

Existe una descarga en formato pdf con la [lista de los 133 controles](#) de la norma y en una sólo página a modo de guía.

Los dominios de control ISO 27002:2005 son:

		<u>05.Política de Seguridad</u>	
			
<u>06.Aspectos Organizativos</u>	<u>07.Gestión de Activos</u>		
			<u>14.Gestión Continuidad de negocio</u>
<u>08.Recursos Humanos</u>			
			
<u>09.Física y Ambiental</u>	<u>13.Gestión de incidentes</u>	<u>12.Adquisición, desarrollo y mantenimiento de sistemas</u>	
		<u>15.Cumplimiento legal</u>	

Las cláusulas de ISO 27002:2005 son:

	<div>• 00. Introducción</div> <div>Conceptos generales de seguridad de la información y SGSI.</div> <div>• 01. Campo de aplicación</div> <div>Se especifica el objetivo de la norma.</div> <div>• 02. Términos y definiciones</div> <div>Breve descripción de los términos más usados en la norma.</div> <div>• 03. Estructura del estándar</div>
---	---

	<p>Descripción de la estructura de la norma.</p> <ul style="list-style-type: none">• 04. Evaluación y tratamiento del riesgo <p>Indicaciones sobre cómo evaluar y tratar los riesgos de seguridad de la información.</p> <ul style="list-style-type: none">• 05. Política de Seguridad <p>Documento de política de seguridad y su gestión.</p> <ul style="list-style-type: none">• 06.Aspectos Organizativos <p>Organización interna; organización externa.</p> <ul style="list-style-type: none">• 07.Gestión de Activos <p>Responsabilidad sobre los activos; clasificación de la información.</p> <ul style="list-style-type: none">• 08.Recursos Humanos <p>Anterior al empleo; durante el empleo; finalización o cambio de empleo.</p> <ul style="list-style-type: none">• 09.Física y Ambiental <p>Áreas seguras; seguridad de los equipos.</p> <ul style="list-style-type: none">• 10.Comunicaciones y Operaciones <p>Procedimientos y responsabilidades de operación; gestión de servicios de terceras partes; planificación y aceptación del sistema; protección contra software malicioso; backup; gestión de seguridad de redes; utilización de soportes de información; intercambio de información y software; servicios de comercio electrónico; monitorización.</p> <ul style="list-style-type: none">• 11.Control Accesos <p>Requisitos de negocio para el control de accesos; gestión de acceso de usuario; responsabilidades del usuario; control de acceso en red; control de acceso al sistema operativo; control de acceso a las aplicaciones e informaciones; informática y conexión móvil.</p> <ul style="list-style-type: none">• 12.Adquisición, desarrollo y mantenimiento de sistemas <p>Requisitos de seguridad de los sistemas de información; procesamiento correcto en aplicaciones; controles criptográficos; seguridad de los ficheros del sistema; seguridad en los procesos de desarrollo y soporte; gestión de vulnerabilidades técnicas.</p> <ul style="list-style-type: none">• 13.Gestión de incidentes <p>Comunicación de eventos y puntos débiles de seguridad de la información; gestión de incidentes y mejoras de seguridad de la información.</p> <ul style="list-style-type: none">• 14.Gestión Continuidad de negocio <p>Aspectos de la seguridad de la información en la gestión de continuidad del negocio.</p> <ul style="list-style-type: none">• 15.Cumplimiento legal <p>Con los requisitos legales; políticas de seguridad y estándares de conformidad y conformidad técnica; consideraciones sobre la auditoría de sistemas de información.</p> <ul style="list-style-type: none">• Bibliografía <p>Normas y publicaciones de referencia.</p>
--	---

La norma está disponible para su adquisición en diversos enlaces:

ISO/IEC 27001:2005 [ISO](#) (inglés y francés)

NTC ISO/IEC 27001:2006 [ICONTEC](#) (Colombia)

NTP ISO/IEC 17799:2007 [INDECOP](#)I (Perú)

0 Comments [Show recent to old](#)
[Post a comment](#)

[Attachments \(13\)](#)

 [RSS of this page](#)

Author: [aglone3](#) Version: [2.8](#) Last Edited By: [aglone3](#) Modified: 14 - days ago

Información de contacto

servicios@iso27002.es

Quick Search

- Navigate pages | Site Map
- ISO 27002
 - 05. Política de Seguridad
 - 06. Organización de la Seguridad de Información
 - 07. Gestión de Activos
 - 08. Seguridad ligada a los Recursos Humanos
 - 09. Seguridad Física y del Entorno
 - 10. Gestión de Comunicaciones y Operaciones
 - 11. Control de Accesos
 - 12. Adquisición, Desarrollo y Mantenimiento de Sistemas de Información
 - 13. Gestión de Incidentes de Seguridad de la Información
 - 14. Gestión de Continuidad del Negocio
 - 15. Conformidad
 - Objetivos
 - Contacto
 - Aviso Legal

Site Map

- ISO 27002
- 05. 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
- 06. Organización de la Seguridad de Información
 - 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
 - 6.1.4. Proceso de Autorización de Recursos para el Tratamiento de la Información
 - 6.1.5. Acuerdos de Confidencialidad
 - 6.1.6. Contacto con las Autoridades
 - 6.1.7. Contacto con Grupos de Interés Especial
 - 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
- 07. Gestión de Activos
 - 7 1 Responsabilidad sobre los activos
 - 7.1.1. Inventario de Activos
 - 7.1.2. Responsable de los activos
 - 7 1 3 Acuerdos sobre el uso adecuado de los activos
 - 7 2 Clasificación de la Información
 - 7.2.1 Directrices de Clasificación
 - 7.2.2 Marcado y tratamiento de la información
- 08. Seguridad ligada a los Recursos Humanos
 - 8 1 Seguridad en la definición del trabajo y los recursos
 - 8.1.1. Inclusión de la seguridad en las responsabilidades laborales
 - 8.1.2. Selección y política de personal
 - 8.1.3. Términos y condiciones de la relación laboral
 - 8 2 Seguridad en el desempeño de las funciones del empleo
 - 8.2.1. Supervisión de las obligaciones
 - 8.2.2. Formación y capacitación en seguridad de la información
 - 8.2.3. Procedimiento disciplinario
 - 8 3 Finalización o cambio del puesto de trabajo
 - 8.3.1. Cese de responsabilidades
 - 8.3.2. Restitución de activos
 - 8.3.3. Cancelación de permisos de acceso
- 09. Seguridad Física y del Entorno
 - 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 y recursos
 - 9.1.4. Protección contra amenazas externas y del entorno
 - 9.1.5. El trabajo en áreas seguras
 - 9.1.6. Áreas aisladas de carga y descarga
 - 9 2 Seguridad de los equipos
 - 9.2.1. Instalación y protección de equipos
 - 9.2.2. Suministro eléctrico
 - 9.2.3. Seguridad del cableado
 - 9.2.4. Mantenimiento de equipos
 - 9 2 5 Seguridad de equipos fuera de los locales de la Organización
 - 9.2.6. Seguridad en la reutilización o eliminación de equipos
 - 9.2.7. Traslado de activos

- [10. Gestión de Comunicaciones y Operaciones](#)
 - [10 1 Procedimientos y responsabilidades de operación](#)
 - [10.1.1. Documentación de procedimientos operativos](#)
 - [10.1.2. Control de cambios operacionales](#)
 - [10.1.3. Segregación de tareas](#)
 - [10.1.4. Separación de los recursos para desarrollo y producción](#)
 - [10 2 Supervisión de los servicios contratados a terceros](#)
 - [10.2.1. Prestación de servicios](#)
 - [10.2.2. Monitorización y revisión de los servicios contratados](#)
 - [10.2.3. Gestión de los cambios en los servicios contratados](#)
 - [10 3 Planificación y aceptación del sistema](#)
 - [10. 3. 1. Planificación de capacidades](#)
 - [10. 3. 2. Aceptación del sistema](#)
 - [10 4 Protección contra software malicioso y código móvil](#)
 - [10. 4. 1. Medidas y controles contra software malicioso](#)
 - [10. 4. 2. Medidas y controles contra código móvil](#)
 - [10 5 Gestión interna de soportes y recuperación](#)
 - [10. 5. 1. Recuperación de la información](#)
 - [10 6 Gestión de redes](#)
 - [10. 6. 1. Controles de red](#)
 - [10. 6. 2. Seguridad en los servicios de red](#)
 - [10 7 Utilización y seguridad de los soportes de información](#)
 - [10. 7. 1. Gestión de soportes extraíbles](#)
 - [10. 7. 2. Eliminación de soportes](#)
 - [10. 7. 3. Procedimientos de utilización de la información](#)
 - [10. 7. 4. Seguridad de la documentación de sistemas](#)
 - [10 8 Intercambio de información y software](#)
 - [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. Seguridad en comercio electrónico](#)
 - [10. 9. 2. Seguridad en transacciones en línea](#)
 - [10 9 3 Seguridad en información pública](#)
 - [10 10 Monitorización](#)
 - [10. 10. 1. Registro de incidencias](#)
 - [10. 10. 2. Supervisión del uso de los sistemas](#)
 - [10. 10. 3. Protección de los registros de incidencias](#)
 - [10. 10. 4. Diarios de operación del administrador y operador](#)
 - [10. 10. 5. Registro de fallos](#)
 - [10. 10. 6. Sincronización del reloj](#)
- [11. Control de Accesos](#)
 - [11 1 Requerimientos de negocio para el control de accesos](#)
 - [11.1.1. Política de control de accesos](#)
 - [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 los usuarios](#)
 - [11 3 Responsabilidades del usuario](#)
 - [11.3.1. Uso de contraseña](#)
 - [11.3.2. Equipo informático de usuario desatendido](#)
 - [11.3.3. Políticas para escritorios y monitores sin información](#)
 - [11 4 Control de acceso en red](#)
 - [11.4.1. Política de uso de los servicios de red](#)
 - [11.4.2. Autenticación de usuario para conexiones externas](#)
 - [11.4.3. Autenticación de nodos de la red](#)
 - [11.4.4. Protección a puertos de diagnóstico remoto](#)
 - [11.4.5. Segregación en las redes](#)
 - [11.4.6. Control de conexión a las redes](#)
 - [11.4.7. Control de encaminamiento en la red](#)
 - [11 5 Control de acceso al sistema operativo](#)
 - [11.5.1. Procedimientos de conexión de terminales](#)

- [11.5.2. Identificación y autenticación de usuario](#)
- [11.5.3. Sistema de gestión de contraseñas](#)
- [11.5.4. Uso de los servicios del sistema](#)
- [11.5.5. Desconexión automática de terminales](#)
- [11.5.6. Limitación del tiempo de conexión](#)
- [11.6 Control de acceso a las aplicaciones](#)
 - [11.6.1. Restricción de acceso a la información](#)
 - [11.6.2 Aislamiento de sistemas sensibles](#)
- [11.7 Informática móvil y tele trabajo](#)
 - [11.7.1 Informática móvil](#)
 - [11.7.2. Tele trabajo](#)
- [12. Adquisición, Desarrollo y Mantenimiento de Sistemas de Información](#)
 - [12.1 Requisitos de seguridad de los sistemas](#)
 - [12.1.1. Análisis y especificación de los requisitos de seguridad](#)
 - [12.2 Seguridad de las aplicaciones del sistema](#)
 - [12.2.1. Validación de los datos de entrada](#)
 - [12.2.2. Control del proceso interno](#)
 - [12.2.3. Autenticación de 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. Cifrado](#)
 - [12.4 Seguridad de los ficheros del 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 a la librería de programas fuente](#)
 - [12.5 Seguridad en los procesos de desarrollo y soporte](#)
 - [12.5.1. Procedimientos de control de cambios](#)
 - [12.5.2. Revisión técnica de los cambios en el sistema operativo](#)
 - [12.5.3. Restricciones en los cambios a los paquetes de software](#)
 - [12.5.4. Canales encubiertos y código Troyano](#)
 - [12.5.5. Desarrollo externalizado del software](#)
 - [12.6 Gestión de las vulnerabilidades técnicas](#)
 - [12.6.1. Control de las vulnerabilidades técnicas](#)
- [13. Gestión de Incidentes de Seguridad de la Información](#)
 - [13.1 Comunicación de eventos y debilidades en la seguridad de la información](#)
 - [13.1.1 Comunicación de eventos en seguridad](#)
 - [13.1.2. Comunicación de debilidades en seguridad](#)
 - [13.2 Gestión de incidentes y mejoras en la seguridad de la información](#)
 - [13.2.1. Identificación de responsabilidades y procedimientos](#)
 - [13.2.2. Evaluación de incidentes en seguridad](#)
 - [13.2.3. Recogida de pruebas](#)
- [14. Gestión de Continuidad del Negocio](#)
 - [14.1 Aspectos de la gestión de continuidad del negocio](#)
 - [14.1.1. Proceso de la gestión de continuidad del negocio](#)
 - [14.1.2. Continuidad del negocio y análisis de impactos](#)
 - [14.1.3. Redacción e implantación de planes de continuidad](#)
 - [14.1.4. Marco de planificación para la continuidad del negocio](#)
 - [14.1.5. Prueba, mantenimiento y reevaluación de planes de continuidad](#)
- [15. Conformidad](#)
 - [15.1 Conformidad con los requisitos legales](#)
 - [15.1.1. Identificación de la legislación aplicable](#)
 - [15.1.2. Derechos de propiedad intelectual \(IPR\)](#)
 - [15.1.3. Salvaguarda de los registros de la Organización](#)
 - [15.1.4. Protección de datos de carácter personal y de la intimidad de las personas](#)
 - [15.1.5. Evitar mal uso de los dispositivos de tratamiento de la información](#)
 - [15.1.6. Reglamentación de los controles de cifrados](#)
 - [15.2 Revisiones de la política de seguridad y de la conformidad técnica](#)
 - [15.2.1. Conformidad con la política de seguridad](#)
 - [15.2.2. Comprobación de la conformidad técnica](#)
 - [15.3 Consideraciones sobre la auditoría de sistemas](#)
 - [15.3.1. Controles de auditoría de sistemas](#)
 - [15.3.2. Protección de las herramientas de auditoría de sistemas](#)

- [Objetivos](#)
- [Contacto](#)
- [Aviso Legal](#)

Información de contacto

servicios@iso27002.es

Quick Search

- Navigate pages | Site Map
- ISO 27002

⊞ 05. Política de Seguridad

⊞ 06. Organización de la Seguridad de Información

⊞ 07. Gestión de Activos

⊞ 08. Seguridad ligada a los Recursos Humanos

⊞ 09. Seguridad Física y del Entorno

⊞ 10. Gestión de Comunicaciones y Operaciones

⊞ 11. Control de Accesos

⊞ 12. Adquisición, Desarrollo y Mantenimiento de Sistemas de Información

⊞ 13. Gestión de Incidentes de Seguridad de la Información

⊞ 14. Gestión de Continuidad del Negocio

⊞ 15. Conformidad

● Objetivos

● Contacto

● Aviso Legal

ISO 27002

Powered by:



Con objeto de mantener las normas relacionadas con la Seguridad de la Información dentro de la serie ISO 2700x, ISO/IEC 27002 sustituye


sólo en la numeración a ISO/IEC 17799:2005, manteniendo intacto su contenido y su relación mediante el Anexo A del estándar ISO 27001.

Existe una descarga en formato pdf con la [lista de los 133 controles](#) de la norma y en una sólo página a modo de guía.

Los dominios de control ISO 27002:2005 son:

		<u>05.Política de Seguridad</u>	
			
<u>06.Aspectos Organizativos</u>		<u>07.Gestión de Activos</u>	
			
<u>08.Recursos Humanos</u>			
			
<u>09.Física y Ambiental</u>		<u>10.Comunicaciones y Operaciones</u>	
			
<u>13.Gestión de incidentes</u>		<u>12.Adquisición, desarrollo y mantenimiento de sistemas</u>	
			
<u>15.Cumplimiento legal</u>			

Las cláusulas de ISO 27002:2005 son:

	• 00. Introducción
	Conceptos generales de seguridad de la información y SGSI.
	• 01. Campo de aplicación
	Se especifica el objetivo de la norma.
	• 02. Términos y definiciones
	Breve descripción de los términos más usados en la norma.
	• 03. Estructura del estándar

	<p>Descripción de la estructura de la norma.</p> <ul style="list-style-type: none">• 04. Evaluación y tratamiento del riesgo <p>Indicaciones sobre cómo evaluar y tratar los riesgos de seguridad de la información.</p> <ul style="list-style-type: none">• 05. Política de Seguridad <p>Documento de política de seguridad y su gestión.</p> <ul style="list-style-type: none">• 06.Aspectos Organizativos <p>Organización interna; organización externa.</p> <ul style="list-style-type: none">• 07.Gestión de Activos <p>Responsabilidad sobre los activos; clasificación de la información.</p> <ul style="list-style-type: none">• 08.Recursos Humanos <p>Anterior al empleo; durante el empleo; finalización o cambio de empleo.</p> <ul style="list-style-type: none">• 09.Física y Ambiental <p>Áreas seguras; seguridad de los equipos.</p> <ul style="list-style-type: none">• 10.Comunicaciones y Operaciones <p>Procedimientos y responsabilidades de operación; gestión de servicios de terceras partes; planificación y aceptación del sistema; protección contra software malicioso; backup; gestión de seguridad de redes; utilización de soportes de información; intercambio de información y software; servicios de comercio electrónico; monitorización.</p> <ul style="list-style-type: none">• 11.Control Accesos <p>Requisitos de negocio para el control de accesos; gestión de acceso de usuario; responsabilidades del usuario; control de acceso en red; control de acceso al sistema operativo; control de acceso a las aplicaciones e informaciones; informática y conexión móvil.</p> <ul style="list-style-type: none">• 12.Adquisición, desarrollo y mantenimiento de sistemas <p>Requisitos de seguridad de los sistemas de información; procesamiento correcto en aplicaciones; controles criptográficos; seguridad de los ficheros del sistema; seguridad en los procesos de desarrollo y soporte; gestión de vulnerabilidades técnicas.</p> <ul style="list-style-type: none">• 13.Gestión de incidentes <p>Comunicación de eventos y puntos débiles de seguridad de la información; gestión de incidentes y mejoras de seguridad de la información.</p> <ul style="list-style-type: none">• 14.Gestión Continuidad de negocio <p>Aspectos de la seguridad de la información en la gestión de continuidad del negocio.</p> <ul style="list-style-type: none">• 15.Cumplimiento legal <p>Con los requisitos legales; políticas de seguridad y estándares de conformidad y conformidad técnica; consideraciones sobre la auditoría de sistemas de información.</p> <ul style="list-style-type: none">• Bibliografía <p>Normas y publicaciones de referencia.</p>
--	---

La norma está disponible para su adquisición en diversos enlaces:

ISO/IEC 27001:2005 [ISO](#) (inglés y francés)

NTC ISO/IEC 27001:2006 [ICONTEC](#) (Colombia)

NTP ISO/IEC 17799:2007 [INDECOP](#)I (Perú)

0 Comments [Show recent to old](#)
[Post a comment](#)

[Attachments \(13\)](#)

 [RSS of this page](#)

Author: [aglone3](#) Version: [2.8](#) Last Edited By: [aglone3](#) Modified: 14 - days ago

Información de contacto

servicios@iso27002.es

Quick Search

- Navigate pages | Site Map
- ISO 27002

05. Política de Seguridad

5 1 Política de seguridad de la información

06. Organización de la Seguridad de Información

07. Gestión de Activos

08. Seguridad ligada a los Recursos Humanos

09. Seguridad Física y del Entorno

10. Gestión de Comunicaciones y Operaciones

11. Control de Accesos

12. Adquisición, Desarrollo y Mantenimiento de Sistemas de Información

13. Gestión de Incidentes de Seguridad de la Información

14. Gestión de Continuidad del Negocio

15. Conformidad

Objetivos

Contacto

Aviso Legal

Site Home » 05. Política de Seguridad

05. Política de Seguridad



La estructura de este punto de la norma es:

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

0 Comments Show recent to old
Post a comment

RSS of this page

Author: [aglonge](#) Version: [1.6](#) Last Edited By: [javier_ruiz](#) Modified: 10 - days ago

Información de contacto

servicios@iso27002.es

Quick Search

- Navigate pages | Site Map
- ISO 27002

⊞ 05. Política de Seguridad

⊞ 06. Organización de la Seguridad de Información

⊞ 6 1 Organización Interna

⊞ 6 2 Terceros

⊞ 07. Gestión de Activos

⊞ 08. Seguridad ligada a los Recursos Humanos

⊞ 09. Seguridad Física y del Entorno

⊞ 10. Gestión de Comunicaciones y Operaciones

⊞ 11. Control de Accesos

⊞ 12. Adquisición, Desarrollo y Mantenimiento de Sistemas de Información

⊞ 13. Gestión de Incidentes de Seguridad de la Información

⊞ 14. Gestión de Continuidad del Negocio

⊞ 15. Conformidad

● Objetivos

● Contacto

● Aviso Legal

 [Site Home](#) >> 06. Organización de la Seguridad de Información

06. Organización de la Seguridad de Información



La estructura de este punto de la norma es:

[6.1. Estructura para la seguridad de la información](#)

- [6.1.1. Comité de gestión de seguridad de la información](#)
- [6.1.2. Coordinación de seguridad de la información](#)
- [6.1.3. Asignación de responsabilidades para la seguridad de la información](#)
- [6.1.4. Proceso de autorización de recursos para el tratamiento de la información](#)
- [6.1.5. Acuerdos de confidencialidad](#)
- [6.1.6. Contacto con las autoridades](#)
- [6.1.7. Contacto con organizaciones 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](#)

0 Comments [Show recent to old](#)
[Post a comment](#)

 [RSS of this page](#)

Author: [aglone](#) Version: [1.2](#) Last Edited By: [aglone3](#) Modified: 26 - days ago

Información de contacto

servicios@iso27002.es

Quick Search

- Navigate pages | Site Map
- ISO 27002
 - 05. Política de Seguridad
 - 06. Organización de la Seguridad de Información
 - 07. Gestión de Activos**
 - 7 1 Responsabilidad sobre los activos
 - 7 2 Clasificación de la Información
 - 08. Seguridad ligada a los Recursos Humanos
 - 09. Seguridad Física y del Entorno
 - 10. Gestión de Comunicaciones y Operaciones
 - 11. Control de Accesos
 - 12. Adquisición, Desarrollo y Mantenimiento de Sistemas de Información
 - 13. Gestión de Incidentes de Seguridad de la Información
 - 14. Gestión de Continuidad del Negocio
 - 15. Conformidad
 - Objetivos
 - Contacto
 - Aviso Legal

07. Gestión de Activos



La estructura de este punto de la norma es:

7.1. Responsabilidad sobre los activos.

- 7.1.1. Inventario de activos.
- 7.1.2. Responsable de los activos.
- 7.1.3. Acuerdos sobre el uso aceptable de los activos.

7.2. Clasificación de la información

- 7.2.1. Directrices de clasificación.
- 7.2.2. Marcado y tratamiento de la información.

0 Comments [Show recent to old](#)
Post a comment

RSS of this page

Author: [aglone](#) Version: [1.2](#) Last Edited By: [aglone3](#) Modified: 26 - days ago

Información de contacto

servicios@iso27002.es

Quick Search

- Navigate pages | Site Map
- ISO 27002

05. Política de Seguridad

06. Organización de la Seguridad de Información

07. Gestión de Activos

08. Seguridad ligada a los Recursos Humanos

8 1 Seguridad en la definición del trabajo y los recursos

8 2 Seguridad en el desempeño de las funciones del empleo

8 3 Finalización o cambio del puesto de trabajo

09. Seguridad Física y del Entorno

10. Gestión de Comunicaciones y Operaciones

11. Control de Accesos

12. Adquisición, Desarrollo y Mantenimiento de Sistemas de Información

13. Gestión de Incidentes de Seguridad de la Información

14. Gestión de Continuidad del Negocio

15. Conformidad

Objetivos

Contacto

Aviso Legal

08. Seguridad ligada a los Recursos Humanos



La estructura de este punto de la norma es:

8.1. Seguridad en la definición del trabajo y los recursos.

8.1.1. [Inclusión de la seguridad en las responsabilidades laborales.](#)

8.1.2. [Selección y política de personal.](#)

8.1.3. [Términos y condiciones de la relación laboral.](#)

8.2. Seguridad en el desempeño de las funciones del empleo.

8.2.1. [Supervisión de las obligaciones.](#)

8.2.2. [Formación y capacitación en seguridad de la información.](#)

8.2.3. [Procedimiento disciplinario.](#)

8.3. Finalización o cambio del puesto de trabajo.

8.3.1. [Cese de responsabilidades.](#)

8.3.2. [Restitución de activos.](#)

8.3.3. [Cancelación de permisos de acceso.](#)

0 Comments

Show recent to old

Post a comment

RSS of this page

Author: [aglone](#)

Version: [1.2](#)

Last Edited By: [aglone3](#)

Modified: 26 - days ago

Información de contacto

servicios@iso27002.es

Quick Search

- Navigate pages | Site Map
- ISO 27002
 - 05. Política de Seguridad
 - 06. Organización de la Seguridad de Información
 - 07. Gestión de Activos
 - 08. Seguridad ligada a los Recursos Humanos
 - 09. Seguridad Física y del Entorno**
 - 9 1 Áreas seguras
 - 9 2 Seguridad de los equipos
 - 10. Gestión de Comunicaciones y Operaciones
 - 11. Control de Accesos
 - 12. Adquisición, Desarrollo y Mantenimiento de Sistemas de Información
 - 13. Gestión de Incidentes de Seguridad de la Información
 - 14. Gestión de Continuidad del Negocio
 - 15. Conformidad
 - Objetivos
 - Contacto
 - Aviso Legal

09. Seguridad Física y del Entorno



La estructura de este punto de la norma es:

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 y recursos.](#)
- 9.1.4. [Protección contra amenazas externas y del entorno.](#)
- 9.1.5. [El trabajo en áreas seguras.](#)
- 9.1.6. [Áreas aisladas de carga y descarga.](#)

9.2. Seguridad de los equipos.

- 9.2.1. [Instalación y protección de equipos.](#)
- 9.2.2. [Suministro eléctrico.](#)
- 9.2.3. [Seguridad del cableado.](#)
- 9.2.4. [Mantenimiento de equipos.](#)
- 9.2.5. [Seguridad de equipos fuera de los locales de la Organización.](#)
- 9.2.6. [Seguridad en la reutilización o eliminación de equipos.](#)
- 9.2.7. [Traslado de activos.](#)

0 Comments [Show recent to old](#)
[Post a comment](#)

RSS of this page

Author: [aglone](#) Version: [1.2](#) Last Edited By: [aglone3](#) Modified: 26 - days ago

Información de contacto

servicios@iso27002.es

Quick Search

- Navigate pages | Site Map
- ISO 27002

05. Política de Seguridad

06. Organización de la Seguridad de Información

07. Gestión de Activos

08. Seguridad ligada a los Recursos Humanos

09. Seguridad Física y del Entorno

10. Gestión de Comunicaciones y Operaciones

10 1 Procedimientos y responsabilidades de operación

10 2 Supervisión de los servicios contratados a terceros

10 3 Planificación y aceptación del sistema

10 4 Protección contra software malicioso y código móvil

10 5 Gestión interna de soportes y recuperación

10 6 Gestión de redes

10 7 Utilización y seguridad de los soportes de información

10 8 Intercambio de información y software

10 9 Servicios de comercio electrónico

10 10 Monitorización

11. Control de Accesos

12. Adquisición, Desarrollo y Mantenimiento de Sistemas de Información

13. Gestión de Incidentes de Seguridad de la Información

14. Gestión de Continuidad del Negocio

15. Conformidad

Objetivos

Contacto

Aviso Legal

 [Site Home](#) » 10. Gestión de Comunicaciones y Operaciones

10. Gestión de Comunicaciones y Operaciones



La estructura de este punto de la norma es:

10.1. Procedimientos y responsabilidades de operación.

- [10.1.1. Documentación de procedimientos operativos.](#)
- [10.1.2. Control de cambios operacionales.](#)
- [10.1.3. Segregación de tareas.](#)
- [10.1.4. Separación de los recursos para desarrollo y producción.](#)

10.2. Supervisión de los servicios contratados a terceros.

- [10.2.1. Prestación de servicios.](#)
- [10.2.2. Monitorización y revisión de los servicios contratados.](#)
- [10.2.3. Gestión de los cambios en los servicios contratados.](#)

10.3. Planificación y aceptación del sistema.

- [10.3.1. Planificación de capacidades.](#)
- [10.3.2. Aceptación del sistema.](#)

10.4. Protección contra software malicioso y código móvil.

- [10.4.1. Medidas y controles contra software malicioso.](#)
- [10.4.2. Medidas y controles contra código móvil.](#)

10.5. Gestión interna de soportes y recuperación.

- [10.5.1. Recuperación de la información.](#)

10.6. Gestión de redes.

- [10.6.1. Controles de red.](#)
- [10.6.2. Seguridad en los servicios de red.](#)

10.7. Utilización y seguridad de los soportes de información.

- [10.7.1. Gestión de soportes extraíbles.](#)
- [10.7.2. Eliminación de soportes.](#)
- [10.7.3. Procedimientos de utilización de la información.](#)
- [10.7.4. Seguridad de la documentación de sistemas.](#)

10.8. Intercambio de información y software.

- [10.8.1. Acuerdos para intercambio de información y software.](#)
- [10.8.2. Seguridad de soportes en tránsito.](#)
- [10.8.3. Mensajería electrónica.](#)
- [10.8.4. Interconexión de sistemas con información de negocio](#)
- [10.8.5. Sistemas de información empresariales.](#)

10.9. Servicios de comercio electrónico.

- [10.9.1. Seguridad en comercio electrónico.](#)
- [10.9.2. Seguridad en transacciones en línea.](#)
- [10.9.3. Seguridad en información pública.](#)

10.10. Monitorización

- [10.10.1. Registro de incidencias.](#)
- [10.10.2. Seguimiento del uso de los sistemas.](#)
- [10.10.3. Protección de los registros de incidencias.](#)
- [10.10.4. Diarios de operación del administrador y operador.](#)

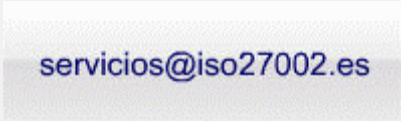
- [10.10.5. Registro de fallos.](#)
- [10.10.6. Sincronización de reloj.](#)

0 Comments [Show recent to old](#)
[Post a comment](#)

 [RSS of this page](#)

Author: [aglone](#) **Version:** [1.1](#) **Last Edited By:** [aglone3](#) **Modified:** 27 - days ago

Información de contacto



Quick Search

- Navigate pages | Site Map
- ISO 27002
 - 05. Política de Seguridad
 - 06. Organización de la Seguridad de Información
 - 07. Gestión de Activos
 - 08. Seguridad ligada a los Recursos Humanos
 - 09. Seguridad Física y del Entorno
 - 10. Gestión de Comunicaciones y Operaciones
 - 11. Control de Accesos**
 - 11 1 Requerimientos de negocio para el control de accesos
 - 11 2 Gestión de acceso de usuario
 - 11 3 Responsabilidades del usuario
 - 11 4 Control de acceso en red
 - 11 5 Control de acceso al sistema operativo
 - 11 6 Control de acceso a las aplicaciones
 - 11 7 Informática móvil y tele trabajo
 - 12. Adquisición, Desarrollo y Mantenimiento de Sistemas de Información
 - 13. Gestión de Incidentes de Seguridad de la Información
 - 14. Gestión de Continuidad del Negocio
 - 15. Conformidad
 - Objetivos
 - Contacto
 - Aviso Legal

11. Control de Accesos



La estructura de este punto de la norma es:

11.1. Requisitos de negocio para el control de accesos.

11.1.1. Política de control de accesos.

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 los usuarios.

11.3. Responsabilidades del usuario.

11.3.1. Uso de contraseña.

11.3.2. Equipo informático de usuario desatendido.

11.3.3. Políticas para escritorios y monitores sin información.

11.4. Control de acceso en red.

11.4.1. Política de uso de los servicios de red.

11.4.2. Autenticación de usuario para conexiones externas.

11.4.3. Autenticación de nodos de la red.

11.4.4. Protección a puertos de diagnóstico remoto.

11.4.5. Segregación en las redes.

11.4.6. Control de conexión a las redes.

11.4.7. Control de encaminamiento en la red.

11.5. Control de acceso al sistema operativo.

11.5.1. Procedimientos de conexión de terminales.

11.5.2. Identificación y autenticación de usuario.

11.5.3. Sistema de gestión de contraseñas.

11.5.4. Uso de los servicios del sistema.

11.5.5. Desconexión automática de terminales.

11.5.6. Limitación del tiempo de conexión.

11.6. Control de acceso a las aplicaciones.

11.6.1. Restricción de acceso a la información.

11.6.2. Aislamiento de sistemas sensibles.

11.7. Informática móvil y tele trabajo.

11.7.1. Informática móvil.

11.7.2. Tele trabajo.

0 Comments Show recent to old
Post a comment

RSS of this page

Author: [aglone](#) Version: [1.1](#) Last Edited By: [aglone3](#) Modified: 27 - days ago

Información de contacto

servicios@iso27002.es

Quick Search

- Navigate pages | Site Map
- ISO 27002
 - 05. Política de Seguridad
 - 06. Organización de la Seguridad de Información
 - 07. Gestión de Activos
 - 08. Seguridad ligada a los Recursos Humanos
 - 09. Seguridad Física y del Entorno
 - 10. Gestión de Comunicaciones y Operaciones
 - 11. Control de Accesos
 - 12. Adquisición, Desarrollo y Mantenimiento de Sistemas de Información**
 - 12 1 Requisitos de seguridad de los sistemas
 - 12 2 Seguridad de las aplicaciones del sistema
 - 12 3 Controles criptográficos
 - 12 4 Seguridad de los ficheros del sistema
 - 12 5 Seguridad en los procesos de desarrollo y soporte
 - 12 6 Gestión de las vulnerabilidades técnicas
 - 13. Gestión de Incidentes de Seguridad de la Información
 - 14. Gestión de Continuidad del Negocio
 - 15. Conformidad
 - Objetivos
 - Contacto
 - Aviso Legal

12. Adquisición, Desarrollo y Mantenimiento de Sistemas de Información



La estructura de este punto de la norma es:

12.1. Requisitos de seguridad de los sistemas.

[12.1.1. Análisis y especificación de los requisitos de seguridad.](#)

12.2. Seguridad de las aplicaciones del sistema.

[12.2.1. Validación de los datos de entrada.](#)

[12.2.2. Control del proceso interno.](#)

[12.2.3. Autenticación de 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. Cifrado.](#)

12.4. Seguridad de los ficheros del 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 a la librería de programas fuente.](#)

12.5. Seguridad en los procesos de desarrollo y soporte.

[12.5.1. Procedimientos de control de cambios.](#)

[12.5.2. Revisión técnica de los cambios en el sistema operativo.](#)

[12.5.3. Restricciones en los cambios a los paquetes de software.](#)

[12.5.4. Canales encubiertos y código Troyano.](#)

[12.5.5. Desarrollo externalizado del software.](#)

12.6. Gestión de las vulnerabilidades técnicas.

[12.6.1. Control de las vulnerabilidades técnicas.](#)

0 Comments

Show recent to old

Post a comment

RSS of this page

Author: [aglone](#)

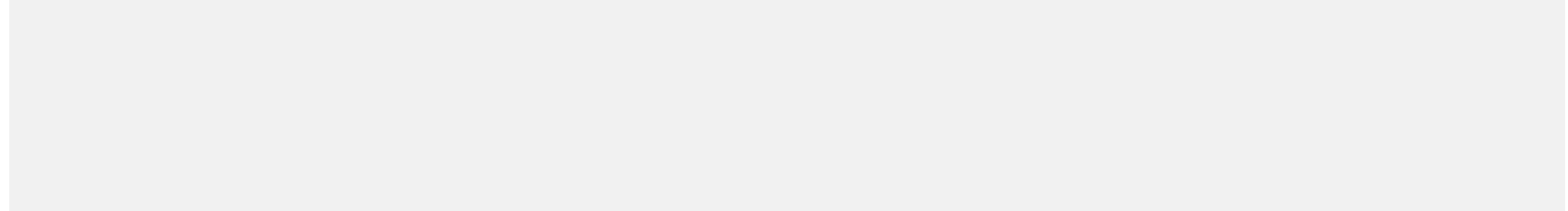
Version: [1.1](#)

Last Edited By: [aglone3](#)

Modified: 27 - days ago

Información de contacto

servicios@iso27002.es



Quick Search

- Navigate pages | Site Map
- ISO 27002
 - 05. Política de Seguridad
 - 06. Organización de la Seguridad de Información
 - 07. Gestión de Activos
 - 08. Seguridad ligada a los Recursos Humanos
 - 09. Seguridad Física y del Entorno
 - 10. Gestión de Comunicaciones y Operaciones
 - 11. Control de Accesos
 - 12. Adquisición, Desarrollo y Mantenimiento de Sistemas de Información
 - 13. Gestión de Incidentes de Seguridad de la Información**
 - 13 1 Comunicación de eventos y debilidades en la seguridad de la información
 - 13 2 Gestión de incidentes y mejoras en la seguridad de la información
 - 14. Gestión de Continuidad del Negocio
 - 15. Conformidad
 - Objetivos
 - Contacto
 - Aviso Legal

13. Gestión de Incidentes de Seguridad de la Información



La estructura de este punto de la norma es:

13.1. Comunicación de eventos y debilidades en la seguridad de la información.

13.1.1. Comunicación de eventos en seguridad.

13.1.2. Comunicación de debilidades en seguridad.

13.2. Gestión de incidentes y mejoras en la seguridad de la información.

13.2.1. Identificación de responsabilidades y procedimientos.

13.2.2. Evaluación de incidentes en seguridad.

13.2.3. Recogida de pruebas.

0 Comments Show recent to old
Post a comment

RSS of this page

Author: [aglone](#) Version: [1.1](#) Last Edited By: [aglone3](#) Modified: 27 - days ago

Información de contacto

servicios@iso27002.es

Quick Search

Navigate pages | Site Map

ISO 27002

05. Política de Seguridad

06. Organización de la Seguridad de Información

07. Gestión de Activos

08. Seguridad ligada a los Recursos Humanos

09. Seguridad Física y del Entorno

10. Gestión de Comunicaciones y Operaciones

11. Control de Accesos

12. Adquisición, Desarrollo y Mantenimiento de Sistemas de Información

13. Gestión de Incidentes de Seguridad de la Información

14. Gestión de Continuidad del Negocio

14 1 Aspectos de la gestión de continuidad del negocio

15. Conformidad

Objetivos

Contacto

Aviso Legal

[Site Home](#) >> 14. Gestión de Continuidad del Negocio

14. Gestión de Continuidad del Negocio



La estructura de este punto de la norma es:

[14.1. Aspectos de la gestión de continuidad del negocio.](#)

[14.1.1. Proceso de la gestión de continuidad del negocio.](#)

[14.1.2. Continuidad del negocio y análisis de impactos.](#)

[14.1.3. Redacción e implantación de planes de continuidad.](#)

[14.1.4. Marco de planificación para la continuidad del negocio.](#)

[14.1.5. Prueba, mantenimiento y reevaluación de planes de continuidad.](#)

0 Comments [Show recent to old](#)
[Post a comment](#)

[RSS of this page](#)

Author: [aglone](#) **Version:** [1.1](#) **Last Edited By:** [aglone3](#) **Modified:** 27 - days ago

Información de contacto

servicios@iso27002.es

Quick Search

- Navigate pages | Site Map
- ISO 27002
 - 05. Política de Seguridad
 - 06. Organización de la Seguridad de Información
 - 07. Gestión de Activos
 - 08. Seguridad ligada a los Recursos Humanos
 - 09. Seguridad Física y del Entorno
 - 10. Gestión de Comunicaciones y Operaciones
 - 11. Control de Accesos
 - 12. Adquisición, Desarrollo y Mantenimiento de Sistemas de Información
 - 13. Gestión de Incidentes de Seguridad de la Información
 - 14. Gestión de Continuidad del Negocio
 - 15. Conformidad**
 - 15 1 Conformidad con los requisitos legales
 - 15 2 Revisiones de la política de seguridad y de la conformidad técnica
 - 15 3 Consideraciones sobre la auditoría de sistemas
 - Objetivos
 - Contacto
 - Aviso Legal

Site Home » 15. Conformidad

15. Conformidad



15.1. Conformidad con los requisitos legales.

- [15.1.1. Identificación de la legislación aplicable.](#)
- [15.1.2. Derechos de propiedad intelectual \(IPR\).](#)
- [15.1.3. Salvaguarda de los registros de la Organización.](#)
- [15.1.4. Protección de datos de carácter personal y de la intimidad de las personas.](#)
- [15.1.5. Evitar mal uso de los dispositivos de tratamiento de la información.](#)
- [15.1.6. Reglamentación de los controles de cifrados.](#)

15.2. Revisiones de la política de seguridad y de la conformidad técnica.

- [15.2.1. Conformidad con la política de seguridad.](#)
- [15.2.2. Comprobación de la conformidad técnica.](#)

15.3. Consideraciones sobre la auditoría de sistemas.

- [15.3.1. Controles de auditoría de sistemas.](#)
- [15.3.2. Protección de las herramientas de auditoría de sistemas.](#)

0 Comments [Show recent to old](#)
[Post a comment](#)

RSS of this page

Author: [aglone](#) Version: [1.1](#) Last Edited By: [aglone3](#) Modified: 27 - days ago

Información de contacto

servicios@iso27002.es

Quick Search

Navigate pages | Site Map

ISO 27002

05. Política de Seguridad

06. Organización de la Seguridad de Información

07. Gestión de Activos

08. Seguridad ligada a los Recursos Humanos

09. Seguridad Física y del Entorno

10. Gestión de Comunicaciones y Operaciones

11. Control de Accesos

12. Adquisición, Desarrollo y Mantenimiento de Sistemas de Información

13. Gestión de Incidentes de Seguridad de la Información

14. Gestión de Continuidad del Negocio

15. Conformidad

Objetivos

Contacto

Aviso Legal

Site Home »

Objetivos

Objetivos

iso27002.es es una iniciativa privada que tiene como objetivo:

- Servir de punto de información de la serie de normas ISO 27000 y de la gestión de seguridad de la información mediante la aplicación de controles óptimos a las necesidades de las organizaciones en cada momento;
- Realizar la libre difusión de información en español en base a las investigaciones, conocimientos y búsquedas de los editores de la web;
- Responder a todas las consultas recibidas en relación a las normas de la serie ISO 27000, independientemente de su origen (empresas grandes, Pymes, organismos públicos, estudiantes, etc.;
- Establecer contactos con todo tipo de organizaciones, desarrolladores y personas relacionadas con la norma, con el objetivo de intercambiar informaciones, opiniones, experiencias o conocimientos, e impulsar la colaboración en actividades de fomento y promoción de las buenas prácticas para la aplicación de controles para la seguridad de la información.

Información de contacto

Interesados en ponerse en contacto con el gestor de contenidos:

servicios@iso27002.es

Petición de cuentas de usuario

El acceso para la gestión de contenidos de este portal no necesita de un alta previa de usuario.

Desde cada página se pueden realizar comentarios, sugerencias y aportaciones sobre las mejores prácticas y productos open source.

No se admiten prácticas en los comentarios de enlaces a productos comerciales o spam en los espacios dedicados a comentarios de los controles del wiki.

Interesados en apoyar el desarrollo de contenidos mediante prácticas comerciales de servicios o productos existen espacios dedicados previo contacto con:

servicios@iso27002.es

0 Comments

Show recent to old

Post a comment

RSS of this page

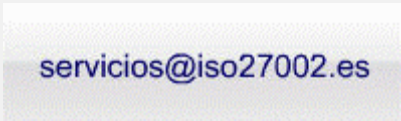
Author: aglone3

Version: 2.0

Last Edited By: aglone3

Modified: 7 - days ago

Información de contacto



Quick Search

- Navigate pages | Site Map
- ISO 27002

05. Política de Seguridad

06. Organización de la Seguridad de Información

07. Gestión de Activos

08. Seguridad ligada a los Recursos Humanos

09. Seguridad Física y del Entorno

10. Gestión de Comunicaciones y Operaciones

11. Control de Accesos

12. Adquisición, Desarrollo y Mantenimiento de Sistemas de Información

13. Gestión de Incidentes de Seguridad de la Información

14. Gestión de Continuidad del Negocio

15. Conformidad

Objetivos

Contacto

Aviso Legal

Site Home » Contacto

Contacto

Información de contacto

servicios@iso27002.es

0 Comments [Show recent to old](#)
[Post a comment](#)



RSS of this page

Author: [aglone3](#) Version: [2.0](#) Last Edited By: [aglone3](#) Modified: 9 - days ago

Información de contacto

servicios@iso27002.es

Quick Search

Navigate pages | Site Map

ISO 27002

05. Política de Seguridad

06. Organización de la Seguridad de Información

07. Gestión de Activos

08. Seguridad ligada a los Recursos Humanos

09. Seguridad Física y del Entorno

10. Gestión de Comunicaciones y Operaciones

11. Control de Accesos

12. Adquisición, Desarrollo y Mantenimiento de Sistemas de Información

13. Gestión de Incidentes de Seguridad de la Información

14. Gestión de Continuidad del Negocio

15. Conformidad

Objetivos

Contacto

Aviso Legal

Aviso Legal

1. Aviso legal y su aceptación.

El presente aviso legal (en adelante, "Aviso Legal") regula el uso del servicio de portal de Internet "iso27002.es" (en adelante, el "Portal") que sus legítimos titulares ponen a disposición de los usuarios de Internet. La utilización del Portal atribuye la condición de usuario del Portal (en adelante, el "Usuario") e implica la aceptación plena y sin reservas de todas y cada una de las disposiciones incluidas en este Aviso Legal en la versión publicada en el Portal en el momento en que el Usuario acceda al mismo. En consecuencia, el Usuario debe leer atentamente el Aviso Legal en cada una de las ocasiones en que se proponga utilizar el Portal, ya que éste puede sufrir modificaciones.

2. Objeto y Modificación de condiciones.

El Portal pone a disposición del Usuario la posibilidad de navegar, accediendo a sus contenidos y servicios siempre que lo haga de acuerdo con lo previsto en el presente Aviso Legal. En cualquier caso, el Portal se reserva el derecho de, en cualquier momento y sin necesidad de previo aviso, modificar o eliminar el contenido, estructura, diseño, servicios y condiciones de acceso y/o uso de este sitio, siempre que lo estime oportuno.

3. Principios Generales - Responsabilidad del Usuario.

El Usuario se obliga a utilizar los servicios y contenidos que le proporciona el Portal conforme a la legislación vigente y a los principios de buena fe y usos generalmente aceptados y a no contravenir con su actuación a través del Web el orden público. Por tanto, queda prohibido todo uso con fines ilícitos o que perjudiquen o impidan, puedan dañar y/o sobrecargar, de cualquier forma, la utilización y normal funcionamiento del Portal, o bien, que directa o indirectamente atenten contra el mismo o contra cualquier tercero. El Usuario no transmitirá a través del servicio nada que atente contra los valores y la dignidad de las personas, de acuerdo con las normas nacionales e internacionales de protección de los derechos humanos. Asimismo, queda prohibida la reproducción, distribución, transmisión, adaptación o modificación, por cualquier medio y en cualquier forma, de los contenidos del Portal (textos, diseños, gráficos, informaciones, bases de datos, archivos de sonido y/o imagen, logos,...) y demás elementos de este sitio, salvo autorización previa de sus legítimos titulares o cuando así resulte permitido por la ley. Se prohíbe asimismo respecto de los contenidos antes detallados, cualquier utilización comercial o publicitaria, distinta de la estrictamente permitida, en su caso, y la vulneración, en general, de cualquier derecho derivado de los mismos.

4. Condiciones que deberán cumplir los usuarios que quieran establecer un hiperenlace entre su página web y este Portal.

No se admite la reproducción de páginas del Portal mediante hiperenlace desde otro portal o página web, permitiéndose exclusivamente el acceso a dicho Portal. En ningún caso se podrá dar a entender que el Portal autoriza el hiperenlace o que ha supervisado o asumido de cualquier forma los servicios o contenidos ofrecidos por la web desde la que se produce el hiperenlace. No se podrán realizar manifestaciones o referencias falsas, incorrectas o inexactas sobre las páginas y servicios del Portal. La página desde donde se establece el hiperenlace no podrá tener ningún distintivo que haga referencia al Portal, exceptuando los signos integrados en el propio hiperenlace. Se prohíbe explícitamente la creación de cualquier tipo de "browser" o "border environment" sobre las páginas del Portal. No se podrán incluir contenidos contrarios a los derechos de terceros, ni contrarios a la moral y las buenas costumbres aceptadas, ni contenidos o informaciones ilícitas, en la página web desde la que se establezca el hiperenlace. La existencia de un hiperenlace entre una página web y este Portal no implica la existencia de relaciones entre el Portal y el propietario de esa página, ni la aceptación y aprobación de sus contenidos y servicios.

5. Uso de "cookies".

Cuando el Usuario navega a través del Portal, puede recibir en su ordenador "cookies" enviadas desde el servidor del Portal o desde el servidor de una tercera empresa contratada para la prestación del servicio de medición de audiencias. Si el Usuario desea conocer el servidor desde el que se han enviado estas "cookies", debe consultar las instrucciones de uso de su navegador. Si el Usuario admite la recepción de "cookies", debe saber que éstas no proporcionan ningún dato de carácter personal suyo y que la única finalidad es permitir que el servidor pueda reconocer el navegador utilizado por el Usuario con objeto de facilitar la navegación, además de conocer el número de usuarios únicos que acceden al Portal. El Usuario puede configurar su navegador para que éste le avise a través de la pantalla del ordenador de la recepción de "cookies". Asimismo, puede impedir la instalación de "cookies" en su ordenador. Para ello, debe consultar las instrucciones de uso de su navegador.

6. Exclusión de garantías y responsabilidades.

El Portal no se hace responsable directa ni indirecta o subsidiariamente de ningún daño o perjuicio sufrido por el Usuario derivado del acceso a dicho Portal o del uso de informaciones o aplicaciones en él contenidas. Se excluye la responsabilidad por los daños y perjuicios de toda naturaleza que puedan deberse a las informaciones contenidas en páginas web a las que este Portal pueda remitir a través de hiperenlaces. La finalidad de los hiperenlaces que aparecen en el Portal es puramente informativa, no siendo éste responsable en ningún caso del resultado que el Usuario pretenda obtener mediante el acceso a los mismos. Por consiguiente, el Portal no responderá por:

- a) La disponibilidad, accesibilidad y funcionamiento o continuidad de los sitios enlazados.b) La calidad, licitud, fiabilidad, utilidad, veracidad, vigencia, exhaustividad y/o autenticidad del contenido existente en los sitios enlazados.c) Del mantenimiento, prestación o transmisión de los contenidos existentes en los sitios enlazados.d) El Portal no tiene conocimiento efectivo de que la actividad o la información a la que remiten o recomiendan es ilícita o de que lesiona bienes o derechos de un tercero susceptibles de indemnización. En caso de tener conocimiento se actuará con la diligencia debida para suprimir o inutilizar el enlace correspondiente, tal y como establece la LSSICE.El Portal no será responsable de los daños y perjuicios de toda naturaleza que puedan deberse a la existencia de virus en el sistema informático, documentos electrónicos o ficheros del Usuario o por la presencia de virus en los servicios prestados por terceros a través del Portal.

7. Disputas ante los Tribunales.

Esta licencia de uso se rige por las leyes españolas independientemente del entorno legal del usuario. Cualquier disputa que pueda surgir en la interpretación de este acuerdo se resolverá en los tribunales españoles.

0 Comments [Show recent to old](#)
[Post a comment](#)



RSS of this page

Author: [aglone3](#) **Version:** [1.1](#) **Last Edited By:** [aglone3](#) **Modified:** 24 - days ago

Información de contacto

servicios@iso27002.es

Quick Search

- Navigate pages | Site Map
- ISO 27002
 - 05. Política de Seguridad
 - 06. Organización de la Seguridad de Información
 - 07. Gestión de Activos
 - 08. Seguridad ligada a los Recursos Humanos
 - 09. Seguridad Física y del Entorno**
 - 9 1 Áreas seguras
 - 9 2 Seguridad de los equipos
 - 10. Gestión de Comunicaciones y Operaciones
 - 11. Control de Accesos
 - 12. Adquisición, Desarrollo y Mantenimiento de Sistemas de Información
 - 13. Gestión de Incidentes de Seguridad de la Información
 - 14. Gestión de Continuidad del Negocio
 - 15. Conformidad
 - Objetivos
 - Contacto
 - Aviso Legal

09. Seguridad Física y del Entorno



La estructura de este punto de la norma es:

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 y recursos.](#)
- 9.1.4. [Protección contra amenazas externas y del entorno.](#)
- 9.1.5. [El trabajo en áreas seguras.](#)
- 9.1.6. [Áreas aisladas de carga y descarga.](#)

9.2. Seguridad de los equipos.

- 9.2.1. [Instalación y protección de equipos.](#)
- 9.2.2. [Suministro eléctrico.](#)
- 9.2.3. [Seguridad del cableado.](#)
- 9.2.4. [Mantenimiento de equipos.](#)
- 9.2.5. [Seguridad de equipos fuera de los locales de la Organización.](#)
- 9.2.6. [Seguridad en la reutilización o eliminación de equipos.](#)
- 9.2.7. [Traslado de activos.](#)

0 Comments [Show recent to old](#)
[Post a comment](#)

RSS of this page

Author: [aglone](#) Version: [1.2](#) Last Edited By: [aglone3](#) Modified: 26 - days ago

Información de contacto

servicios@iso27002.es

Quick Search

Navigate pages | Site Map

ISO 27002

05. Política de Seguridad

06. Organización de la Seguridad de Información

07. Gestión de Activos

08. Seguridad ligada a los Recursos Humanos

09. Seguridad Física y del Entorno

10. Gestión de Comunicaciones y Operaciones

11. Control de Accesos

12. Adquisición, Desarrollo y Mantenimiento de Sistemas de Información

13. Gestión de Incidentes de Seguridad de la Información

14. Gestión de Continuidad del Negocio

15. Conformidad

Objetivos

Contacto

Aviso Legal

Wiki Index

Show: **AII** | [A](#) | [B](#) | [C](#) | [D](#) | [E](#) | [F](#) | [G](#) | [H](#) | [I](#) | [J](#) | [K](#) | [L](#) | [M](#) | [N](#) | [O](#) | [P](#) | [Q](#) | [R](#) | [S](#) | [T](#) | [U](#) | [V](#) | [W](#) | [X](#) | [Y](#) | [Z](#)

- [05. Política de Seguridad](#)

► [08. Seguridad ligada a los Recursos Humanos](#)

► [10.1.2. Control de cambios operacionales](#)

► [10 1 Procedimientos y responsabilidades de operación](#)

► [10. 10. 3. Protección de los registros de incidencias](#)

► [10. 10. 6. Sincronización del reloj](#)

► [10.2.2. Monitorización y revisión de los servicios contratados](#)

► [10. 3. 1. Planificación de capacidades](#)

► [10. 4. 1. Medidas y controles contra software malicioso](#)

► [10. 5. 1. Recuperación de la información](#)

► [10. 6. 2. Seguridad en los servicios de red](#)

► [10. 7. 2. Eliminación de soportes](#)

► [10 7 Utilización y seguridad de los soportes de información](#)

► [10. 8. 3. Soportes físicos en tránsito](#)

► [10 8 Intercambio de información y software](#)

► [10 9 3 Seguridad en información pública](#)

► [11.1.1. Política de control de accesos](#)

► [11.2.2. Gestión de privilegios](#)

► [11 2 Gestión de acceso de usuario](#)

► [11.3.3. Políticas para escritorios y monitores sin información](#)

► [11.4.2. Autenticación de usuario para conexiones externas](#)

► [11.4.5. Segregación en las redes](#)

► [11 4 Control de acceso en red](#)

► [11.5.3. Sistema de gestión de contraseñas](#)

► [11.5.6. Limitación del tiempo de conexión](#)

► [11 6 2 Aislamiento de sistemas sensibles](#)

► [11.7.2. Tele trabajo](#)

► [12.1.1. Análisis y especificación de los requisitos de seguridad](#)

► [12.2.2. Control del proceso interno](#)

► [12 2 Seguridad de las aplicaciones del sistema](#)

► [12 3 Controles criptográficos](#)

► [12.4.3. Control de acceso a la librería de programas fuente](#)

► [12.5.2. Revisión técnica de los cambios en el sistema operativo](#)

► [12.5.5. Desarrollo externalizado del software](#)

► [12 6 Gestión de las vulnerabilidades técnicas](#)

► [13.1.2. Comunicación de debilidades en seguridad](#)

► [13.2.2. Evaluación de incidentes en seguridad](#)

► [13. Gestión de Incidentes de Seguridad de la Información](#)

► [14.1.3. Redacción e implantación de planes de continuidad](#)

► [14 1 Aspectos de la gestión de continuidad del negocio](#)

► [15.1.2. Derechos de propiedad intelectual \(IPR\)](#)

► [15.1.5. Evitar mal uso de los dispositivos de tratamiento de la información](#)

► [15.2.1. Conformidad con la política de seguridad](#)

► [06. Organización de la Seguridad de Información](#)

► [09. Seguridad Física y del Entorno](#)

► [10.1.3. Segregación de tareas](#)

► [10. 10. 1. Registro de incidencias](#)

► [10. 10. 4. Diarios de operación del administrador y operador](#)

► [10 10 Monitorización](#)

► [10.2.3. Gestión de los cambios en los servicios contratados](#)

► [10. 3. 2. Aceptación del sistema](#)

► [10. 4. 2. Medidas y controles contra código móvil](#)

► [10 5 Gestión interna de soportes y recuperación](#)

► [10 6 Gestión de redes](#)

► [10. 7. 3. Procedimientos de utilización de la información](#)

► [10. 8. 1. Políticas y procedimientos de intercambio de información](#)

► [10. 8. 4. Mensajería electrónica](#)

► [10. 9. 1. Seguridad en comercio electrónico](#)

► [10 9 Servicios de comercio electrónico](#)

► [11 1 Requerimientos de negocio para el control de accesos](#)

► [11.2.3. Gestión de contraseñas de usuario](#)

► [11.3.1. Uso de contraseña](#)

► [11 3 Responsabilidades del usuario](#)

► [11.4.3. Autenticación de nodos de la red](#)

► [11.4.6. Control de conexión a las redes](#)

► [11.5.1. Procedimientos de conexión de terminales](#)

► [11.5.4. Uso de los servicios del sistema](#)

► [11 5 Control de acceso al sistema operativo](#)

► [11 6 Control de acceso a las aplicaciones](#)

► [11 7 Informática móvil y tele trabajo](#)

► [12 1 Requisitos de seguridad de los sistemas](#)

► [12.2.3. Autenticación de mensajes](#)

► [12.3.1. Política de uso de los controles criptográficos](#)

► [12.4.1. Control del software en explotación](#)

► [12 4 Seguridad de los ficheros del sistema](#)

► [12.5.3. Restricciones en los cambios a los paquetes de software](#)

► [12 5 Seguridad en los procesos de desarrollo y soporte](#)

► [12. Adquisición, Desarrollo y Mantenimiento de Sistemas de Información](#)

► [13 1 Comunicación de eventos y debilidades en la seguridad de la información](#)

► [13.2.3. Recogida de pruebas](#)

► [14.1.1. Proceso de la gestión de continuidad del negocio](#)

► [14.1.4. Marco de planificación para la continuidad del negocio](#)

► [14. Gestión de Continuidad del Negocio](#)

► [15.1.3. Salvaguarda de los registros de la Organización](#)

► [15.1.6. Reglamentación de los controles de cifrados](#)

► [15.2.2. Comprobación de la conformidad técnica](#)

► [07. Gestión de Activos](#)

► [10.1.1. Documentación de procedimientos operativos](#)

► [10.1.4. Separación de los recursos para desarrollo y producción](#)

► [10. 10. 2. Supervisión del uso de los sistemas](#)

► [10. 10. 5. Registro de fallos](#)

► [10.2.1. Prestación de servicios](#)

► [10 2 Supervisión de los servicios contratados a terceros](#)

► [10 3 Planificación y aceptación del sistema](#)

► [10 4 Protección contra software malicioso y código móvil](#)

► [10. 6. 1. Controles de red](#)

► [10. 7. 1. Gestión de soportes extraíbles](#)

► [10. 7. 4. Seguridad de la documentación de sistemas](#)

► [10. 8. 2. Acuerdos de intercambio](#)

► [10. 8. 5. Sistemas de información empresariales](#)

► [10. 9. 2. Seguridad en transacciones en línea](#)

► [10. Gestión de Comunicaciones y Operaciones](#)

► [11.2.1. Registro de usuario](#)

► [11.2.4. Revisión de los derechos de acceso de los usuarios](#)

► [11.3.2. Equipo informático de usuario desatendido](#)

► [11.4.1. Política de uso de los servicios de red](#)

► [11.4.4. Protección a puertos de diagnóstico remoto](#)

► [11.4.7. Control de encaminamiento en la red](#)

► [11.5.2. Identificación y autenticación de usuario](#)

► [11.5.5. Desconexión automática de terminales](#)

► [11.6.1. Restricción de acceso a la información](#)

► [11 7 1 Informática móvil](#)

► [11. Control de Accesos](#)

► [12.2.1. Validación de los datos de entrada](#)

► [12.2.4. Validación de los datos de salida](#)

► [12.3.2. Cifrado](#)

► [12.4.2. Protección de los datos de prueba del sistema](#)

► [12.5.1. Procedimientos de control de cambios](#)

► [12.5.4. Canales encubiertos y código Troyano](#)

► [12.6.1. Control de las vulnerabilidades técnicas](#)

► [13 1 1 Comunicación de eventos en seguridad](#)

► [13.2.1. Identificación de responsabilidades y procedimientos](#)

► [13 2 Gestión de incidentes y mejoras en la seguridad de la información](#)

► [14.1.2. Continuidad del negocio y análisis de impactos](#)

► [14.1.5. Prueba, mantenimiento y reevaluación de planes de continuidad](#)

► [15.1.1. Identificación de la legislación aplicable](#)

► [15.1.4. Protección de datos de carácter personal y de la intimidad de las personas](#)

► [15 1 Conformidad con los requisitos legales](#)

► [15 2 Revisiones de la política de seguridad y de la conformidad técnica](#)

- ▶ [15.3.1. Controles de auditoria de sistemas](#)
- ▶ [15.3.2. Protección de las herramientas de auditoria de sistemas](#)
- ▶ [15 3 Consideraciones sobre la auditoría de sistemas](#)
- ▶ [15. Conformidad](#)
- ▶ [5.1.1 Documento de política de seguridad de la información](#)
- ▶ [5.1.2 Revisión de la política de seguridad de la información](#)
- ▶ [5 1 Política de seguridad de la información](#)
- ▶ [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](#)
- ▶ [6.1.4. Proceso de Autorización de Recursos para el Tratamiento de la Información](#)
- ▶ [6.1.5. Acuerdos de Confidencialidad](#)
- ▶ [6.1.6. Contacto con las Autoridades](#)
- ▶ [6.1.7. Contacto con Grupos de Interés Especial](#)
- ▶ [6.1.8. Revisión Independiente de la Seguridad de la Información](#)
- ▶ [6 1 Organización Interna](#)
- ▶ [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](#)
- ▶ [6 2 Terceros](#)
- ▶ [7.1.2. Responsable de los activos](#)
- ▶ [7 1 3 Acuerdos sobre el uso adecuado de los activos](#)
- ▶ [7.1.1. Inventario de Activos](#)
- ▶ [7.2.1 Directrices de Clasificación](#)
- ▶ [7 2 Clasificación de la Información](#)
- ▶ [8.1.1. Inclusión de la seguridad en las responsabilidades laborales](#)
- ▶ [8.1.2. Selección y política de personal](#)
- ▶ [8.1.3. Términos y condiciones de la relación laboral](#)
- ▶ [8 1 Seguridad en la definición del trabajo y los recursos](#)
- ▶ [8.2.1. Supervisión de las obligaciones](#)
- ▶ [8.2.2. Formación y capacitación en seguridad de la información](#)
- ▶ [8.2.3. Procedimiento disciplinario](#)
- ▶ [8 2 Seguridad en el desempeño de las funciones del empleo](#)
- ▶ [8.3.1. Cese de responsabilidades](#)
- ▶ [8.3.2. Restitución de activos](#)
- ▶ [8.3.3. Cancelación de permisos de acceso](#)
- ▶ [8 3 Finalización o cambio del puesto de trabajo](#)
- ▶ [9.1.1. Perímetro de seguridad física](#)
- ▶ [9.1.2. Controles físicos de entrada](#)
- ▶ [9.1.3. Seguridad de oficinas, despachos y recursos](#)
- ▶ [9.1.4. Protección contra amenazas externas y del entorno](#)
- ▶ [9.1.5. El trabajo en áreas seguras](#)
- ▶ [9.1.6. Áreas aisladas de carga y descarga](#)
- ▶ [9 1 Áreas seguras](#)
- ▶ [9.2.1. Instalación y protección de equipos](#)
- ▶ [9.2.2. Suministro eléctrico](#)
- ▶ [9 2 5 Seguridad de equipos fuera de los locales de la Organización](#)
- ▶ [9.2.3. Seguridad del cableado](#)
- ▶ [9.2.4. Mantenimiento de equipos](#)
- ▶ [9 2 Seguridad de los equipos](#)
- ▶ [9.2.6. Seguridad en la reutilización o eliminación de equipos](#)
- ▶ [9.2.7. Traslado de activos](#)
- ▶ [Aviso Legal](#)
- ▶ [Contacto](#)
- ▶ [ISO 27002](#)
- ▶ [Objetivos](#)

Información de contacto

servicios@iso27002.es

Quick Search

- Navigate pages | Site Map
- ISO 27002

05. 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

06. Organización de la Seguridad de Información

07. Gestión de Activos

08. Seguridad ligada a los Recursos Humanos

09. Seguridad Física y del Entorno

10. Gestión de Comunicaciones y Operaciones

11. Control de Accesos

12. Adquisición, Desarrollo y Mantenimiento de Sistemas de Información

13. Gestión de Incidentes de Seguridad de la Información

14. Gestión de Continuidad del Negocio

15. Conformidad





Objetivos

Contacto

Aviso Legal

5 1 Política de seguridad de la información



 <div>Objetivo</div>	Proporcionar la guía y apoyo de la Dirección para la seguridad de la información en relación a los requisitos del negocio y a las leyes y regulaciones relevantes.
 <div>Principios</div>	La Dirección debería establecer una política clara y en línea con los objetivos del negocio y demostrar su apoyo y compromiso con la seguridad de la información mediante la publicación y mantenimiento de una política de seguridad de la información para toda la organización.
	<p>Piense en términos de un manual o wiki de políticas de seguridad de la información que contenga un conjunto coherente e internamente consistente de políticas, normas, procedimientos y directrices.</p> <p>Determine la frecuencia de revisión de la política de seguridad de la información y las formas de comunicación a toda la organización.</p> <p>La revisión de la idoneidad y adecuación de la política de seguridad de la información puede ser incluida en las revisiones de la dirección.</p>
	Cobertura de la política (es decir, porcentaje de secciones de ISO/IEC 27001/2 para las cuales se han especificado, escrito, aprobado y publicado políticas y sus normas, procedimientos y directrices asociadas. Grado de despliegue y adopción de la política en la organización (medido por auditoría, gerencia o auto-evaluación).

0 Comments [Show recent to old](#)
[Post a comment](#)

[Attachments \(2\)](#)

 [RSS of this page](#)

Author: [aglone](#) Version: [1.6](#) Last Edited By: [aglone3](#) Modified: 26 - days ago

Información de contacto

servicios@iso27002.es

Quick Search

Navigate pages | Site Map

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

Site Home » 05. Política de Seguridad » 5 1 Política de seguridad de la información » 5.1.1 Documento de política de seguridad de la información

5.1.1 Documento de política de seguridad de la información



Control:

La Dirección debería aprobar y publicar un documento de la política de seguridad de la información y comunicar la política a todos los empleados y las partes externas relevantes.

Posibles Soluciones a este control:

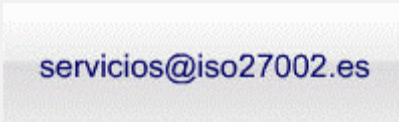
ISO27000.es	Relación de diferentes referencias para el desarrollo de políticas de seguridad de la información y plantillas	ISO27000.es - Herramientas
	Elementos a considerar en una política de seguridad. Manual de políticas de seguridad Plantilla de una política de seguridad (libre descarga-inglés)	Elementos Manual Declaración de la Política

0 Comments [Show recent to old](#)
[Post a comment](#)

RSS of this page

Author: [aglonge](#) Version: [2.4](#) Last Edited By: [javier ruiz](#) Modified: 2 - days ago

Información de contacto



Quick Search

Navigate pages | Site Map

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

Site Home

>>

05. Política de Seguridad

>>

5 1 Política de seguridad de la información

>>

5.1.2 Revisión de la política de seguridad de la información

5.1.2 Revisión de la política de seguridad de la información



Control:

La política de seguridad de la información se debería revisar a intervalos planificados (o en caso que se produzcan cambios significativos) para garantizar que es adecuada, eficaz y suficiente.


(consultar 6.1.8)

(consultar 6.1.8 y 15.2.1)

(consultar 13.1)

(consultar 6.1.6)

Posibles Soluciones a este control:

callio.gif 	Plantilla del proceso de revisión de la política de seguridad (libre descarga-inglés)	Callio Technologies
--	--	-------------------------------------

0 Comments

Show recent to old

Post a comment

 RSS of this page

Author: [aglone](#)

Version: [1.3](#)

Last Edited By: [aglone3](#)

Modified: 27 - days ago






Información de contacto



Quick Search

- Navigate pages | Site Map
- ISO 27002
 - 05. Política de Seguridad
 - 06. Organización de la Seguridad de Información
 - 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
 - 6.1.4. Proceso de Autorización de Recursos para el Tratamiento de la Información
 - 6.1.5. Acuerdos de Confidencialidad
 - 6.1.6. Contacto con las Autoridades
 - 6.1.7. Contacto con Grupos de Interés Especial
 - 6.1.8. Revisión Independiente de la Seguridad de la Información
 - 6 2 Terceros
 - 07. Gestión de Activos
 - 08. Seguridad ligada a los Recursos Humanos
 - 09. Seguridad Física y del Entorno
 - 10. Gestión de Comunicaciones y Operaciones
 - 11. Control de Accesos
 - 12. Adquisición, Desarrollo y Mantenimiento de Sistemas de Información
 - 13. Gestión de Incidentes de Seguridad de la Información
 - 14. Gestión de Continuidad del Negocio
 - 15. Conformidad
 - Objetivos
 - Contacto
 - Aviso Legal

6 1 Organización Interna

	<h1>Espacio de Patrocinio disponible</h1>
	Gestionar la seguridad de la información dentro de la Organización.
	<p>Se debería establecer una estructura de gestión con objeto de iniciar y controlar la implantación de la seguridad de la información dentro de la Organización.</p> <p>El órgano de dirección debería aprobar la política de seguridad de la información, asignar los roles de seguridad y coordinar y revisar la implantación de la seguridad en toda la Organización.</p> <p>Si fuera necesario, en la Organización se debería establecer y facilitar el acceso a una fuente especializada de consulta en seguridad de la información. Deberían desarrollarse contactos con especialistas externos en seguridad, que incluyan a las administraciones pertinentes, con objeto de mantenerse actualizado en las tendencias de la industria, la evolución de las normas y los métodos de evaluación, así como proporcionar enlaces adecuados para el tratamiento de las incidencias de seguridad.</p> <p>Debería fomentarse un enfoque multidisciplinario de la seguridad de la información, que, por ejemplo, implique la cooperación y la colaboración de directores, usuarios, administradores, diseñadores de aplicaciones, auditores y el equipo de seguridad con expertos en áreas como la gestión de seguros y la gestión de riesgos.</p>
	Reproduzca la estructura y tamaño de otras funciones corporativas especializadas, como Legal, Riesgos y Compliance.
	<p>Porcentaje de funciones/unidades organizativas para las cuales se ha implantado una estrategia global para mantener los riesgos de seguridad de la información por debajo de umbrales explícitamente aceptados por la dirección.</p> <p>Porcentaje de empleados que han (a) recibido y (b) aceptado formalmente, roles y responsabilidades de seguridad de la información.</p>

0 Comments [Show recent to old](#)
[Post a comment](#)

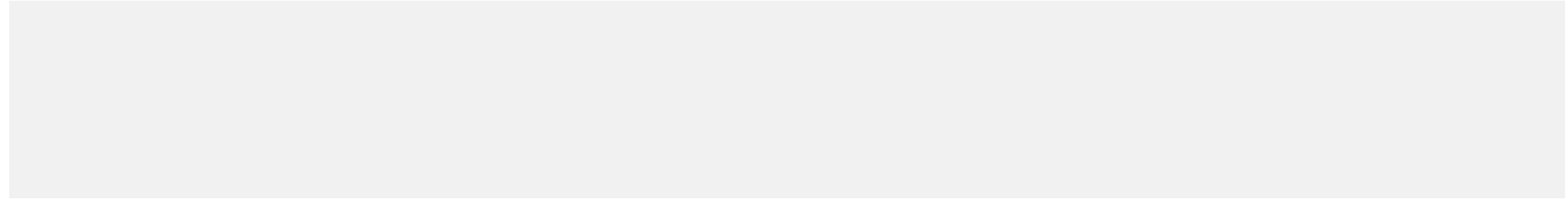
[Attachments \(2\)](#)

 [RSS of this page](#)

Author: [aglone](#) Version: [1.4](#) Last Edited By: [aglone3](#) Modified: 26 - days ago

Información de contacto

servicios@iso27002.es



Quick Search

- Navigate pages | Site Map
- 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

6.1.4. Proceso de Autorización de Recursos para el Tratamiento de la Información

6.1.5. Acuerdos de Confidencialidad

6.1.6. Contacto con las Autoridades

6.1.7. Contacto con Grupos de Interés Especial

6.1.8. Revisión Independiente de la Seguridad de la Información

Site Home » 06. Organización de la Seguridad de Información » 6 1 Organización Interna » 6.1.1. Compromiso de la Dirección con la Seguridad de la Información

6.1.1. Compromiso de la Dirección con la Seguridad de la Información



Control:

Los miembros de la Dirección deberían respaldar activamente las iniciativas de seguridad demostrando su claro apoyo y compromiso, asignando y aprobando explícitamente las responsabilidades en seguridad de la información dentro de la Organización.

(consultar 6.1.2)

Posibles Soluciones a este control:

Espacio pendiente de posibles aportaciones.

0 Comments Show recent to old
Post a comment

RSS of this page

Author: aglone Version: 1.1 Last Edited By: aglone3 Modified: 30 - days ago

Información de contacto

servicios@iso27002.es

Quick Search

- Navigate pages | Site Map
- 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

6.1.4. Proceso de Autorización de Recursos para el Tratamiento de la Información

6.1.5. Acuerdos de Confidencialidad

6.1.6. Contacto con las Autoridades

6.1.7. Contacto con Grupos de Interés Especial

6.1.8. Revisión Independiente de la Seguridad de la Información

Site Home » 06. Organización de la Seguridad de Información » 6 1 Organización Interna » 6.1.2. Coordinación de la Seguridad de la Información


6.1.2. Coordinación de la Seguridad de la Información



Control:

Las actividades para la seguridad de la información deberían ser coordinadas por representantes que posean de cierta relevancia en su puesto y funciones y de los distintos sectores que forman la Organización.

Posibles Soluciones a este control:

callio.gif 	Plantilla para el registro de los miembros del grupo para la gestión de la seguridad (libre descarga-inglés)	Callio Technologies
--	---	-------------------------------------

0 Comments [Show recent to old](#)
[Post a comment](#)

 RSS of this page

Author: [aglone](#) Version: [1.1](#) Last Edited By: [aglone3](#) Modified: 30 - days ago

Información de contacto

servicios@iso27002.es

Quick Search

- Navigate pages | Site Map
- 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

6.1.4. Proceso de Autorización de Recursos para el Tratamiento de la Información

6.1.5. Acuerdos de Confidencialidad

6.1.6. Contacto con las Autoridades

6.1.7. Contacto con Grupos de Interés Especial

6.1.8. Revisión Independiente de la Seguridad de la Información

Site Home » 06. Organización de la Seguridad de Información » 6 1 Organización Interna » 6.1.3. Asignación de responsabilidades

6.1.3. Asignación de responsabilidades



Control:

Se deberían definir claramente todas las responsabilidades para la seguridad de la información.

(consultar también 7.1.2)

Posibles Soluciones a este control:

Callio Technologies	Plantilla en inglés de definición de responsabilidades de un asesor o responsable de seguridad de la información.	-Information+Security+Advisor.doc
ASIS International	Guía en inglés que analiza las responsabilidades, competencias y perfil profesional de un CSO (Chief Security Officer).	Chief Security Officer (CSO) Guideline

0 Comments Show recent to old
Post a comment

RSS of this page

Author: [aglone](#) Version: [1.2](#) Last Edited By: [javier ruiz](#) Modified: 8 - days ago

Información de contacto

servicios@iso27002.es

Quick Search

- Navigate pages | Site Map
- 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

6.1.4. Proceso de Autorización de Recursos para el Tratamiento de la Información

6.1.5. Acuerdos de Confidencialidad

6.1.6. Contacto con las Autoridades

6.1.7. Contacto con Grupos de Interés Especial

6.1.8. Revisión Independiente de la Seguridad de la Información

Site Home » 06. Organización de la Seguridad de Información » 6 1 Organización Interna » 6.1.4. Proceso de Autorización de Recursos para el Tratamiento de la Información

6.1.4. Proceso de Autorización de Recursos para el Tratamiento de la Información



Control:

Se debería definir y establecer un proceso de gestión de autorizaciones para los nuevos recursos de tratamiento de la información.

Posibles Soluciones a este control:

FFIEC	Guía del FFIEC (Federal Financial Institutions Examination Council), en inglés, sobre cómo implantar un proceso de desarrollo y adquisición de TI eficaz en una organización. La acompaña una lista de verificación -checklist-, útil para auditar dicho proceso.	FFIEC D&A IT Handbook FFIEC Audit of D_A workprogram
-------	---	---

0 Comments

Show recent to old

Post a comment

RSS of this page

Author: [aglonge](#)

Version: [1.2](#)

Last Edited By: [javier_ruiz](#)

Modified: 7 - days ago

Información de contacto

servicios@iso27002.es

Quick Search

- Navigate pages | Site Map
- 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

6.1.4. Proceso de Autorización de Recursos para el Tratamiento de la Información

6.1.5. Acuerdos de Confidencialidad

6.1.6. Contacto con las Autoridades

6.1.7. Contacto con Grupos de Interés Especial

6.1.8. Revisión Independiente de la Seguridad de la Información

6.1.5. Acuerdos de Confidencialidad



Control:

Se deberían identificar y revisar regularmente en los acuerdos aquellos requisitos de confidencialidad o no divulgación que contemplan las necesidades de protección de la información de la Organización.

([consultar también 15.1.1](#))

Posibles Soluciones a este control:

Espacio pendiente de posibles aportaciones.

0 Comments [Show recent to old](#)
[Post a comment](#)

RSS of this page

Author: [aglone](#) Version: [1.4](#) Last Edited By: [aglone3](#) Modified: 30 - days ago

Información de contacto

servicios@iso27002.es

Quick Search

- Navigate pages | Site Map
- 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

6.1.4. Proceso de Autorización de Recursos para el Tratamiento de la Información

6.1.5. Acuerdos de Confidencialidad

6.1.6. Contacto con las Autoridades

6.1.7. Contacto con Grupos de Interés Especial

6.1.8. Revisión Independiente de la Seguridad de la Información

6.1.6. Contacto con las Autoridades



Control:

Se deberían mantener los contactos apropiados con las autoridades pertinentes.

Posibles Soluciones a este control:

	El GDT está creado para perseguir los delitos informáticos. Si Vd. identifica un problema de seguridad en la red, localiza un contenido ilícito o cree haber detectado u observado una conducta que pudiera ser delictiva, puede comunicarlo al GDT. Todo lo que en ella se recibe es tratado con la máxima discreción.	Guardia Civil
	La Agencia de Protección de Datos tiene por objetivo velar por el cumplimiento de la legislación sobre protección de datos y controlar su aplicación, en especial en lo relativo a los derechos de información, acceso, rectificación, oposición y cancelación de datos.	ADPG
	La piratería de software es la copia o distribución no autorizada de software con copyright. Puede hacerse copiando, descargando, compartiendo, vendiendo o instalando múltiples copias en ordenadores personales o de trabajo. Lo que mucha gente no advierte o no sabe es que cuando se compra software, realmente se está comprando una licencia para usarlo, no el software en sí. Esa licencia es la que le dice cuántas veces puede instalar el software, por lo que es importante leerla. Si hace más copias del software de las permitidas por la licencia, está pirateando.	BSA
Logo.gif 	CCN-CERT es la Capacidad de Respuesta a incidentes de Seguridad de la Información del Centro Criptológico Nacional (CCN), dependiente del Centro Nacional de Inteligencia (CNI). Este servicio se creó a principios de 2007 como CERT gubernamental español y está presente en los principales foros internacionales en los que se comparte objetivos, ideas e información sobre la seguridad de forma global.	CNI
	INTECO tiene encomendadas a través del Plan Avanza las misiones de sentar las bases de coordinación de distintas iniciativas públicas en torno a la seguridad informática, impulsar la investigación aplicada y la formación especializada en el ámbito de la seguridad en el uso de las TIC y convertirse en el Centro de Referencia en Seguridad Informática a nivel nacional.	INTECO

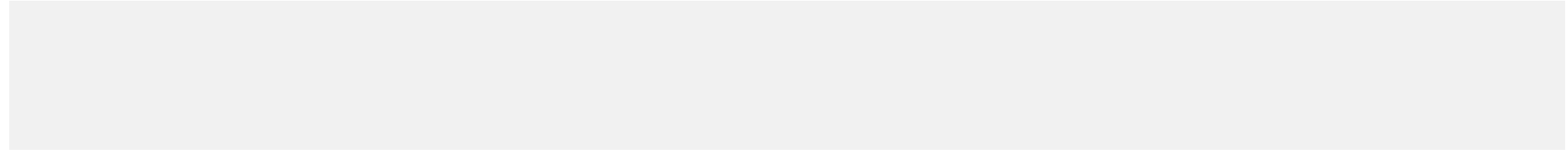
0 Comments [Show recent to old](#)
[Post a comment](#)

RSS of this page

Author: [aglone](#) Version: [1.1](#) Last Edited By: [aglone3](#) Modified: 30 - days ago

Información de contacto

servicios@iso27002.es



Quick Search

- Navigate pages | Site Map
- 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

6.1.4. Proceso de Autorización de Recursos para el Tratamiento de la Información

6.1.5. Acuerdos de Confidencialidad

6.1.6. Contacto con las Autoridades

6.1.7. Contacto con Grupos de Interés Especial

6.1.8. Revisión Independiente de la Seguridad de la Información

6.1.7. Contacto con Grupos de Interés Especial



Control:

Se debería mantener el contacto con grupos o foros de seguridad especializados y asociaciones profesionales.

(consultar también 13.2.1).

Posibles Soluciones a este control:

	McAfee Consumer Threat Alerts warn you about the most dangerous downloads, poisonous pop-ups and suspicious spam so you can stay ahead of the cyberscammers, and keep your PC and personal information safe. Sign up for the free alerts by filling out the information below.	McAfee Alerts
	International in scope and free for public use, CWE™ provides a unified, measurable set of software weaknesses that is enabling more effective discussion, description, selection, and use of software security tools and services that can find these weaknesses in source code and operational systems as well as better understanding and management of software weaknesses related to architecture and design.	CWE
	Información actualizada y muy completa sobre aquellas amenazas de Internet que están activas, y explica cómo evitarlas. El portal incluye diferentes secciones con artículos informativos y análisis, blogs, una enciclopedia de seguridad informática y descripciones de malware, así como un amplio glosario de términos.	Kaspersky Alerts
	Consejos de seguridad para el uso seguro del ordenador y de la información sensible y personal.	Alertas ESET
	La “Oficina de Seguridad del Internauta” (OSI) es un servicio del Gobierno para proporcionar la información y el soporte necesarios para evitar y resolver los problemas de seguridad que pueden afectarnos al navegar por Internet. Nuestro objetivo es elevar la cultura de seguridad, prevenir, concienciar y formar proporcionando información clara y concisa acerca de la tecnología y el estado de la seguridad en Internet. Al mismo tiempo impulsamos la detección y denuncia de nuevas amenazas en la red, de fraudes, estafas online o de cualquier otro tipo de ataque de Seguridad Informática.	OSI

0 Comments

Show recent to old

Post a comment

RSS of this page

Author: [aglone](#)

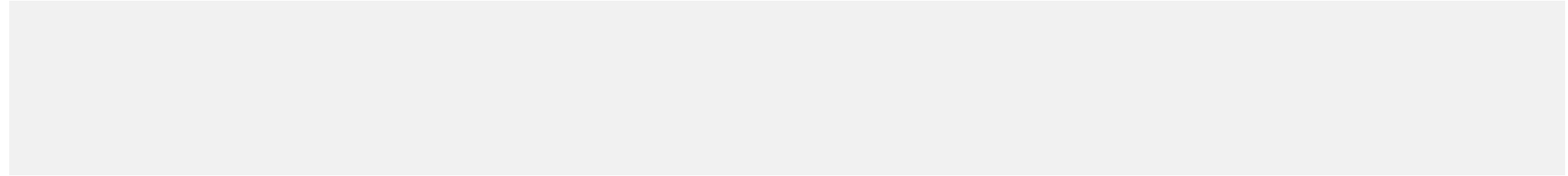
Version: [1.2](#)

Last Edited By: [aglone3](#)

Modified: 30 - days ago

Información de contacto

servicios@iso27002.es



Quick Search

- Navigate pages | Site Map
- 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

6.1.4. Proceso de Autorización de Recursos para el Tratamiento de la Información

6.1.5. Acuerdos de Confidencialidad

6.1.6. Contacto con las Autoridades

6.1.7. Contacto con Grupos de Interés Especial

6.1.8. Revisión Independiente de la Seguridad de la Información

Site Home » 06. Organización de la Seguridad de Información » 6 1 Organización Interna » 6.1.8. Revisión Independiente de la Seguridad de la Información

6.1.8. Revisión Independiente de la Seguridad de la Información



Control:

Se deberían revisar las prácticas de la Organización para la gestión de la seguridad de la información y su implantación (por ej., objetivos de control, políticas, procesos y procedimientos de seguridad) de forma independiente y a intervalos planificados o cuando se produzcan cambios significativos para la seguridad de la información.

(consultar 5.1.1)

Posibles Soluciones a este control:

	ISMS auditing guideline.	iso27001security
	This procedure includes planning, execution, reporting and follow–up of an internal ISMS audit and applies to all departments that form part of the company information security management system.	iso27001security
	La Herramienta de Evaluación de Seguridad de Microsoft (MSAT) es una herramienta gratuita diseñada para ayudar a las organizaciones de menos de 1.000 empleados a evaluar los puntos débiles de su entorno de seguridad de TI. Presenta un listado de cuestiones ordenadas por prioridad así como orientación específica para minimizar esos riesgos.	TechCenter de seguridad
	The Symantec Small Business Check-up enables small businesses to benchmark themselves against survey results from 700 small businesses across Europe, the Middle East and Africa (EMEA).	Symantec Small Business Check-up

0 Comments [Show recent to old](#)
[Post a comment](#)

RSS of this page

Author: [aglone](#) Version: [1.1](#) Last Edited By: [aglone3](#) Modified: 30 - days ago


Información de contacto

servicios@iso27002.es





Quick Search

- Navigate pages | Site Map
- ISO 27002
 - 05. Política de Seguridad
 - 06. Organización de la Seguridad de Información
 - 6 1 Organización Interna
 - 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
 - 07. Gestión de Activos
 - 08. Seguridad ligada a los Recursos Humanos
 - 09. Seguridad Física y del Entorno
 - 10. Gestión de Comunicaciones y Operaciones
 - 11. Control de Accesos
 - 12. Adquisición, Desarrollo y Mantenimiento de Sistemas de Información
 - 13. Gestión de Incidentes de Seguridad de la Información
 - 14. Gestión de Continuidad del Negocio
 - 15. Conformidad
 - Objetivos
 - Contacto
 - Aviso Legal

6 2 Terceros



Espacio de Patrocinio disponible

 Objetivo	Mantener la seguridad de que los recursos de tratamiento de la información y de los activos de información de la organización sean accesibles por terceros..
 Principios	<p>La seguridad de la información de la organización y las instalaciones de procesamiento de la información no debería ser reducida por la introducción de un servicio o producto externo.</p> <p>Debería controlarse el acceso de terceros a los dispositivos de tratamiento de información de la organización.</p> <p>Cuando el negocio requiera dicho acceso de terceros, se debería realizar una evaluación del riesgo para determinar sus implicaciones sobre la seguridad y las medidas de control que requieren. Estas medidas de control deberían definirse y aceptarse en un contrato con la tercera parte.</p>
	<p>Haga inventario de conexiones de red y flujos de información significativos con 3as partes, evalúe sus riesgos y revise los controles de seguridad de información existentes respecto a los requisitos. ¡Esto puede dar miedo, pero es 100% necesario!</p> <p>Considere exigir certificados en ISO/IEC 27001 a los partners más críticos, tales como outsourcing de TI, proveedores de servicios de seguridad TI, etc.</p>
	Porcentaje de conexiones con terceras partes que han sido identificadas, evaluadas en cuanto a su riesgo y estimadas como seguras.

0 Comments [Show recent to old](#)
[Post a comment](#)

[Attachments \(2\)](#)

 [RSS of this page](#)

Author: [aglone](#) Version: [1.4](#) Last Edited By: [aglone3](#) Modified: 26 - days ago

Información de contacto

servicios@iso27002.es

Quick Search

- Navigate pages | [Site Map](#)
- 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

Site Home

»

06. Organización de la Seguridad de Información

»

6 2 Terceros

»6.2.1. Identificación de los riesgos derivados del acceso de terceros

6.2.1. Identificación de los riesgos derivados del acceso de terceros




Control:

Se deberían identificar los riesgos a la información de la organización y a las instalaciones del procesamiento de información de los procesos de negocio que impliquen a terceros y se deberían implementar controles apropiados antes de conceder el acceso.

([6.2.3](#) y [6.2.3](#)).

Posibles Soluciones a este control:

	Cisco Systems is offering these ASP security evaluation criteria as a step toward mitigating the risks of outsourcing to ASPs(Application Service Providers). These criteria are specific measurements of an ASP's security posture and maturity.	Cisco ASP evaluation
---	--	--------------------------------------

0 Comments

[Show recent to old](#)

[Post a comment](#)



RSS of this page

Author: [aglone](#)

Version: [1.1](#)

Last Edited By: [aglone3](#)

Modified: 30 - days ago

Información de contacto

servicios@iso27002.es

Quick Search

- Navigate pages | Site Map
- 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

Site Home » 06. Organización de la Seguridad de Información » 6 2 Terceros » 6.2.2. Tratamiento de la seguridad en la relación con los clientes

6.2.2. Tratamiento de la seguridad en la relación con los clientes



Control:

Se deberían anexar todos los requisitos identificados de seguridad antes de dar a los clientes acceso a la información o a los activos de la organización.

([consultar 15.1](#))

([consultar 15.1.2.](#))

([consultar 6.1.5](#)).

([consultar 6.2.1.](#)).

Posibles Soluciones a este control:

Espacio pendiente de posibles aportaciones.

0 Comments [Show recent to old](#)
[Post a comment](#)

RSS of this page

Author: [aglone](#) Version: [1.1](#) Last Edited By: [aglone3](#) Modified: 30 - days ago

Información de contacto

servicios@iso27002.es

Quick Search

Navigate pages | Site Map

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

Site Home » 06. Organización de la Seguridad de Información » 6 2 Terceros » 6.2.3. Tratamiento de la seguridad en contratos con terceros

6.2.3. Tratamiento de la seguridad en contratos con terceros



Control:

Los acuerdos con terceras partes que implican el acceso, proceso, comunicación o gestión de la información de la organización o de las instalaciones de procesamiento de información o la adición de productos o servicios a las instalaciones, deberían cubrir todos los requisitos de seguridad relevantes.

([consultar 6.2.1](#))

([consultar 10.4.1](#))

([consultar 6.1.5](#))

([consultar 7.2.1](#))


([consultar 15.1](#))

([consultar 15.1.2](#))

([consultar 6.1.5](#))

([consultar 6.2.1](#))

Posibles Soluciones a este control:

	Política de referencia para la externalización dentro del contexto de un SGSI	Outsourcing security policy
---	---	---

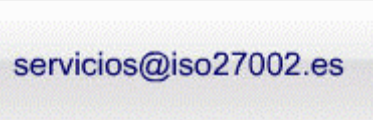
0 Comments [Show recent to old](#)

[Post a comment](#)

 RSS of this page

Author: [aglone](#) Version: [1.1](#) Last Edited By: [aglone3](#) Modified: 30 - days ago

Información de contacto



Quick Search

- Navigate pages | Site Map
- ISO 27002

05. Política de Seguridad

06. Organización de la Seguridad de Información

07. Gestión de Activos

7 1 Responsabilidad sobre los activos

7.1.1. Inventario de Activos

7.1.2. Responsable de los activos

7 1 3 Acuerdos sobre el uso adecuado de los activos

7 2 Clasificación de la Información

08. Seguridad ligada a los Recursos Humanos

09. Seguridad Física y del Entorno

10. Gestión de Comunicaciones y Operaciones

11. Control de Accesos

12. Adquisición, Desarrollo y Mantenimiento de Sistemas de Información

13. Gestión de Incidentes de Seguridad de la Información

14. Gestión de Continuidad del Negocio


15. Conformidad

Objetivos





Contacto

Aviso Legal

7 1 Responsabilidad sobre los activos



Espacio de Patrocinio disponible

 <div>Objetivo</div>	Alcanzar y mantener una protección adecuada de los activos de la Organización
 <div>Principios</div>	<p>Todos los activos deberían ser justificados y tener asignado un propietario.</p> <p>Se deberían identificar a los propietarios para todos los activos y asignarles la responsabilidad del mantenimiento de los controles adecuados. La implantación de controles específicos podría ser delegada por el propietario convenientemente. No obstante, el propietario permanece como responsable de la adecuada protección de los activos.</p> <p>El término “propietario” identifica a un individuo o entidad responsable, que cuenta con la aprobación del órgano de dirección, para el control de la producción, desarrollo, mantenimiento, uso y seguridad de los activos. El término “propietario” no significa que la persona disponga de los derechos de propiedad reales del activo.</p>
	<p>Elabore y mantenga un inventario de activos de información (similar al preparado en su día para el Efecto 2000), mostrando los propietarios de los activos (directivos o gestores responsables de proteger sus activos) y los detalles relevantes (p. ej., ubicación, nº de serie, nº de versión, estado de desarrollo / pruebas / producción, etc.).</p> <p>Use códigos de barras para facilitar las tareas de realización de inventario y para vincular equipos de TI que entran y salen de las instalaciones con empleados.</p>
	<p>Porcentaje de activos de información en cada fase del proceso de clasificación (identificado / inventariado / propietario asignado / riesgo evaluado / clasificado / asegurado).</p> <p>Porcentaje de activos de información claves para los cuales se ha implantado una estrategia global para mitigar riesgos de seguridad de la información según sea necesario y para mantener dichos riesgos en niveles aceptables.</p>

0 Comments [Show recent to old](#)
[Post a comment](#)

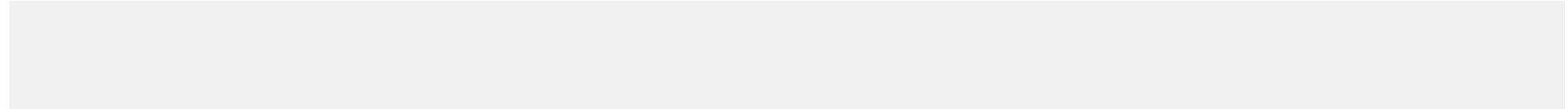
[Attachments \(2\)](#)

 [RSS of this page](#)

Author: [aglone](#) Version: [1.4](#) Last Edited By: [aglone3](#) Modified: 26 - days ago

Información de contacto

servicios@iso27002.es



Quick Search

Navigate pages | Site Map

7 1 Responsabilidad sobre los activos

7.1.1. Inventario de Activos

7.1.2. Responsable de los activos

7 1 3 Acuerdos sobre el uso adecuado de los activos

Site Home » 07. Gestión de Activos » 7 1 Responsabilidad sobre los activos » 7.1.1. Inventario de Activos

7.1.1. Inventario de Activos






Control:

Todos los activos deberían estar claramente identificados, confeccionando y manteniendo un inventario con los más importantes.

(consultar 7.1.2)

(consultar 7.2)

Posibles Soluciones a este control:

	Spiceworks is the complete network management & monitoring, helpdesk, PC inventory & software reporting solution to manage Everything IT in small and medium businesses.	Spiceworks
logo.png 	Paglo is on-demand tool. Businesses can discover all their IT information and get instant answers to their computer, network, and security questions.	Paglo
callio.gif 	Plantilla de inventario de activos manual en hoja excel (libre descarga-inglés)	Callio Technologies

0 Comments [Show recent to old](#)
[Post a comment](#)

 [RSS of this page](#)

Author: [aglone](#) Version: [1.1](#) Last Edited By: [aglone3](#) Modified: 27 - days ago

Información de contacto

servicios@iso27002.es

Quick Search

- Navigate pages | Site Map
- 7 1 Responsabilidad sobre los activos

7.1.1. Inventario de Activos

7.1.2. Responsable de los activos

7 1 3 Acuerdos sobre el uso adecuado de los activos

Site Home » 07. Gestión de Activos » 7 1 Responsabilidad sobre los activos » 7.1.2. Responsable de los activos


7.1.2. Responsable de los activos



Control:

Toda la información y activos asociados a los recursos para el tratamiento de la información deberían pertenecer a una parte designada de la Organización.

Posibles Soluciones a este control:

callio.gif 	Plantilla para la gestión de roles y responsabilidades asociadas a los activos (libre descarga- inglés)	Callio Technologies
--	--	-------------------------------------

0 Comments [Show recent to old](#)
[Post a comment](#)

 RSS of this page

Author: [aglone](#) Version: [1.1](#) Last Edited By: [aglone3](#) Modified: 27 - days ago

Información de contacto

servicios@iso27002.es

Quick Search

Navigate pages | Site Map

7 1 Responsabilidad sobre los activos

- 7.1.1. Inventario de Activos
- 7.1.2. Responsable de los activos
- 7 1 3 Acuerdos sobre el uso adecuado de los activos**

7 1 3 Acuerdos sobre el uso adecuado de los activos



Control:

Se deberían identificar, documentar e implantar regulaciones para el uso adecuado de la información y los activos asociados a recursos de tratamiento de la información.

(consultar 10.8)

(consultar 11.7.1)

Posibles Soluciones a este control:

	Guía para proteger y usar de forma segura su móvil	Guía INTECO
--	--	-----------------------------

0 Comments [Show recent to old](#)
[Post a comment](#)

Attachments (1)

RSS of this page

Author: [aglone](#) Version: [1.2](#) Last Edited By: [aglone3](#) Modified: 27 - days ago


Información de contacto

servicios@iso27002.es





Quick Search

- Navigate pages | Site Map
- ISO 27002
 - 05. Política de Seguridad
 - 06. Organización de la Seguridad de Información
 - 07. Gestión de Activos
 - 7 1 Responsabilidad sobre los activos
 - 7 2 Clasificación de la Información**
 - 7.2.1 Directrices de Clasificación
 - 7.2.2 Marcado y tratamiento de la información
 - 08. Seguridad ligada a los Recursos Humanos
 - 09. Seguridad Física y del Entorno
 - 10. Gestión de Comunicaciones y Operaciones
 - 11. Control de Accesos
 - 12. Adquisición, Desarrollo y Mantenimiento de Sistemas de Información
 - 13. Gestión de Incidentes de Seguridad de la Información
 - 14. Gestión de Continuidad del Negocio
 - 15. Conformidad
 - Objetivos
 - Contacto
 - Aviso Legal

7 2 Clasificación de la Información



Espacio de Patrocinio disponible

 Objetivo	Asegurar que se aplica un nivel de protección adecuado a la información.
 Principios	<p>Se debería clasificar la información para indicar la necesidad, prioridades y nivel de protección previsto para su tratamiento.</p> <p>La información tiene diversos grados de sensibilidad y criticidad. Algunos ítems podrían requerir niveles de protección adicionales o de un tratamiento especial. Debería utilizarse un esquema de clasificación de la información para definir el conjunto adecuado de niveles de protección y comunicar la necesidad de medidas especiales para el tratamiento.</p>
	<p>¡Mantenga la sencillez! Distinga los requisitos de seguridad básicos (globales) de los avanzados, de acuerdo con el riesgo.</p> <p>Comience quizás con la confidencialidad, pero no olvide los requisitos de integridad y disponibilidad.</p>
	Porcentaje de activos de información en cada categoría de clasificación (incluida la de "aún sin clasificar").

0 Comments [Show recent to old](#)
[Post a comment](#)

[Attachments](#) (2)

 [RSS of this page](#)

Author: [aglone](#) Version: [1.4](#) Last Edited By: [aglone3](#) Modified: 26 - days ago

Información de contacto

servicios@iso27002.es

Quick Search

- Navigate pages | Site Map
- 7 2 Clasificación de la Información

7.2.1 Directrices de Clasificación

7.2.2 Marcado y tratamiento de la información

Site Home » 07. Gestión de Activos » 7 2 Clasificación de la Información » 7.2.1 Directrices de Clasificación

7.2.1 Directrices de Clasificación



Control:

La información debería clasificarse en relación a su valor, requisitos legales, sensibilidad y criticidad para la Organización.

(consultar 11.1.1)

(consultar 7.1.2)

(consultar 10.7.2)

Posibles Soluciones a este control:

callio.gif	Plantilla con clasificación de la informacion de 3 y de 4 niveles (libre descarga-inglés)	Callio Technologies
	MEHARI 2010 : Guide de l'analyse des enjeux et de la classification	MEHARI

0 Comments [Show recent to old](#)
[Post a comment](#)

RSS of this page

Author: [aglone](#) Version: [1.1](#) Last Edited By: [aglone3](#) Modified: 27 - days ago

Información de contacto

servicios@iso27002.es

Quick Search

- Navigate pages | Site Map
- 7 2 Clasificación de la Información

7.2.1 Directrices de Clasificación

7.2.2 Marcado y tratamiento de la información

Site Home » 07. Gestión de Activos » 7 2 Clasificación de la Información » 7.2.2 Marcado y tratamiento de la información

7.2.2 Marcado y tratamiento de la información



Control:

Se debería desarrollar e implantar un conjunto apropiado de procedimientos para el etiquetado y tratamiento de la información, de acuerdo con el esquema de clasificación adoptado por la Organización.

(consultar 7.2.1)

Posibles Soluciones a este control:

Espacio pendiente de posibles aportaciones.

0 Comments Show recent to old
Post a comment

RSS of this page

Author: [aglone](#) Version: [1.1](#) Last Edited By: [aglone3](#) Modified: 27 - days ago

Información de contacto


servicios@iso27002.es

Quick Search




- Navigate pages | Site Map
- ISO 27002
 - 05. Política de Seguridad
 - 06. Organización de la Seguridad de Información
 - 07. Gestión de Activos
 - 08. Seguridad ligada a los Recursos Humanos
 - 8 1 Seguridad en la definición del trabajo y los recursos**
 - 8.1.1. Inclusión de la seguridad en las responsabilidades laborales
 - 8.1.2. Selección y política de personal
 - 8.1.3. Términos y condiciones de la relación laboral
 - 8 2 Seguridad en el desempeño de las funciones del empleo
 - 8 3 Finalización o cambio del puesto de trabajo
 - 09. Seguridad Física y del Entorno
 - 10. Gestión de Comunicaciones y Operaciones
 - 11. Control de Accesos
 - 12. Adquisición, Desarrollo y Mantenimiento de Sistemas de Información
 - 13. Gestión de Incidentes de Seguridad de la Información
 - 14. Gestión de Continuidad del Negocio
 - 15. Conformidad
 - Objetivos
 - Contacto
 - Aviso Legal

Site Home » 08. Seguridad ligada a los Recursos Humanos » 8 1 Seguridad en la definición del trabajo y los recursos

8 1 Seguridad en la definición del trabajo y los recursos



Espacio de Patrocinio disponible

	Asegurar que los empleados, contratistas y usuarios de terceras partes entiendan sus responsabilidades y sean aptos para las funciones que desarrollen. Reducir el riesgo de robo, fraude y mal uso de las instalaciones y medios.
	<p>Las responsabilidades de la seguridad se deberían definir antes de la contratación laboral mediante la descripción adecuada del trabajo y los términos y condiciones del empleo.</p> <p>Todos los candidatos para el empleo, los contratistas y los usuarios de terceras partes se deberían seleccionar adecuadamente, especialmente para los trabajos sensibles.</p> <p>Los empleados, contratistas y usuarios de terceras partes de los servicios de procesamiento de la información deberían firmar un acuerdo sobre sus funciones y responsabilidades con relación a la seguridad.</p>
	<p>Conjuntamente con RRHH, asegure que se emplea un proceso de verificación de antecedentes proporcional a la clasificación de seguridad de aquella información a la que va a acceder el empleado a contratar.</p> <p>Dicho simplemente, el proceso de contratación de un administrador de sistemas TI debería ser muy diferente del de un administrativo. Haga comprobaciones de procedencia, formación, conocimientos, etc.</p>
	Porcentaje de nuevos empleados o pseudo-empleados (contratistas, consultores, temporales, etc.) que hayan sido totalmente verificados y aprobados de acuerdo con las políticas de la empresa antes de comenzar a trabajar.

0 Comments

Show recent to old

Post a comment

Attachments (2)

RSS of this page

Author: [aglone](#) Version: [1.4](#) Last Edited By: [aglone3](#) Modified: 26 - days ago

Información de contacto

servicios@iso27002.es

Powered by [Zoho Wiki](#) | [Zoho](#) | [Report Abuse](#) | [Wiki Index](#) | [Site Map](#) | [Help](#) | [Feedback](#) | [Jump Start with 2 Free Wikis](#) | [Sign in](#)

http://iso27002.wiki.zoho.com/8-1-Seguridad-en-la-definición-del-trabajo-y-los-recursos.html[28/01/2011 08:16:56 p.m.]

Quick Search

Navigate pages | Site Map

8 1 Seguridad en la definición del trabajo y los recursos

8.1.1. Inclusión de la seguridad en las responsabilidades laborales

8.1.2. Selección y política de personal

8.1.3. Términos y condiciones de la relación laboral

Site Home » 08. Seguridad ligada a los Recursos Humanos » 8 1 Seguridad en la definición del trabajo y los recursos » 8.1.1.

Inclusión de la seguridad en las responsabilidades laborales

8.1.1. Inclusión de la seguridad en las responsabilidades laborales



Espacio de Patrocinio disponible

Control:

Se deberían definir y documentar los roles y responsabilidades de la seguridad de los empleados, contratistas y terceros en concordancia con la política de seguridad de la información de la organización.

(consultar 5.1)

Posibles Soluciones a este control:

<div>callio.gif</div> <div></div>	Diversas Plantillas relacionadas (inglés)	<div>Elementos de la descripción de trabajo</div> <div>Modelo de descripción de funciones</div> <div>Ejemplo 1: Descripción Asesor de Seguridad</div> <div>Ejemplo 2: Descripciones de posiciones y funciones en seguridad</div>
--	---	--

0 Comments

Show recent to old

Post a comment



RSS of this page

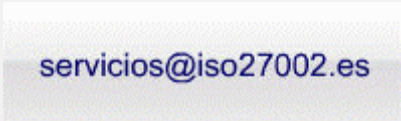
Author: [aglone](#)

Version: [1.1](#)

Last Edited By: [aglone3](#)

Modified: 27 - days ago

Información de contacto



Quick Search

- Navigate pages | Site Map
- 8 1 Seguridad en la definición del trabajo y los recursos

8.1.1. Inclusión de la seguridad en las responsabilidades laborales

8.1.2. Selección y política de personal

8.1.3. Términos y condiciones de la relación laboral

🌐 Site Home » 08. Seguridad ligada a los Recursos Humanos » 8 1 Seguridad en la definición del trabajo y los recursos » 8.1.2.

Selección y política de personal

8.1.2. Selección y política de personal



Control:

Se deberían realizar revisiones de verificación de antecedentes de los candidatos al empleo, contratistas y terceros y en concordancia con las regulaciones, ética y leyes relevantes y deben ser proporcionales a los requerimientos del negocio, la clasificación de la información a la cual se va a tener acceso y los riesgos percibidos.

Posibles Soluciones a este control:

<div>callio.gif</div> <div>?</div>	Diversas Plantillas relacionadas (inglés).	Relación para el chequeo de referencias Autorización previa al chequeo de referencias
<div>BSI SHOP</div>	Security screening of individuals employed in a security environment. Code of practice.	BS 7858:2006+A2:2009
<div>ASIS International</div>	Guía en inglés de cómo realizar comprobaciones de antecedentes a la hora de contratar personal.	Screening guideline

0 Comments

Show recent to old

Post a comment

RSS of this page

Author: [aglone](#)

Version: [1.2](#)

Last Edited By: [javier_ruiz](#)

Modified: 8 - days ago

Información de contacto

servicios@iso27002.es

Quick Search

- Navigate pages | Site Map
- 8 1 Seguridad en la definición del trabajo y los recursos

8.1.1. Inclusión de la seguridad en las responsabilidades laborales

8.1.2. Selección y política de personal

8.1.3. Términos y condiciones de la relación laboral

Site Home » 08. Seguridad ligada a los Recursos Humanos » 8 1 Seguridad en la definición del trabajo y los recursos » 8.1.3.

Términos y condiciones de la relación laboral

8.1.3. Términos y condiciones de la relación laboral



Control:

Como parte de su obligación contractual, empleados, contratistas y terceros deberían aceptar y firmar los términos y condiciones del contrato de empleo, el cual establecerá sus obligaciones y las obligaciones de la organización para la seguridad de información.

(consultar también 7.2.1 y 10.7.3)

(consultar también 9.2.5 y 11.7.1)

(consultar 8.2.3)

(consultar 8.3)

Posibles Soluciones a este control:

<div>callio.gif</div> <div></div>	<div>Diversas Plantillas relacionadas (inglés)</div>	<div>Acuerdo de Confidencialidad</div> <div>Ejemplo 1: acuerdo de confidencialidad</div> <div>Ejemplo 2: acuerdo de no revelación</div> <div>Contrato del personal</div>
-----------------------------------	--	--

0 Comments

Show recent to old

Post a comment

RSS of this page

Author: [aglone](#)

Version: [1.1](#)

Last Edited By: [aglone3](#)

Modified: 27 - days ago






Información de contacto

servicios@iso27002.es

Quick Search

- Navigate pages | Site Map
- ISO 27002
 - 05. Política de Seguridad
 - 06. Organización de la Seguridad de Información
 - 07. Gestión de Activos
 - 08. Seguridad ligada a los Recursos Humanos
 - 8 1 Seguridad en la definición del trabajo y los recursos
 - 8 2 Seguridad en el desempeño de las funciones del empleo**
 - 8.2.1. Supervisión de las obligaciones
 - 8.2.2. Formación y capacitación en seguridad de la información
 - 8.2.3. Procedimiento disciplinario
 - 8 3 Finalización o cambio del puesto de trabajo
 - 09. Seguridad Física y del Entorno
 - 10. Gestión de Comunicaciones y Operaciones
 - 11. Control de Accesos
 - 12. Adquisición, Desarrollo y Mantenimiento de Sistemas de Información
 - 13. Gestión de Incidentes de Seguridad de la Información
 - 14. Gestión de Continuidad del Negocio
 - 15. Conformidad
 - Objetivos
 - Contacto
 - Aviso Legal

8 2 Seguridad en el desempeño de las funciones del empleo

	Espacio de Patrocinio disponible
	Asegurar que los empleados, contratistas y terceras partes son conscientes de las amenazas de seguridad, de sus responsabilidades y obligaciones y que están equipados para cumplir con la política de seguridad de la organización en el desempeño de sus labores diarias, para reducir el riesgo asociado a los errores humanos.
	<p>Se debería definir las responsabilidades de la Dirección para garantizar que la seguridad se aplica en todos los puestos de trabajo de las personas de la organización.</p> <p>A todos los usuarios empleados, contratistas y terceras personas se les debería proporcionar un adecuado nivel de concienciación, educación y capacitación en procedimientos de seguridad y en el uso correcto de los medios disponibles para el procesamiento de la información con objeto de minimizar los posibles riesgos de seguridad.</p> <p>Se debería establecer un proceso disciplinario normal para gestionar las brechas en seguridad.</p>
	<p>La responsabilidad con respecto a la protección de la información no finaliza cuando un empleado se va a casa o abandona la organización. Asegure que esto se documenta claramente en materiales de concienciación, contratos de empleo, etc.</p> <p>Contemple la posibilidad de una revisión anual por RRHH de los contratos junto con los empleados para refrescar las expectativas expuestas en los términos y condiciones de empleo, incluyendo su compromiso con la seguridad de la información.</p>
	Respuesta a las actividades de concienciación en seguridad medidas por (por ejemplo) el número de e-mails y llamadas relativas a iniciativas de concienciación individuales.

0 Comments [Show recent to old](#)
[Post a comment](#)

[Attachments \(2\)](#)

 [RSS of this page](#)

Author: [aglone](#) Version: [1.5](#) Last Edited By: [aglone3](#) Modified: 26 - days ago

Información de contacto

servicios@iso27002.es

Quick Search

Navigate pages | Site Map

8 2 Seguridad en el desempeño de las funciones del empleo

8.2.1. Supervisión de las obligaciones

8.2.2. Formación y capacitación en seguridad de la información

8.2.3. Procedimiento disciplinario

Site Home » 08. Seguridad ligada a los Recursos Humanos » 8 2 Seguridad en el desempeño de las funciones del empleo » 8.2.1. Supervisión de las obligaciones

8.2.1. Supervisión de las obligaciones



Espacio de Patrocinio disponible

Control:

La Dirección debería requerir a empleados, contratistas y usuarios de terceras partes aplicar la seguridad en concordancia con las políticas y los procedimientos establecidos de la organización.

(consultar 8.2.2)

Posibles Soluciones a este control:

<div>callio.gif</div> <div></div>	Diversas Plantillas relacionadas (inglés)	<div>Relación para la supervisión del personal</div> <div>Formulario de supervision del personal</div>
--	---	--

0 Comments

Show recent to old

Post a comment



RSS of this page

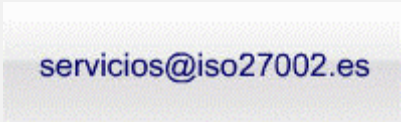
Author: aglone

Version: 1.1

Last Edited By: aglone3

Modified: 27 - days ago

Información de contacto



Quick Search

Navigate pages | Site Map

8 2 Seguridad en el desempeño de las funciones del empleo

8.2.1. Supervisión de las obligaciones

8.2.2. Formación y capacitación en seguridad de la información

8.2.3. Procedimiento disciplinario

8.2.2. Formación y capacitación en seguridad de la información



Control:

Todos los empleados de la organización y donde sea relevante, contratistas y usuarios de terceros deberían recibir entrenamiento apropiado del conocimiento y actualizaciones regulares en políticas y procedimientos organizacionales como sean relevantes para la función de su trabajo.

(consultar 8.2.3)

(consultar 13.1)

Posibles Soluciones a este control:

	Curso introductorio gratuito de 20h. a los Sistemas de Gestión de la Seguridad de la Información (SGSI) según la norma UNE-ISO/IEC 27001. Se darán a conocer los conceptos básicos necesarios para introducir al usuario en la gestión de la Seguridad de la Información, así como conocer la dimensión y alcance que suponen la implantación, certificación y mantenimiento de un Sistema de Gestión de Seguridad de la Información en una Organización, en base a la norma ISO/IEC 27001.	Inteco.es
	The business value of ISO27k: case_study for senior managers. This case is derived from a presentation by the Managing Director of "serviceCo", an IT services company, to an audience of information security and IT audit specialist.	iso27001security
	This kit includes a planning guide, templates, pointers to material can that can help speed the development of a security awareness program, a sample general security awareness presentation that can be modified and tailored to any organization, material to help articulate the value to peers and managers, and three example awareness campaigns from Microsoft Information Security.	Microsoft Security Awareness Toolkit
	Un LMS es un programa (aplicación de software) instalado en un servidor, que se emplea para administrar, distribuir y controlar las actividades de formación no presencial o e-Learning de una institución u organización.	Learning Management systems
	Incluye contenido de muestra sobre concienciación utilizado en todo el mundo para ayudar a reconocer y responder a problemas de seguridad y protección. Este contenido se ha utilizado en programas de la comunidad, en escuelas, empresas industriales y en línea a través de staysafe.org. Puede emplear este material como ejemplo o directamente en sus propios programas internos de concienciación.	TechCenter de seguridad
	InfoSec Institute's Enterprise Security Awareness for Software Developers highlights the important subject areas and best practices of secure coding. An emphasis is placed on the most common threats to applications, as well as language or architecture-specific remediation. There are three formats of the course available: * Security Awareness for .NET/C#/VB developers, * Security Awareness for J2EE/Java developers, * Security Awareness for C/C++ developers.	InfoSec Institute
	MindfulSecurity.com is a personal website created, owned and maintained by Paul Johnson. This site is primarily designed as a resource for businesses seeking materials and ideas for raising the information security awareness levels of their employees and workers.	mindfulsecurity
	En esta página la AEPD pone a disposición de los ciudadanos información, consejos así como recursos y materiales para fomentar una participación segura en las múltiples posibilidades que hoy nos ofrece Internet.	Agencia Protección de Datos
	Formación en qué consiste y cómo informar de Incidentes de seguridad. Sirve como modelo de formación útil a implantar internamente por una organización. IQS dispone de material diverso de demostración y tambien para su adquisición y traducción al español.	ISO

0 Comments Show recent to old Post a comment

RSS of this page

Author: [aglone](#) Version: [1.1](#) Last Edited By: [aglone3](#) Modified: 27 - days ago

Información de contacto

servicios@iso27002.es

Quick Search

- Navigate pages | Site Map
- 8 2 Seguridad en el desempeño de las funciones del empleo
 - 8.2.1. Supervisión de las obligaciones
 - 8.2.2. Formación y capacitación en seguridad de la información
 - 8.2.3. Procedimiento disciplinario**

 [Site Home](#) » [08. Seguridad ligada a los Recursos Humanos](#) » [8 2 Seguridad en el desempeño de las funciones del empleo](#) »

8.2.3. Procedimiento disciplinario

8.2.3. Procedimiento disciplinario



Control:

Debería existir un proceso formal disciplinario para empleados que produzcan brechas en la seguridad.

([consultar 13.2.3](#))

Posibles Soluciones a este control:

Espacio pendiente de posibles aportaciones.

0 Comments [Show recent to old](#)
[Post a comment](#)

 [RSS of this page](#)

Author: [aglone](#) **Version:** [1.1](#) **Last Edited By:** [aglone3](#) **Modified:** 27 - days ago

Información de contacto


servicios@iso27002.es

Quick Search





Navigate pages | Site Map

- ISO 27002
- 05. Política de Seguridad
- 06. Organización de la Seguridad de Información
- 07. Gestión de Activos
- 08. Seguridad ligada a los Recursos Humanos
 - 8 1 Seguridad en la definición del trabajo y los recursos
 - 8 2 Seguridad en el desempeño de las funciones del empleo
 - 8 3 Finalización o cambio del puesto de trabajo**
 - 8.3.1. Cese de responsabilidades
 - 8.3.2. Restitución de activos
 - 8.3.3. Cancelación de permisos de acceso
- 09. Seguridad Física y del Entorno
- 10. Gestión de Comunicaciones y Operaciones
- 11. Control de Accesos
- 12. Adquisición, Desarrollo y Mantenimiento de Sistemas de Información
- 13. Gestión de Incidentes de Seguridad de la Información
- 14. Gestión de Continuidad del Negocio
- 15. Conformidad
- Objetivos
- Contacto
- Aviso Legal

8 3 Finalización o cambio del puesto de trabajo



Espacio de Patrocinio disponible

 Objetivo	Garantizar que los empleados, contratistas y terceras personas abandonan la organización o cambian de empleo de forma organizada.
 Principios	<p>Se deberían establecer las responsabilidades para asegurar que el abandono de la organización por parte de los empleados, contratistas o terceras personas se controla, que se devuelve todo el equipamiento y se eliminan completamente todos los derechos de acceso.</p> <p>Los cambios en las responsabilidades y empleos en la organización se deberían manejar, en el caso de su finalización en línea con esta sección, y para el caso de nuevos empleos como se describe en la sección 8.1.</p>
	<p><u>Véase Sección 7.1.</u> La devolución de los activos de la organización cuando un empleado se marcha sería mucho más sencilla de verificar si el inventario de activos ha sido actualizado y verificado regularmente.</p> <p>Examine qué accesos necesita revocar en primer lugar cuando un empleado presenta su carta de dimisión: ¿cuáles son los sistemas más críticos o vulnerables?.</p> <p>Haga un seguimiento del uso del e-mail por estas personas antes de salir definitivamente de la empresa, por si comienzan a sacar información confidencial (sujeto a las políticas aplicables y a consideraciones legales sobre privacidad).</p>
	Porcentaje de identificadores de usuario pertenecientes a personas que han dejado la organización, separados por las categorías de activos (pendientes de desactivación) e inactivos (pendientes de archivo y borrado).

0 Comments [Show recent to old](#)
[Post a comment](#)

[Attachments](#) (2)

 [RSS of this page](#)

Author: [aglone](#) Version: [1.7](#) Last Edited By: [aglone3](#) Modified: 26 - days ago

Información de contacto

servicios@iso27002.es

Quick Search

Navigate pages | Site Map

8 3 Finalización o cambio del puesto de trabajo

- 8.3.1. Cese de responsabilidades
- 8.3.2. Restitución de activos
- 8.3.3. Cancelación de permisos de acceso

Site Home » 08. Seguridad ligada a los Recursos Humanos » 8 3 Finalización o cambio del puesto de trabajo » 8.3.1. Cese de responsabilidades

8.3.1. Cese de responsabilidades



Control:

Las responsabilidades para ejecutar la finalización de un empleo o el cambio de éste deberían estar claramente definidas y asignadas.

(consultar 6.1.5)

(consultar 8.1.3)

(sección 8.1)

Posibles Soluciones a este control:

Espacio pendiente de posibles aportaciones.

0 Comments Show recent to old
Post a comment

RSS of this page

Author: aglone Version: 1.1 Last Edited By: aglone3 Modified: 27 - days ago

Información de contacto

servicios@iso27002.es

Quick Search

Navigate pages | Site Map

8 3 Finalización o cambio del puesto de trabajo

8.3.1. Cese de responsabilidades

8.3.2. Restitución de activos

8.3.3. Cancelación de permisos de acceso

Restitución de activos

8.3.2. Restitución de activos



Control:

Todos los empleados, contratistas y terceros deberían devolver todos los activos de la organización que estén en su posesión a la finalización de su empleo, contrato o acuerdo.

Guía:

El proceso de finalización debería estar formalizado para incluir el retorno previo de los software, documentos corporativos y equipos.

Otros activos de la organización como dispositivos móviles de compute, tarjetas de crédito, tarjetas de acceso, manuales, software e información guardada en medios electrónicos, también necesitan ser devueltos.

En casos donde el empleado, contratista o tercero compra el equipo de la organización o usa su propio equipo, se debería seguir procedimientos para asegurar que toda la información relevante es transferida a la organización y borrado con seguridad del equipo ([consultar 10.7.1](#)).

En casos donde un empleado, contratista o tercero tiene conocimiento que es importante para las operaciones en curso, esa información debe ser documentada y transferida a la organización.

Posibles Soluciones a este control:

Espacio pendiente de posibles aportaciones.

0 Comments [Show recent to old](#)
[Post a comment](#)

RSS of this page

Author: [aglone](#) Version: [1.1](#) Last Edited By: [aglone3](#) Modified: 27 - days ago

Información de contacto

servicios@iso27002.es

Quick Search

Navigate pages | Site Map

8 3 Finalización o cambio del puesto de trabajo

8.3.1. Cese de responsabilidades

8.3.2. Restitución de activos

8.3.3. Cancelación de permisos de acceso

Cancelación de permisos de acceso

8.3.3. Cancelación de permisos de acceso



Control:

Se deberían retirar los derechos de acceso para todos los empleados, contratistas o usuarios de terceros a la información y a las instalaciones del procesamiento de información a la finalización del empleo, contrato o acuerdo, o ser revisada en caso de cambio.

Guía:

Tras la finalización, se deberían reconsiderar los derechos de acceso de un individuo a los activos asociados con los sistemas de información y a los servicios. Esto determinara si es necesario retirar los derechos de acceso.

Los cambios en un empleo deberían reflejarse en la retirada de todos los derechos de acceso que no sean aprobados para el nuevo empleo.

Los derechos de acceso deberían ser retirados o adaptados, incluyendo acceso físico y lógico, llaves, tarjetas de identificación, instalaciones del proceso de información ([consultar 11.2.4](#)), subscripciones y retirada de cualquier documentación que los identifica como un miembro actual de la organización.

Si un empleado, contratista o usuario de tercero saliente ha sabido contraseñas para activos restantes de las cuentas, deberían ser cambiadas hasta la finalización o cambio del empleo, contrato o acuerdo.

Los derechos de acceso para activos de información y equipos se deberían reducir o retirar antes que el empleo termine o cambie, dependiendo de la evaluación de los factores de riesgo como:

- a) si la finalización o cambio es iniciado por el empleado, contratista o usuario de tercero, o por la gerencia y la razón de la finalización;
- b) las responsabilidades actuales del empleado u otro usuario;
- c) el valor de los activos a los que se accede actualmente.

Información adicional:

En ciertas circunstancias los derechos de acceso pueden ser asignados en base a la disponibilidad hacia más personas que el empleado, contratista o usuario de tercero saliente.

En estas circunstancias, los individuos salientes deberían ser removidos de cualquier lista de grupos de acceso y se deben realizar arreglos para advertir a los demás empleados, contratistas y usuarios de terceros involucrados de no compartir esta información con la persona saliente.

En casos de gerencia terminada, contrariedad con los empleados, contratistas o usuarios de terceros pueden llevar a corromper información deliberadamente o a sabotear las instalaciones del procesamiento de información.

En casos de renuncia de personal, estos pueden ser tentados a recolectar información para usos futuros.

Posibles Soluciones a este control:

Espacio pendiente de posibles aportaciones.

0 Comments [Show recent to old](#)
[Post a comment](#)

RSS of this page

Author: [aglone](#) Version: [1.1](#) Last Edited By: [aglone3](#) Modified: 27 - days ago

Información de contacto

servicios@iso27002.es

Quick Search

- Navigate pages | Site Map
- ISO 27002

05. Política de Seguridad

06. Organización de la Seguridad de Información

07. Gestión de Activos

08. Seguridad ligada a los Recursos Humanos

09. Seguridad Física y del Entorno

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 y recursos

9.1.4. Protección contra amenazas externas y del entorno

9.1.5. El trabajo en áreas seguras

9.1.6. Áreas aisladas de carga y descarga

9 2 Seguridad de los equipos

10. Gestión de Comunicaciones y Operaciones

11. Control de Accesos

12. Adquisición, Desarrollo y Mantenimiento de Sistemas de Información

13. Gestión de Incidentes de Seguridad de la Información

14. Gestión de Continuidad del Negocio


15. Conformidad

Objetivos





Contacto

Aviso Legal

9 1 Áreas seguras



Espacio de Patrocinio disponible

 <div>Objetivo</div>	Evitar el acceso físico no autorizado, daños o intromisiones en las instalaciones y a la información de la organización.
 <div>Principios</div>	Los servicios de procesamiento de información sensible deberían ubicarse en áreas seguras y protegidas en un perímetro de seguridad definido por barreras y controles de entrada adecuados. Estas áreas deberían estar protegidas físicamente contra accesos no autorizados, daños e interferencias. La protección suministrada debería estar acorde con los riesgos identificados.
	<p>El estándar parece centrarse en el CPD pero hay muchas otras áreas vulnerables a considerar, p. ej., armarios de cableado, "servidores departamentales" y archivos (recuerde: los estándares se refieren a asegurar la información, no sólo las TI).</p> <p>Examine la entrada y salida de personas a/de su organización. ¿Hasta dónde podría llegar el repartidor de pizza o el mensajero sin ser parado, identificado y acompañado? ¿Qué podrían ver, llevarse o escuchar mientras están dentro?</p> <p>Algunas organizaciones usan tarjetas de identificación de colores para indicar las áreas accesibles por los visitantes (p. ej., azul para la 1ª planta, verde para la 3ª, etc.; ahora, si ve a alguien con una identificación verde en la 4º planta, reténgalo).</p> <p>Asegúrese de retirar todos los pases de empleado y de visita cuando se vayan. Haga que los sistemas de acceso con tarjeta rechacen y alarmen ante intentos de acceso. Use pases de visita que se vuelvan opacos o muestren de alguna manera que ya no son válidos a las x horas de haberse emitido.</p>
	Informes de inspecciones periódicas de seguridad física de instalaciones, incluyendo actualización regular del estado de medidas correctivas identificadas en inspecciones previas que aún estén pendientes.

0 Comments [Show recent to old](#)
[Post a comment](#)

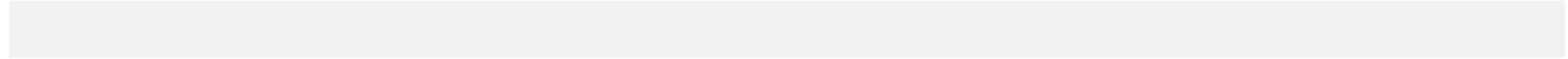
Attachments (2)

 [RSS of this page](#)

Author: [aglone](#) Version: [1.4](#) Last Edited By: [aglone3](#) Modified: 26 - days ago

Información de contacto

servicios@iso27002.es



Quick Search

- Navigate pages | Site Map
- 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 y recursos

9.1.4. Protección contra amenazas externas y del entorno

9.1.5. El trabajo en áreas seguras

9.1.6. Áreas aisladas de carga y descarga

Site Home » 09. Seguridad Física y del Entorno » 9 1 Áreas seguras » 9.1.1. Perímetro de seguridad física

9.1.1. Perímetro de seguridad física



Control:

Los perímetros de seguridad (como paredes, tarjetas de control de entrada a puertas o un puesto manual de recepción) deberían utilizarse para proteger las áreas que contengan información y recursos para su procesamiento.

Posibles Soluciones a este control:

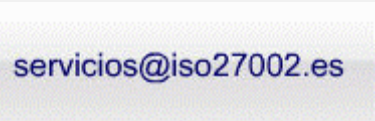
ASIS International	Guía en inglés sobre medidas de seguridad física.	ASIS Facilities Physical Security Measures Guideline
--------------------	---	--

0 Comments [Show recent to old](#)
[Post a comment](#)

RSS of this page

Author: [aglone](#) Version: [1.2](#) Last Edited By: [javier_ruiz](#) Modified: 8 - days ago

Información de contacto



Quick Search

- Navigate pages | Site Map
- 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 y recursos

9.1.4. Protección contra amenazas externas y del entorno

9.1.5. El trabajo en áreas seguras

9.1.6. Áreas aisladas de carga y descarga

Site Home » 09. Seguridad Física y del Entorno » 9 1 Áreas seguras » 9.1.2. Controles físicos de entrada

9.1.2. Controles físicos de entrada



Control:

Las áreas de seguridad deberían estar protegidas por controles de entrada adecuados que garanticen el acceso únicamente al personal autorizado.

(consultar 8.3.3)

Posibles Soluciones a este control:

Espacio pendiente de posibles aportaciones.

0 Comments Show recent to old
Post a comment

RSS of this page

Author: aglone Version: 1.1 Last Edited By: aglone3 Modified: 27 - days ago

Información de contacto

servicios@iso27002.es

Quick Search

- Navigate pages | Site Map
- 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 y recursos

9.1.4. Protección contra amenazas externas y del entorno

9.1.5. El trabajo en áreas seguras

9.1.6. Áreas aisladas de carga y descarga

Site Home » 09. Seguridad Física y del Entorno » 9 1 Áreas seguras » 9.1.3. Seguridad de oficinas, despachos y recursos

9.1.3. Seguridad de oficinas, despachos y recursos



Control:

Se debería asignar y aplicar la seguridad física para oficinas, despachos y recursos.

Posibles Soluciones a este control:

Espacio pendiente de posibles aportaciones.

0 Comments [Show recent to old](#)
[Post a comment](#)

RSS of this page

Author: [aglone](#) Version: [1.1](#) Last Edited By: [aglone3](#) Modified: 27 - days ago

Información de contacto

servicios@iso27002.es

Quick Search

- Navigate pages | Site Map
- 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 y recursos

9.1.4. Protección contra amenazas externas y del entorno

9.1.5. El trabajo en áreas seguras

9.1.6. Áreas aisladas de carga y descarga

Site Home » 09. Seguridad Física y del Entorno » 9 1 Áreas seguras » 9.1.4. Protección contra amenazas externas y del entorno

9.1.4. Protección contra amenazas externas y del entorno



Control:

Se debería designar y aplicar medidas de protección física contra incendio, inundación, terremoto, explosión, malestar civil y otras formas de desastre natural o humano.

Posibles Soluciones a este control:

Espacio pendiente de posibles aportaciones.

0 Comments [Show recent to old](#)
[Post a comment](#)

RSS of this page

Author: [aglone](#) Version: [1.1](#) Last Edited By: [aglone3](#) Modified: 27 - days ago

Información de contacto

servicios@iso27002.es

Quick Search

- Navigate pages | Site Map
- 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 y recursos

9.1.4. Protección contra amenazas externas y del entorno

9.1.5. El trabajo en áreas seguras

9.1.6. Áreas aisladas de carga y descarga

Site Home » 09. Seguridad Física y del Entorno » 9 1 Áreas seguras » 9.1.5. El trabajo en áreas seguras

9.1.5. El trabajo en áreas seguras



Control:

Se debería diseñar y aplicar protección física y pautas para trabajar en las áreas seguras.

Posibles Soluciones a este control:

Espacio pendiente de posibles aportaciones.

0 Comments [Show recent to old](#)
[Post a comment](#)

RSS of this page

Author: [aglone](#) Version: [1.1](#) Last Edited By: [aglone3](#) Modified: 27 - days ago

Información de contacto

servicios@iso27002.es

Quick Search

- Navigate pages | Site Map
- 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 y recursos

9.1.4. Protección contra amenazas externas y del entorno

9.1.5. El trabajo en áreas seguras

9.1.6. Áreas aisladas de carga y descarga

Site Home » 09. Seguridad Física y del Entorno » 9 1 Áreas seguras » 9.1.6. Áreas aisladas de carga y descarga

9.1.6. Áreas aisladas de carga y descarga



Control:

Se deberían controlar las áreas de carga y descarga con objeto de evitar accesos no autorizados y, si es posible, aislarlas de los recursos para el tratamiento de la información.

(consultar 9.2.1d)

(consultar 7.1.1)

Posibles Soluciones a este control:

Espacio pendiente de posibles aportaciones.

0 Comments Show recent to old
Post a comment

RSS of this page

Author: aglone Version: 1.1 Last Edited By: aglone3 Modified: 27 - days ago

Información de contacto

servicios@iso27002.es

Quick Search

- Navigate pages | Site Map
- ISO 27002

05. Política de Seguridad

06. Organización de la Seguridad de Información

07. Gestión de Activos

08. Seguridad ligada a los Recursos Humanos

09. Seguridad Física y del Entorno

9 1 Áreas seguras

9 2 Seguridad de los equipos

9.2.1. Instalación y protección de equipos

9.2.2. Suministro eléctrico

9.2.3. Seguridad del cableado

9.2.4. Mantenimiento de equipos

9 2 5 Seguridad de equipos fuera de los locales de la Organización

9.2.6. Seguridad en la reutilización o eliminación de equipos

9.2.7. Traslado de activos

10. Gestión de Comunicaciones y Operaciones

11. Control de Accesos

12. Adquisición, Desarrollo y Mantenimiento de Sistemas de Información

13. Gestión de Incidentes de Seguridad de la Información

14. Gestión de Continuidad del Negocio






15. Conformidad

Objetivos

Contacto

Aviso Legal

9 2 Seguridad de los equipos

	<h1>Espacio de Patrocinio disponible</h1>
	Evitar la pérdida, daño, robo o puesta en peligro de los activos y interrupción de las actividades de la organización.
	<p>Deberían protegerse los equipos contra las amenazas físicas y ambientales. La protección del equipo es necesaria para reducir el riesgo de acceso no autorizado a la información y su protección contra pérdida o robo.</p> <p>Así mismo, se debería considerar la ubicación y eliminación de los equipos.</p> <p>Se podrían requerir controles especiales para la protección contra amenazas físicas y para salvaguardar servicios de apoyo como energía eléctrica e infraestructura del cableado.</p>
	<p>Haga que los vigilantes de seguridad impidan a cualquiera (empleados, visitas, personas de soporte TI, mensajeros, personal de mudanzas, etc.) sacar equipos informáticos de las instalaciones sin autorización escrita.</p> <p>Conviértalo en un elemento disuasorio visible mediante chequeos aleatorios (o, incluso, arcos de detección de metales).</p> <p>Esté especialmente atento a puertas traseras, rampas de carga, salidas para fumadores, etc.</p> <p>Tome en consideración el uso de códigos de barras para hacer los chequeos más eficientes.</p>
	Número de chequeos (a personas a la salida y a existencias en stock) realizados en el último mes y porcentaje de chequeos que evidenciaron movimientos no autorizados de equipos o soportes informáticos u otras cuestiones de seguridad.

0 Comments

Show recent to old

Post a comment

Attachments (2)

 RSS of this page

Author: [aglone](#)

Version: [1.4](#)

Last Edited By: [aglone3](#)

Modified: 26 - days ago

Información de contacto

servicios@iso27002.es

Quick Search

- Navigate pages | Site Map
- 9 2 Seguridad de los equipos

 - 9.2.1. Instalación y protección de equipos
 - 9.2.2. Suministro eléctrico
 - 9.2.3. Seguridad del cableado
 - 9.2.4. Mantenimiento de equipos
 - 9 2 5 Seguridad de equipos fuera de los locales de la Organización
 - 9.2.6. Seguridad en la reutilización o eliminación de equipos
 - 9.2.7. Traslado de activos

Site Home » 09. Seguridad Física y del Entorno » 9 2 Seguridad de los equipos » 9.2.1. Instalación y protección de equipos

9.2.1. Instalación y protección de equipos



Control:

El equipo debería situarse y protegerse para reducir el riesgo de materialización de las amenazas del entorno, así como las oportunidades de acceso no autorizado.

Posibles Soluciones a este control:

Espacio pendiente de posibles aportaciones.

0 Comments [Show recent to old](#)
[Post a comment](#)

RSS of this page

Author: [aglone](#) Version: [1.1](#) Last Edited By: [aglone3](#) Modified: 27 - days ago

Información de contacto

servicios@iso27002.es

Quick Search

- Navigate pages | Site Map
- 9 2 Seguridad de los equipos

9.2.1. Instalación y protección de equipos

9.2.2. Suministro eléctrico

9.2.3. Seguridad del cableado

9.2.4. Mantenimiento de equipos

9 2 5 Seguridad de equipos fuera de los locales de la Organización

9.2.6. Seguridad en la reutilización o eliminación de equipos

9.2.7. Traslado de activos

Site Home » 09. Seguridad Física y del Entorno » 9 2 Seguridad de los equipos » 9.2.2. Suministro eléctrico

9.2.2. Suministro eléctrico



Control:

Se deberían proteger los equipos contra fallos en el suministro de energía u otras anomalías eléctricas en los equipos de apoyo.

Posibles Soluciones a este control:

Espacio pendiente de posibles aportaciones.

0 Comments [Show recent to old](#)
[Post a comment](#)

RSS of this page

Author: [aglone](#) Version: [1.1](#) Last Edited By: [aglone3](#) Modified: 27 - days ago

Información de contacto

servicios@iso27002.es

Quick Search

- Navigate pages | Site Map
- 9 2 Seguridad de los equipos
 - 9.2.1. Instalación y protección de equipos
 - 9.2.2. Suministro eléctrico
 - 9.2.3. Seguridad del cableado**
 - 9.2.4. Mantenimiento de equipos
 - 9 2 5 Seguridad de equipos fuera de los locales de la Organización
 - 9.2.6. Seguridad en la reutilización o eliminación de equipos
 - 9.2.7. Traslado de activos

9.2.3. Seguridad del cableado



Control:

Se debería proteger el cableado de energía y de telecomunicaciones que transporten datos o soporten servicios de información contra posibles interceptaciones o daños.

Posibles Soluciones a este control:

Espacio pendiente de posibles aportaciones.

0 Comments [Show recent to old](#)
[Post a comment](#)

 [RSS of this page](#)

Author: [aglone](#) Version: [1.1](#) Last Edited By: [aglone3](#) Modified: 27 - days ago

Información de contacto

servicios@iso27002.es

Quick Search

- Navigate pages | Site Map
- 9 2 Seguridad de los equipos
 - 9.2.1. Instalación y protección de equipos
 - 9.2.2. Suministro eléctrico
 - 9.2.3. Seguridad del cableado
 - 9.2.4. Mantenimiento de equipos**
 - 9 2 5 Seguridad de equipos fuera de los locales de la Organización
 - 9.2.6. Seguridad en la reutilización o eliminación de equipos
 - 9.2.7. Traslado de activos

 [Site Home](#) » [09. Seguridad Física y del Entorno](#) » [9 2 Seguridad de los equipos](#) » 9.2.4. Mantenimiento de equipos

9.2.4. Mantenimiento de equipos



Control:

Se deberían mantener adecuadamente los equipos para garantizar su continua disponibilidad e integridad.

Posibles Soluciones a este control:

Espacio pendiente de posibles aportaciones.

0 Comments [Show recent to old](#)
[Post a comment](#)

 [RSS of this page](#)

Author: [aglone](#) Version: [1.1](#) Last Edited By: [aglone3](#) Modified: 27 - days ago

Información de contacto

servicios@iso27002.es

Quick Search

- Navigate pages | Site Map
- 9 2 Seguridad de los equipos

9.2.1. Instalación y protección de equipos

9.2.2. Suministro eléctrico

9.2.3. Seguridad del cableado

9.2.4. Mantenimiento de equipos

9 2 5 Seguridad de equipos fuera de los locales de la Organización

9.2.6. Seguridad en la reutilización o eliminación de equipos

9.2.7. Traslado de activos

Site Home » 09. Seguridad Física y del Entorno » 9 2 Seguridad de los equipos » 9 2 5 Seguridad de equipos fuera de los locales de la Organización

9 2 5 Seguridad de equipos fuera de los locales de la Organización



Control:

Se debería aplicar seguridad a los equipos que se encuentran fuera de los locales de la organización considerando los diversos riesgos a los que están expuestos.

(consultar 11.7.1.)

Posibles Soluciones a este control:

	Guía para proteger y usar de forma segura su móvil	Guía INTECO
--	--	-----------------------------

0 Comments Show recent to old
Post a comment

Attachments (1)

RSS of this page

Author: [aglone](#) Version: [1.3](#) Last Edited By: [aglone3](#) Modified: 27 - days ago

Información de contacto

servicios@iso27002.es

Quick Search

- Navigate pages | Site Map
- 9 2 Seguridad de los equipos

9.2.1. Instalación y protección de equipos

9.2.2. Suministro eléctrico

9.2.3. Seguridad del cableado

9.2.4. Mantenimiento de equipos

9 2 5 Seguridad de equipos fuera de los locales de la Organización

9.2.6. Seguridad en la reutilización o eliminación de equipos

9.2.7. Traslado de activos

Site Home » 09. Seguridad Física y del Entorno » 9 2 Seguridad de los equipos » 9.2.6. Seguridad en la reutilización o eliminación de equipos

9.2.6. Seguridad en la reutilización o eliminación de equipos




Control:

Debería revisarse cualquier elemento del equipo que contenga dispositivos de almacenamiento con el fin de garantizar que cualquier dato sensible y software con licencia se haya eliminado o sobrescrito con seguridad antes de la eliminación.

(consultar 10.7.2).

Posibles Soluciones a este control:

	Darik's Boot and Nuke ("DBAN") is a self-contained boot disk that securely wipes the hard disks of most computers. DBAN will automatically and completely delete the contents of any hard disk that it can detect, which makes it an appropriate utility for bulk or emergency data destruction.	DBAN
--	--	----------------------

0 Comments [Show recent to old](#)
[Post a comment](#)

 RSS of this page

Author: [aglone](#) Version: [1.1](#) Last Edited By: [aglone3](#) Modified: 27 - days ago

Información de contacto

servicios@iso27002.es

Quick Search

- Navigate pages | Site Map
- 9 2 Seguridad de los equipos

9.2.1. Instalación y protección de equipos

9.2.2. Suministro eléctrico

9.2.3. Seguridad del cableado

9.2.4. Mantenimiento de equipos

9 2 5 Seguridad de equipos fuera de los locales de la Organización

9.2.6. Seguridad en la reutilización o eliminación de equipos

9.2.7. Traslado de activos

Site Home » 09. Seguridad Física y del Entorno » 9 2 Seguridad de los equipos » 9.2.7. Traslado de activos

9.2.7. Traslado de activos



Control:

No deberían sacarse equipos, información o software fuera del local sin una autorización.

Posibles Soluciones a este control:

Espacio pendiente de posibles aportaciones.

0 Comments [Show recent to old](#)
[Post a comment](#)

RSS of this page

Author: [aglone](#) Version: [1.1](#) Last Edited By: [aglone3](#) Modified: 27 - days ago

Información de contacto





servicios@iso27002.es

Quick Search

- Navigate pages | Site Map
- ISO 27002
 - 05. Política de Seguridad
 - 06. Organización de la Seguridad de Información
 - 07. Gestión de Activos
 - 08. Seguridad ligada a los Recursos Humanos
 - 09. Seguridad Física y del Entorno
 - 10. Gestión de Comunicaciones y Operaciones
 - 10 1 Procedimientos y responsabilidades de operación**
 - 10.1.1. Documentación de procedimientos operativos
 - 10.1.2. Control de cambios operacionales
 - 10.1.3. Segregación de tareas
 - 10.1.4. Separación de los recursos para desarrollo y producción
 - 10 2 Supervisión de los servicios contratados a terceros
 - 10 3 Planificación y aceptación del sistema
 - 10 4 Protección contra software malicioso y código móvil
 - 10 5 Gestión interna de soportes y recuperación
 - 10 6 Gestión de redes
 - 10 7 Utilización y seguridad de los soportes de información
 - 10 8 Intercambio de información y software
 - 10 9 Servicios de comercio electrónico
 - 10 10 Monitorización
 - 11. Control de Accesos
 - 12. Adquisición, Desarrollo y Mantenimiento de Sistemas de Información
 - 13. Gestión de Incidentes de Seguridad de la Información
 - 14. Gestión de Continuidad del Negocio
 - 15. Conformidad
 - Objetivos
 - Contacto
 - Aviso Legal

10 1 Procedimientos y responsabilidades de operación



 Objetivo	Asegurar la operación correcta y segura de los recursos de tratamiento de información.
 Principios	<p>Se deberían establecer responsabilidades y procedimientos para la gestión y operación de todos los recursos para el tratamiento de la información.</p> <p>Esto incluye el desarrollo de instrucciones apropiadas de operación y de procedimientos de respuesta ante incidencias.</p> <p>Se implantará la segregación de tareas, cuando sea adecuado, para reducir el riesgo de un mal uso del sistema deliberado o por negligencia.</p>
	Documente procedimientos, normas y directrices de seguridad de la información, además de roles y responsabilidades, identificadas en el manual de política de seguridad de la organización.
	Métricas de madurez de procesos TI relativos a seguridad, tales como el semiperiodo de aplicación de parches de seguridad (tiempo que ha llevado parchear al menos la mitad de los sistemas vulnerables -esta medida evita la cola variable provocada por los pocos sistemas inevitables que permanecen sin parchear por no ser de uso diario, estar normalmente fuera de la oficina o cualquier otra razón-).

0 Comments [Show recent to old](#)
[Post a comment](#)

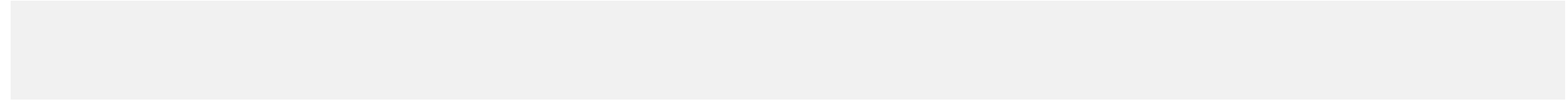
[Attachments \(2\)](#)

 [RSS of this page](#)

Author: [aglone](#) **Version:** [1.5](#) **Last Edited By:** [aglone3](#) **Modified:** 26 - days ago

Información de contacto

servicios@iso27002.es



Quick Search

- ## Navigate pages | Site Map
- ☐ 10 1 Procedimientos y responsabilidades de operación
 - **10.1.1. Documentación de procedimientos operativos**
 - 10.1.2. Control de cambios operacionales
 - 10.1.3. Segregación de tareas
 - 10.1.4. Separación de los recursos para desarrollo y producción

Documentación de procedimientos operativos

10.1.1. Documentación de procedimientos operativos



Control:

Se deberían documentar y mantener los procedimientos de operación y ponerlos a disposición de todos los usuarios que lo necesiten.

(consultar 10.5)

([consultar 11.5.4](#))

([consultar 10.7.2](#) y [10.7.3](#))

(consultar 10.10)

Posibles Soluciones a este control:

Espacio pendiente de posibles aportaciones.

0 Comments [Show recent to old](#)
[Post a comment](#)



RSS of this page

Author: [aglone](#) **Version:** [1.1](#) **Last Edited By:** [aglone3](#) **Modified:** 27 - days ago

Información de contacto

servicios@iso27002.es

Quick Search

- Navigate pages | Site Map
- 10 1 Procedimientos y responsabilidades de operación

10.1.1. Documentación de procedimientos operativos

10.1.2. Control de cambios operacionales

10.1.3. Segregación de tareas

10.1.4. Separación de los recursos para desarrollo y producción

Site Home » 10. Gestión de Comunicaciones y Operaciones » 10 1 Procedimientos y responsabilidades de operación » 10.1.2.

Control de cambios operacionales

10.1.2. Control de cambios operacionales



Control:

Se deberían controlar los cambios en los sistemas y en los recursos de tratamiento de la información.

(consultar 12.5.1)

Posibles Soluciones a este control:

Espacio pendiente de posibles aportaciones.

0 Comments

Show recent to old

Post a comment

RSS of this page

Author: [aglone](#)

Version: [1.1](#)

Last Edited By: [aglone3](#)

Modified: 27 - days ago

Información de contacto

servicios@iso27002.es

Quick Search

- Navigate pages | Site Map
- 10 1 Procedimientos y responsabilidades de operación

10.1.1. Documentación de procedimientos operativos

10.1.2. Control de cambios operacionales

10.1.3. Segregación de tareas

10.1.4. Separación de los recursos para desarrollo y producción

Site Home » 10. Gestión de Comunicaciones y Operaciones » 10 1 Procedimientos y responsabilidades de operación » 10.1.3. Segregación de tareas


10.1.3. Segregación de tareas



Control:

Se deberían segregar las tareas y las áreas de responsabilidad con el fin de reducir las oportunidades de una modificación no autorizada o no intencionada, o el de un mal uso de los activos de la organización.

Posibles Soluciones a este control:

logo.gif	The software-based solution captures user activity in any user session, including Terminal, Remote Desktop, Citrix, VMWare, VNC, NetOP and PC Anywhere. ObserveIT Xpress is a completely free version of the ObserveIT product, with no time limit. The free version can monitor a maximum of 5 servers	ObserveIT Xpress
	The segregation of duties control matrix is illustrative of potential segregation of duties issues.	ISACA

0 Comments

Show recent to old

Post a comment

 RSS of this page

Author: [aglone](#) Version: [1.1](#) Last Edited By: [aglone3](#) Modified: 27 - days ago

Información de contacto

servicios@iso27002.es

Quick Search

- Navigate pages | Site Map
- 10 1 Procedimientos y responsabilidades de operación

10.1.1. Documentación de procedimientos operativos

10.1.2. Control de cambios operacionales

10.1.3. Segregación de tareas

10.1.4. Separación de los recursos para desarrollo y producción

Site Home » 10. Gestión de Comunicaciones y Operaciones » 10 1 Procedimientos y responsabilidades de operación » 10.1.4.

Separación de los recursos para desarrollo y producción

10.1.4. Separación de los recursos para desarrollo y producción



Control:

La separación de los recursos para el desarrollo, prueba y producción es importante para reducir los riesgos de un acceso no autorizado o de cambios al sistema operacional.

(consultar 12.4.2)

Posibles Soluciones a este control:

Espacio pendiente de posibles aportaciones.

0 Comments

Show recent to old

Post a comment

 RSS of this page

Author: aglone

Version: 1.1

Last Edited By: aglone3

Modified: 27 - days ago

Información de contacto

servicios@iso27002.es

Quick Search

Navigate pages | Site Map

ISO 27002

05. Política de Seguridad

06. Organización de la Seguridad de Información

07. Gestión de Activos

08. Seguridad ligada a los Recursos Humanos

09. Seguridad Física y del Entorno

10. Gestión de Comunicaciones y Operaciones

10 1 Procedimientos y responsabilidades de operación

10 2 Supervisión de los servicios contratados a terceros

10.2.1. Prestación de servicios

10.2.2. Monitorización y revisión de los servicios contratados

10.2.3. Gestión de los cambios en los servicios contratados

10 3 Planificación y aceptación del sistema

10 4 Protección contra software malicioso y código móvil

10 5 Gestión interna de soportes y recuperación

10 6 Gestión de redes

10 7 Utilización y seguridad de los soportes de información

10 8 Intercambio de información y software

10 9 Servicios de comercio electrónico

10 10 Monitorización

11. Control de Accesos

12. Adquisición, Desarrollo y Mantenimiento de Sistemas de Información

13. Gestión de Incidentes de Seguridad de la Información

14. Gestión de Continuidad del Negocio

15. Conformidad





Objetivos

Contacto

Aviso Legal

10 2 Supervisión de los servicios contratados a terceros



	Implementar y mantener un nivel apropiado de seguridad de la información y de la prestación del servicio en línea con los acuerdos de prestación del servicio por terceros.
	La organización debería verificar la implementación de acuerdos, el monitoreo de su cumplimiento y gestión de los cambios con el fin de asegurar que los servicios que se ser prestan cumplen con todos los requerimientos acordados con los terceros.
	<p>¿Lo que recibe vale lo que paga por ello? Dé respuesta a esta pregunta y respáldela con hechos, estableciendo un sistema de supervisión de terceros proveedores de servicios y sus respectivas entregas de servicio.</p> <p>Revise periódicamente los acuerdos de nivel de servicio (SLA) y compárelos con los registros de supervisión. En algunos casos puede funcionar un sistema de premio y castigo.</p> <p>sté atento a cambios que tengan impacto en la seguridad.</p>
	Coste del tiempo de inactividad debido al incumplimiento de los acuerdos de nivel de servicio. Evaluación del rendimiento de proveedores incluyendo la calidad de servicio, entrega, coste, etc.

0 Comments [Show recent to old](#)
[Post a comment](#)

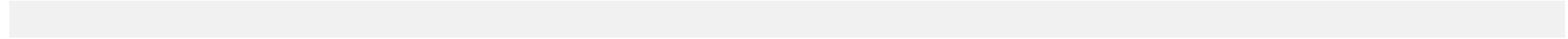
[Attachments](#) (2)

 [RSS of this page](#)

Author: [aglone](#) **Version:** [1.5](#) **Last Edited By:** [aglone3](#) **Modified:** 26 - days ago

Información de contacto

servicios@iso27002.es



Quick Search

- Navigate pages | Site Map
- 10 2 Supervisión de los servicios contratados a terceros

 - 10.2.1. Prestación de servicios
 - 10.2.2. Monitorización y revisión de los servicios contratados
 - 10.2.3. Gestión de los cambios en los servicios contratados

Site Home » 10. Gestión de Comunicaciones y Operaciones » 10 2 Supervisión de los servicios contratados a terceros »

10.2.1. Prestación de servicios

10.2.1. Prestación de servicios




Control:

Se debería garantizar que los controles de seguridad, definiciones de servicio y niveles de entrega incluidos en el acuerdo de entrega de servicio externo sean implementados, operados y mantenidos por la parte externa.

(consultar 14.1)

Posibles Soluciones a este control:

	Ejemplos de peticiones de propuestas en los que se incluyen descripciones del servicio entregado y acuerdos de seguridad con terceros, así como, definiciones de servicio y aspectos de la gestión del servicio (inglés)	Kerala State Wide Area Network Infrastructure Kerala State ISMS implantation
--	--	---

0 Comments [Show recent to old](#)
[Post a comment](#)

 RSS of this page

Author: [aglone](#) Version: [1.1](#) Last Edited By: [aglone3](#) Modified: 27 - days ago

Información de contacto

servicios@iso27002.es

Quick Search

- Navigate pages | Site Map
- 10 2 Supervisión de los servicios contratados a terceros
 - 10.2.1. Prestación de servicios
 - 10.2.2. Monitorización y revisión de los servicios contratados**
 - 10.2.3. Gestión de los cambios en los servicios contratados

 [Site Home](#) >> [10. Gestión de Comunicaciones y Operaciones](#) >> [10 2 Supervisión de los servicios contratados a terceros](#) >>

10.2.2. Monitorización y revisión de los servicios contratados

10.2.2. Monitorización y revisión de los servicios contratados



Control:

Los servicios, informes y registros suministrados por terceros deberían ser monitoreados y revisados regularmente, y las auditorias se deberían realizar a intervalos regulares.

([consultar 6.2.3](#))

Posibles Soluciones a este control:

Espacio pendiente de posibles aportaciones.

0 Comments [Show recent to old](#)
[Post a comment](#)

 [RSS of this page](#)

Author: [aglone](#) Version: [1.1](#) Last Edited By: [aglone3](#) Modified: 27 - days ago

Información de contacto

servicios@iso27002.es

Quick Search

- Navigate pages | Site Map
- 10 2 Supervisión de los servicios contratados a terceros

10.2.1. Prestación de servicios

10.2.2. Monitorización y revisión de los servicios contratados

10.2.3. Gestión de los cambios en los servicios contratados

Site Home » 10. Gestión de Comunicaciones y Operaciones » 10 2 Supervisión de los servicios contratados a terceros »

10.2.3. Gestión de los cambios en los servicios contratados

10.2.3. Gestión de los cambios en los servicios contratados



Control:

Se deberían gestionar los cambios en la provisión del servicio, incluyendo mantenimiento y mejoras en las políticas de seguridad de información existentes, en los procedimientos y los controles teniendo en cuenta la importancia de los sistemas y procesos del negocio involucrados, así como la reevaluación de los riesgos.

Posibles Soluciones a este control:

Espacio pendiente de posibles aportaciones.

0 Comments [Show recent to old](#)
[Post a comment](#)

RSS of this page

Author: [aglone](#) Version: [1.1](#) Last Edited By: [aglone3](#) Modified: 27 - days ago

Información de contacto

servicios@iso27002.es

Quick Search

Navigate pages | Site Map

ISO 27002

05. Política de Seguridad

06. Organización de la Seguridad de Información

07. Gestión de Activos

08. Seguridad ligada a los Recursos Humanos

09. Seguridad Física y del Entorno

10. Gestión de Comunicaciones y Operaciones

10 1 Procedimientos y responsabilidades de operación

10 2 Supervisión de los servicios contratados a terceros

10 3 Planificación y aceptación del sistema

10. 3. 1. Planificación de capacidades

10. 3. 2. Aceptación del sistema

10 4 Protección contra software malicioso y código móvil

10 5 Gestión interna de soportes y recuperación

10 6 Gestión de redes

10 7 Utilización y seguridad de los soportes de información

10 8 Intercambio de información y software

10 9 Servicios de comercio electrónico

10 10 Monitorización

11. Control de Accesos

12. Adquisición, Desarrollo y Mantenimiento de Sistemas de Información

13. Gestión de Incidentes de Seguridad de la Información

14. Gestión de Continuidad del Negocio

15. Conformidad





Objetivos

Contacto

Aviso Legal

10 3 Planificación y aceptación del sistema



	Minimizar el riesgo de fallos en los sistemas.
	<p>Se requiere una planificación y preparación avanzadas para garantizar la adecuada capacidad y recursos con objeto de mantener la disponibilidad de los sistemas requerida.</p> <p>Deberían realizarse proyecciones de los requisitos de capacidad en el futuro para reducir el riesgo de sobrecarga de los sistemas.</p> <p>Se deberían establecer, documentar y probar, antes de su aceptación, los requisitos operacionales de los nuevos sistemas.</p>
	<p>Adopte procesos estructurados de planificación de capacidad TI, desarrollo seguro, pruebas de seguridad, etc., usando estándares aceptados como ISO 20000 (ITIL) donde sea posible.</p> <p>Defina e imponga estándares de seguridad básica (mínimos aceptables) para todas las plataformas de sistemas operativos, usando las recomendaciones de seguridad de CIS, NIST, NSA y fabricantes de sistemas operativos y, por supuesto, sus propias políticas de seguridad de la información.</p>
	<p>Porcentaje de cambios de riesgo bajo, medio, alto y de emergencia. Número y tendencia de cambios revertidos y rechazados frente a cambios exitosos.</p> <p>Porcentaje de sistemas (a) que deberían cumplir con estándares de seguridad básica o similares y (b) cuya conformidad con dichos estándares ha sido comprobada mediante benchmarking o pruebas.</p>

0 Comments [Show recent to old](#)
[Post a comment](#)

[Attachments \(2\)](#)

 [RSS of this page](#)

Author: [aglone](#) Version: [1.4](#) Last Edited By: [aglone3](#) Modified: 26 - days ago

Información de contacto

servicios@iso27002.es

Quick Search

- Navigate pages | Site Map
- 10 3 Planificación y aceptación del sistema

10. 3. 1. Planificación de capacidades

10. 3. 2. Aceptación del sistema

 [Site Home](#) » [10. Gestión de Comunicaciones y Operaciones](#) » [10 3 Planificación y aceptación del sistema](#) » 10. 3. 1. Planificación de capacidades

10. 3. 1. Planificación de capacidades



Control:

Se debería monitorizar el uso de recursos, así como de las proyecciones de los requisitos de las capacidades adecuadas para el futuro con objeto de asegurar el funcionamiento requerido del sistema.

Posibles Soluciones a este control:

Espacio pendiente de posibles aportaciones.

0 Comments [Show recent to old](#)
[Post a comment](#)

 [RSS of this page](#)

Author: [aglone](#) **Version:** [1.1](#) **Last Edited By:** [aglone3](#) **Modified:** 27 - days ago

Información de contacto

servicios@iso27002.es

Quick Search

- Navigate pages | Site Map
- 10 3 Planificación y aceptación del sistema
 - 10. 3. 1. Planificación de capacidades
 - 10. 3. 2. Aceptación del sistema**

 [Site Home](#) >> [10. Gestión de Comunicaciones y Operaciones](#) >> [10 3 Planificación y aceptación del sistema](#) >> 10. 3. 2. Aceptación del sistema

10. 3. 2. Aceptación del sistema



Control:

Se deberían establecer criterios de aceptación para nuevos sistemas de información, actualizaciones y versiones nuevas. Se deberían desarrollar las pruebas adecuadas del sistema durante el desarrollo y antes de su aceptación.

([consultar 14.1](#))

Posibles Soluciones a este control:

Espacio pendiente de posibles aportaciones.

0 Comments [Show recent to old](#)
[Post a comment](#)

 [RSS of this page](#)

Author: [aglone](#) Version: [1.1](#) Last Edited By: [aglone3](#) Modified: 27 - days ago

Información de contacto

servicios@iso27002.es

Quick Search

- Navigate pages | Site Map
- ISO 27002

05. Política de Seguridad

06. Organización de la Seguridad de Información

07. Gestión de Activos

08. Seguridad ligada a los Recursos Humanos

09. Seguridad Física y del Entorno

10. Gestión de Comunicaciones y Operaciones

10 1 Procedimientos y responsabilidades de operación

10 2 Supervisión de los servicios contratados a terceros

10 3 Planificación y aceptación del sistema

10 4 Protección contra software malicioso y código móvil

10. 4. 1. Medidas y controles contra software malicioso

10. 4. 2. Medidas y controles contra código móvil

10 5 Gestión interna de soportes y recuperación

10 6 Gestión de redes

10 7 Utilización y seguridad de los soportes de información

10 8 Intercambio de información y software

10 9 Servicios de comercio electrónico

10 10 Monitorización

11. Control de Accesos

12. Adquisición, Desarrollo y Mantenimiento de Sistemas de Información

13. Gestión de Incidentes de Seguridad de la Información

14. Gestión de Continuidad del Negocio

15. Conformidad

Objetivos

Contacto

Aviso Legal
- Site Home

>>

10. Gestión de Comunicaciones y Operaciones

>>

10 4 Protección contra software malicioso y código móvil
- 10 4 Protección contra software malicioso y código móvil
- 

Espacio de Patrocinio disponible

 <div>Objetivo</div>	Proteger la integridad del software y de la información.
 <div>Principios</div>	<p>Se requieren ciertas precauciones para prevenir y detectar la introducción de código malicioso y códigos móviles no autorizados.</p> <p>El software y los recursos de tratamiento de información son vulnerables a la introducción de software malicioso como virus informáticos, gusanos de la red, caballos de troya y bombas lógicas.</p> <p>Los usuarios deberían conocer los peligros que puede ocasionar el software malicioso o no autor izado y los administradores deberían introducir controles y medidas especiales para detectar o evitar su introducción.</p>
	<p>Combine controles tecnológicos (p. ej., software antivirus) con medidas no técnicas (educación, concienciación y formación).</p> <p>¡No sirve de mucho tener el mejor software antivirus del mercado si los empleados siguen abriendo e-mails de remitentes desconocidos o descargando ficheros de sitios no confiables!</p>
	Tendencia en el número de virus, gusanos, troyanos o spam detectados y bloqueados. Número y costes acumulados de incidentes por software malicioso.
- 0 Comments [Show recent to old](#)
Post a comment
- Attachments (2)**
-  [RSS of this page](#)
- Author:** [aglone](#) **Version:** [1.5](#) **Last Edited By:** [aglone3](#) **Modified:** 26 - days ago
- Información de contacto
- servicios@iso27002.es
- Powered by [Zoho Wiki](#) | [Zoho](#) | [Report Abuse](#) | [Wiki Index](#) | [Site Map](#) | [Help](#) | [Feedback](#) | [Jump Start with 2 Free Wikis](#) | [Sign in](#)
- http://iso27002.wiki.zoho.com/10-4-Protección-contra-software-malicioso-y-código-móvil.html[28/01/2011 08:24:55 p.m.]

Quick Search

Navigate pages | Site Map

10 4 Protección contra software malicioso y código móvil

10. 4. 1. Medidas y controles contra software malicioso

10. 4. 2. Medidas y controles contra código móvil

10. 4. 1. Medidas y controles contra software malicioso



Control:






Se deberían implantar controles de detección, prevención y recuperación contra el software malicioso, junto a procedimientos adecuados para la concienciación de los usuarios.

(consultar 15.1.2)

(consultar 13.1 y 13.2)

(consultar 14)

Posibles Soluciones a este control:

	Service on-line for malware. Submit your Windows executable and receive an analysis report telling you what it does. For analyzing Javascript and Flash files try Wepawet	Anubis
	VirusTotal es un servicio de análisis de archivos sospechosos que permite detectar virus, gusanos, troyanos, y malware en general. Características: Servicio independiente y gratuito, Uso simultáneo de múltiples motores antivirus, Actualización automática de los motores en tiempo real, Resultados detallados por cada uno de los antivirus, Estadísticas globales en tiempo real	VirusTotal
 <div>International Organization for Standardization</div>	Especificaciones para el etiquetado de software con el objeto de optimizar su identificación y gestión. (inglés)	ISO/IEC 19077-2:2009
	Microsoft Security Essentials proporciona protección en tiempo real contra virus, spyware y otros tipos de software malintencionado para PCs.	Microsoft Security Essentials
	NetCop is UTM server with integrated OS.No need to install any software at client side.NetCop does Content filter,Cache Engine,Spam protection,Hotspot,bandwidth control. Also protect your network from incoming threats like Virus, SPAM , Trojan etc.	NetCop UTM

0 Comments [Show recent to old](#)
[Post a comment](#)

 RSS of this page

Author: [aglone](#) Version: [1.1](#) Last Edited By: [aglone3](#) Modified: 27 - days ago

Información de contacto

servicios@iso27002.es

Quick Search

- Navigate pages | Site Map
- 10 4 Protección contra software malicioso y código móvil
 - 10. 4. 1. Medidas y controles contra software malicioso
 - 10. 4. 2. Medidas y controles contra código móvil**

 [Site Home](#) » [10. Gestión de Comunicaciones y Operaciones](#) » [10 4 Protección contra software malicioso y código móvil](#) » 10.

4. 2. Medidas y controles contra código móvil

10. 4. 2. Medidas y controles contra código móvil



Control:

Cuando se autorica la utilización de código móvil, la configuración debería asegurar que dicho código móvil opera de acuerdo a una política de seguridad definida y se debería evitar la ejecución de los códigos móviles no autorizados.

Posibles Soluciones a este control:

Espacio pendiente de posibles aportaciones.

0 Comments [Show recent to old](#)
[Post a comment](#)

 [RSS of this page](#)

Author: [aglone](#) Version: [1.1](#) Last Edited By: [aglone3](#) Modified: 27 - days ago

Información de contacto

servicios@iso27002.es

Quick Search

- Navigate pages | Site Map
- ISO 27002

05. Política de Seguridad

06. Organización de la Seguridad de Información

07. Gestión de Activos

08. Seguridad ligada a los Recursos Humanos

09. Seguridad Física y del Entorno

10. Gestión de Comunicaciones y Operaciones

10 1 Procedimientos y responsabilidades de operación

10 2 Supervisión de los servicios contratados a terceros

10 3 Planificación y aceptación del sistema

10 4 Protección contra software malicioso y código móvil

10 5 Gestión interna de soportes y recuperación

10. 5. 1. Recuperación de la información

10 6 Gestión de redes

10 7 Utilización y seguridad de los soportes de información

10 8 Intercambio de información y software

10 9 Servicios de comercio electrónico

10 10 Monitorización

11. Control de Accesos

12. Adquisición, Desarrollo y Mantenimiento de Sistemas de Información






13. Gestión de Incidentes de Seguridad de la Información

14. Gestión de Continuidad del Negocio

15. Conformidad

Objetivos

Contacto

Aviso Legal
- Site Home » 10. Gestión de Comunicaciones y Operaciones » 10 5 Gestión interna de soportes y recuperación
- ## 10 5 Gestión interna de soportes y recuperación
-
- | | |
|---|---|
|  Objetivo | Mantener la integridad y la disponibilidad de los servicios de tratamiento de información y comunicación. |
|  Principios | Se deberían establecer procedimientos rutinarios para conseguir la estrategia aceptada de respaldo (consultar 14.1) para realizar copias de seguridad y probar su puntual recuperación. |
|  | <p>Implante procedimientos de backup y recuperación que satisfagan no sólo requisitos contractuales sino también requisitos de negocio "internos" de la organización.</p> <p>Básese en la evaluación de riesgos realizada para determinar cuáles son los activos de información más importantes y use esta información para crear su estrategia de backup y recuperación.</p> <p>Hay que decidir y establecer el tipo de almacenamiento, soporte a utilizar, aplicación de backup, frecuencia de copia y prueba de soportes.</p> <p>Encrpte copias de seguridad y archivos que contengan datos sensibles o valiosos (en realidad, serán prácticamente todos porque, si no, ¿para qué hacer copias de seguridad?).</p> |
|  | <p>Porcentaje de operaciones de backup exitosas.</p> <p>Porcentaje de recuperaciones de prueba exitosas.</p> <p>Tiempo medio transcurrido desde la recogida de los soportes de backup de su almacenamiento fuera de las instalaciones hasta la recuperación exitosa de los datos en todas ubicaciones principales.</p> <p>Porcentaje de backups y archivos con datos sensibles o valiosos que están encriptados.</p> |
- 0 Comments [Show recent to old](#)
Post a comment
- Attachments (2)**
-  [RSS of this page](#)
- Author: [aglone](#) Version: [1.4](#) Last Edited By: [aglone3](#) Modified: 26 - days ago
- ### Información de contacto
- servicios@iso27002.es
- Powered by [Zoho Wiki](#) | [Zoho](#) | [Report Abuse](#) | [Wiki Index](#) | [Site Map](#) | [Help](#) | [Feedback](#) | [Jump Start with 2 Free Wikis](#) | [Sign in](#)
- <http://iso27002.wiki.zoho.com/10-5-Gestión-interna-de-soportes-y-recuperación.html>[28/01/2011 08:25:30 p.m.]

Quick Search

- Navigate pages | Site Map
- 10 5 Gestión interna de soportes y recuperación
 - 10. 5. 1. Recuperación de la información

Site Home » 10. Gestión de Comunicaciones y Operaciones » 10 5 Gestión interna de soportes y recuperación » 10. 5. 1. Recuperación de la información

10. 5. 1. Recuperación de la información



Control:

Se deberían hacer regularmente copias de seguridad de toda la información esencial del negocio y del software, de acuerdo con la política acordada de recuperación.

(consultar 9)

(consultar 14)

(consultar 15.1.3)

Posibles Soluciones a este control:

Espacio pendiente de posibles aportaciones.

0 Comments Show recent to old
Post a comment

RSS of this page

Author: aglone Version: 1.1 Last Edited By: aglone3 Modified: 27 - days ago

Información de contacto

servicios@iso27002.es

Quick Search

- Navigate pages | Site Map
- ISO 27002

⊞ 05. Política de Seguridad

⊞ 06. Organización de la Seguridad de Información

⊞ 07. Gestión de Activos

⊞ 08. Seguridad ligada a los Recursos Humanos

⊞ 09. Seguridad Física y del Entorno

⊞ 10. Gestión de Comunicaciones y Operaciones

⊞ 10 1 Procedimientos y responsabilidades de operación

⊞ 10 2 Supervisión de los servicios contratados a terceros

⊞ 10 3 Planificación y aceptación del sistema

⊞ 10 4 Protección contra software malicioso y código móvil

⊞ 10 5 Gestión interna de soportes y recuperación

⊞ 10 6 Gestión de redes

● 10. 6. 1. Controles de red

● 10. 6. 2. Seguridad en los servicios de red

⊞ 10 7 Utilización y seguridad de los soportes de información

⊞ 10 8 Intercambio de información y software

⊞ 10 9 Servicios de comercio electrónico

⊞ 10 10 Monitorización

⊞ 11. Control de Accesos

⊞ 12. Adquisición, Desarrollo y Mantenimiento de Sistemas de Información

⊞ 13. Gestión de Incidentes de Seguridad de la Información

⊞ 14. Gestión de Continuidad del Negocio

⊞ 15. Conformidad





● Objetivos

● Contacto

● Aviso Legal

10 6 Gestión de redes



 Objetivo	Asegurar la protección de la información en las redes y la protección de su infraestructura de apoyo.
 Principios	<p>La gestión de la seguridad de las redes, las cuales pueden cruzar las fronteras de la organización, exige la atención a los flujos de datos, implicaciones legales, monitoreo y la protección.</p> <p>Podrían ser necesarios controles adicionales con el fin de proteger la información sensible que pasa por las redes publicas.</p>
	Prepare e implante estándares, directrices y procedimientos de seguridad técnicos para redes y herramientas de seguridad de red como IDS/IPS (detección y prevención de intrusiones), gestión de vulnerabilidades, etc.
	Número de incidentes de seguridad de red identificados en el mes anterior, dividido por categorías de leve / importante / grave, con análisis de tendencias y descripción comentada de todo incidente serio y tendencia adversa.

0 Comments [Show recent to old](#)
[Post a comment](#)

[Attachments](#) (2)

 [RSS of this page](#)

Author: [aglone](#) **Version:** [1.5](#) **Last Edited By:** [aglone3](#) **Modified:** 26 - days ago

Información de contacto

servicios@iso27002.es

Quick Search

Navigate pages | Site Map

10 6 Gestión de redes

- 10. 6. 1. Controles de red
- 10. 6. 2. Seguridad en los servicios de red

10. 6. 1. Controles de red



Control:

Se deberían mantener y controlar adecuadamente las redes para protegerlas de amenazas y mantener la seguridad en los sistemas y aplicaciones que utilizan las redes, incluyendo la información en tránsito.








(consultar 10.1.3)

(consultar 11.4 y 12.3)

Infomación adicional:

Se puede encontrar información adicional sobre en seguridad de redes en ISO/IEC 18028, *Tecnología de la información. Técnicas de seguridad. Seguridad de la red de tecnología de la información*

Posibles Soluciones a este control:

	Nmap ("Network Mapper") es una utilidad libre y en código abierto de exploración de redes o auditoría de seguridad. Útil para inventario de red, planificación de actualizaciones y monitorización de disponibilidad de servidores o servicios (inglés)	NMAP
	The OSWA-Assistant™ is a freely-downloadable, self-contained, wireless-auditing toolkit for both IT-security professionals and End-users alike.	OSWA
	Kismet identifies networks by passively collecting packets and detecting standard named networks, detecting (and given time, decloaking) hidden networks, and inferring the presence of nonbeaconing networks via data traffic.	Kismet
	KisMAC is a free, open source wireless stumbling and security tool for Mac OS X.	Kismac
	Freeware employee monitoring. Network-Tools owner sues Microsoft, Cisco, Comcast and TRUSTe over IP Address Blacklisting. Suit alleges eavdropping, privacy policy fraud, breach of contract and defamation.	NetworkTools
	Free ISO 27001/ISO17799 Wireless LAN Security Summary	controlscada
	Flint examines firewalls, quickly computes the effect of all the configuration rules, and then spots problems	Matasano Flint

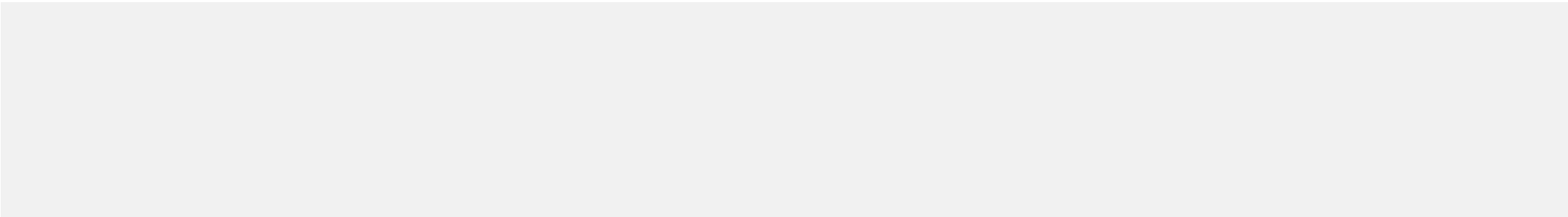
0 Comments [Show recent to old](#)
[Post a comment](#)

 [RSS of this page](#)

Author: [aglone](#) Version: [1.1](#) Last Edited By: [aglone3](#) Modified: 27 - days ago

Información de contacto

servicios@iso27002.es



Quick Search

Navigate pages | Site Map

10 6 Gestión de redes

10. 6. 1. Controles de red

10. 6. 2. Seguridad en los servicios de red

10. 6. 2. Seguridad en los servicios de red



Control:

Se deberían identificar e incluir, en cualquier acuerdo sobre servicios de red, las características de seguridad, los niveles de servicio y los requisitos de gestión de todos los servicios de red, independientemente de que estos servicios sean provistos desde la propia organización o se contratan desde el exterior.

Posibles Soluciones a este control:

	Cisco Router Audit Tool for Windows and Unix. Ability to score Cisco Router IOS, Ability to score Cisco PIX firewalls and Includes benchmark documents (PDF) for both Cisco IOS and Cisco ASA, FWSM, and PIX security settings. (Inglés)	RAT Cisco
	This guide discusses the Cisco SAFE best practices, designs and configurations, and provides network and security engineers with the necessary information to help them succeed in designing, implementing and operating secure network infrastructures based on Cisco products and technologies. (Inglés)	SAFE Cisco
	Open Source Tripwire® software is a security and data integrity tool useful for monitoring and alerting on specific file change(s) on a range of systems. The project is based on code originally contributed by Tripwire, Inc. in 2000.	Tripwire
	Advanced Intrusion Detection Environment. Host-based tool.	AIDE
	<i>Open-source</i> host-based intrusion detection system (HIDS) provides file integrity checking and log file monitoring/analysis, as well as rootkit detection, port monitoring, detection of rogue SUID executables, and hidden processes. Designed to monitor multiple hosts with potentially different operating systems (Unix, Linux, Cygwin/Windows).	Samhain

0 Comments [Show recent to old](#)
[Post a comment](#)

RSS of this page

Author: [aglone](#) Version: [1.1](#) Last Edited By: [aglone3](#) Modified: 27 - days ago

Información de contacto

servicios@iso27002.es

Quick Search

- Navigate pages | Site Map
- ISO 27002

05. Política de Seguridad

06. Organización de la Seguridad de Información

07. Gestión de Activos

08. Seguridad ligada a los Recursos Humanos

09. Seguridad Física y del Entorno

10. Gestión de Comunicaciones y Operaciones

10 1 Procedimientos y responsabilidades de operación

10 2 Supervisión de los servicios contratados a terceros

10 3 Planificación y aceptación del sistema

10 4 Protección contra software malicioso y código móvil

10 5 Gestión interna de soportes y recuperación

10 6 Gestión de redes

10 7 Utilización y seguridad de los soportes de información

10. 7. 1. Gestión de soportes extraíbles

10. 7. 2. Eliminación de soportes

10. 7. 3. Procedimientos de utilización de la información

10. 7. 4. Seguridad de la documentación de sistemas

10 8 Intercambio de información y software

10 9 Servicios de comercio electrónico

10 10 Monitorización

11. Control de Accesos

12. Adquisición, Desarrollo y Mantenimiento de Sistemas de Información

13. Gestión de Incidentes de Seguridad de la Información

14. Gestión de Continuidad del Negocio

15. Conformidad





Objetivos

Contacto

Aviso Legal

10 7 Utilización y seguridad de los soportes de información



	Evitar la divulgación, modificación, retirada o destrucción de activos no autorizada e interrupciones en las actividades de la organización.
	Los medios deberían ser controlados y físicamente protegidos. Se deberían establecer los procedimientos operativos adecuados para proteger los documentos, medios informáticos (discos, cintas, etc.), datos de entrada o salida y documentación del sistema contra la divulgación, modificación, retirada o destrucción de activos no autorizadas .
	Asegure los soportes y la información en tránsito no solo físico sino electrónico (a través de las redes). Encripte todos los datos sensibles o valiosos antes de ser transportados.
	Porcentaje de soportes de backup o archivo que están totalmente encriptados.

0 Comments

Show recent to old

Post a comment

Attachments (2)



RSS of this page

Author: [aglone](#)

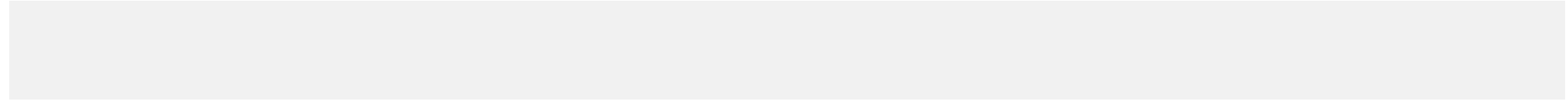
Version: [1.4](#)

Last Edited By: [aglone3](#)

Modified: 26 - days ago

Información de contacto

servicios@iso27002.es



Quick Search

Navigate pages | [Site Map](#)

10 7 Utilización y seguridad de los soportes de información

- **10. 7. 1. Gestión de soportes extraíbles**
- 10. 7. 2. Eliminación de soportes
- 10. 7. 3. Procedimientos de utilización de la información
- 10. 7. 4. Seguridad de la documentación de sistemas

 [Site Home](#) » [10. Gestión de Comunicaciones y Operaciones](#) » [10 7 Utilización y seguridad de los soportes de información](#) » 10. 7. 1. Gestión de soportes extraíbles

10. 7. 1. Gestión de soportes extraíbles



Control:

Se deberían establecer procedimientos para la gestión de los medios informáticos removibles.

Posibles Soluciones a este control:

Espacio pendiente de posibles aportaciones.

0 Comments [Show recent to old](#)
[Post a comment](#)

 [RSS of this page](#)

Author: [aglone](#) Version: [1.1](#) Last Edited By: [aglone3](#) Modified: 27 - days ago

Información de contacto

servicios@iso27002.es

Quick Search

- Navigate pages | Site Map
- 10 7 Utilización y seguridad de los soportes de información
 - 10. 7. 1. Gestión de soportes extraíbles
 - 10. 7. 2. Eliminación de soportes**
 - 10. 7. 3. Procedimientos de utilización de la información
 - 10. 7. 4. Seguridad de la documentación de sistemas

 [Site Home](#) » [10. Gestión de Comunicaciones y Operaciones](#) » [10 7 Utilización y seguridad de los soportes de información](#) » 10. 7. 2. Eliminación de soportes

10. 7. 2. Eliminación de soportes





Control:

Se deberían eliminar los medios de forma segura y sin riesgo cuando ya no sean requeridos, utilizando procedimientos formales.

([consultar 9.2.6](#))

Posibles Soluciones a este control:

	NAID ® es la asociación internacional de empresas que prestan servicios de destrucción de la información. Enlace para localizar sus miembros de los distintos países e información sobre normas, ética y auditorías de certificación de empresas.	naidonline.org
	Eraser is an advanced security tool for Windows which allows you to completely remove sensitive data from your hard drive by overwriting it several times with carefully selected patterns. Eraser is currently supported under Windows XP (with Service Pack 3), Windows Server 2003 (with Service Pack 2), Windows Vista, Windows Server 2008, Windows 7 and Windows Server 2008 R2. Eraser is Free software and its source code is released under GNU General Public License..	Eraser

0 Comments [Show recent to old](#)
[Post a comment](#)

 [RSS of this page](#)

Author: [aglone](#) Version: [1.1](#) Last Edited By: [aglone3](#) Modified: 27 - days ago

Información de contacto

servicios@iso27002.es

Quick Search

- Navigate pages | Site Map
- 10 7 Utilización y seguridad de los soportes de información
 - 10. 7. 1. Gestión de soportes extraíbles
 - 10. 7. 2. Eliminación de soportes
 - 10. 7. 3. Procedimientos de utilización de la información**
 - 10. 7. 4. Seguridad de la documentación de sistemas

 [Site Home](#) >> [10. Gestión de Comunicaciones y Operaciones](#) >> [10 7 Utilización y seguridad de los soportes de información](#) >> 10.

7. 3. Procedimientos de utilización de la información

10. 7. 3. Procedimientos de utilización de la información



Control:

Se deberían establecer procedimientos para la manipulación y almacenamiento de la información con el objeto de proteger esta información contra divulgaciones o usos no autorizados o inadecuados.

([consultar 7.2](#))

Posibles Soluciones a este control:

Espacio pendiente de posibles aportaciones.

0 Comments [Show recent to old](#)
[Post a comment](#)

 [RSS of this page](#)

Author: [aglone](#) Version: [1.1](#) Last Edited By: [aglone3](#) Modified: 27 - days ago

Información de contacto

servicios@iso27002.es

Quick Search

- Navigate pages | [Site Map](#)
- 10 7 Utilización y seguridad de los soportes de información

10. 7. 1. Gestión de soportes extraíbles

10. 7. 2. Eliminación de soportes

10. 7. 3. Procedimientos de utilización de la información

10. 7. 4. Seguridad de la documentación de sistemas

[Site Home](#) » [10. Gestión de Comunicaciones y Operaciones](#) » [10 7 Utilización y seguridad de los soportes de información](#) » 10. 7. 4. Seguridad de la documentación de sistemas

10. 7. 4. Seguridad de la documentación de sistemas



Control:

Se debería proteger la documentación de los sistemas contra accesos no autorizados.

Posibles Soluciones a este control:

Espacio pendiente de posibles aportaciones.

0 Comments [Show recent to old](#)
[Post a comment](#)

[RSS of this page](#)

Author: [aglone](#) Version: [1.1](#) Last Edited By: [aglone3](#) Modified: 27 - days ago

Información de contacto

servicios@iso27002.es

Quick Search

- Navigate pages | Site Map
- ISO 27002

05. Política de Seguridad

06. Organización de la Seguridad de Información

07. Gestión de Activos

08. Seguridad ligada a los Recursos Humanos

09. Seguridad Física y del Entorno

10. Gestión de Comunicaciones y Operaciones

10 1 Procedimientos y responsabilidades de operación

10 2 Supervisión de los servicios contratados a terceros

10 3 Planificación y aceptación del sistema

10 4 Protección contra software malicioso y código móvil

10 5 Gestión interna de soportes y recuperación

10 6 Gestión de redes

10 7 Utilización y seguridad de los soportes de información

10 8 Intercambio de información y software

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 10 Monitorización

11. Control de Accesos

12. Adquisición, Desarrollo y Mantenimiento de Sistemas de Información

13. Gestión de Incidentes de Seguridad de la Información

14. Gestión de Continuidad del Negocio


15. Conformidad

Objetivos

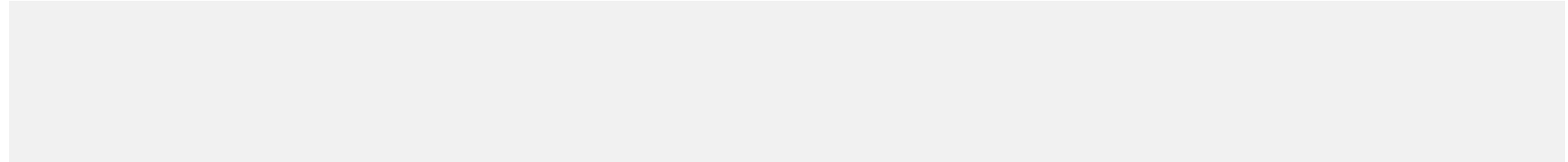
Contacto

Aviso Legal
- Site Home » 10. Gestión de Comunicaciones y Operaciones » 10 8 Intercambio de información y software
- 10 8 Intercambio de información y software
-
- | | |
|---|--|
|  | Mantener la seguridad de la información y del software que se intercambian dentro de la organización o con cualquier entidad externa. |
|  | Se deberían realizar los intercambios sobre la base de una política formal de intercambio, según los acuerdos de intercambio y cumplir con la legislación correspondiente (consultar cláusula 15).

Se deberían establecer procedimientos y normas para proteger la información y los medios físicos que contienen información en tránsito. |
|  | Estudie canales de comunicaciones alternativos y "pre-autorizados", en especial direcciones de e-mail secundarias por si fallan las primarias o el servidor de correo, y comunicaciones offline por si caen las redes.

El verificar canales de comunicación alternativos reducirá el estrés en caso de un incidente real. |
|  | Porcentaje de enlaces de terceras partes para los cuales se han (a) definido y (b) implementado satisfactoriamente los requisitos de seguridad de la información. |
- 0 Comments [Show recent to old](#)
[Post a comment](#)
- [Attachments](#) (2)
-  RSS of this page

Author: [aglone](#) Version: [1.5](#) Last Edited By: [aglone3](#) Modified: 26 - days ago
- Información de contacto
- servicios@iso27002.es
- Powered by [Zoho Wiki](#) | [Zoho](#) | [Report Abuse](#) | [Wiki Index](#) | [Site Map](#) | [Help](#) | [Feedback](#) | [Jump Start with 2 Free Wikis](#) | [Sign in](#)
- http://iso27002.wiki.zoho.com/10-8-Intercambio-de-información-y-software.html[28/01/2011 08:27:14 p.m.]



Quick Search

Navigate pages | Site Map

10 8 Intercambio de información y software

- 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

Site Home » 10. Gestión de Comunicaciones y Operaciones » 10 8 Intercambio de información y software » 10. 8. 1. Políticas y procedimientos de intercambio de información

10. 8. 1. Políticas y procedimientos de intercambio de información



Control:

Se deberían establecer políticas, procedimientos y controles formales de intercambio con objeto de proteger la información mediante el uso de todo tipo de servicios de comunicación.

(consultar 10.4.1)

(consultar 7.1.3)





(consultar 12.3)

(consultar 15)

(consultar 10.3 y 14)

(consultar 11)

Posibles Soluciones a este control:

 Firefox	Complementos para navegador relacionados con la Privacidad y seguridad	Complementos FireFox
	Análisis de vulnerabilidades para PBX (voz)	Special Publication NIST 800-24
 VAST VIPER Assessment Security Tools	VAST has been released with UCSniff 3.0 which includes GUI interface, VoIP video realtime monitoring, TFTP MitM modification of IP phone features, Gratuitous ARP disablement bypass support, and support for several compression codecs	VIPERVAST
	WarVOX is a suite of tools for exploring, classifying, and auditing telephone systems.	WarVOX

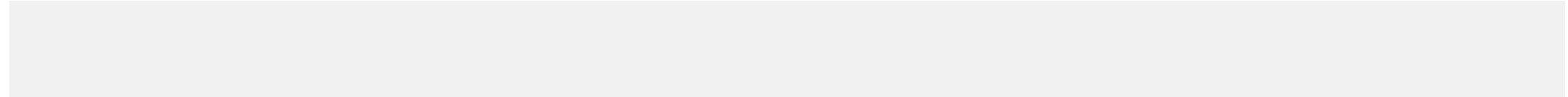
0 Comments [Show recent to old](#)
[Post a comment](#)

 RSS of this page

Author: [aglone](#) Version: [1.1](#) Last Edited By: [aglone3](#) Modified: 27 - days ago

Información de contacto

servicios@iso27002.es



Quick Search

- Navigate pages | Site Map
- 10 8 Intercambio de información y software

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

Site Home » 10. Gestión de Comunicaciones y Operaciones » 10 8 Intercambio de información y software » 10. 8. 2. Acuerdos de intercambio

10. 8. 2. Acuerdos de intercambio



Control:

Se deberían establecer acuerdos para el intercambio de información y software entre la organización y las partes externas.

(consultar 15.1.2 y 15.1.4)

(consultar 12.3)

(consultar 10.8.3)

Posibles Soluciones a este control:

	Free Open-Source Disk Encryption Software	http://www.truecrypt.org
--	---	---

0 Comments Show recent to old
Post a comment

 RSS of this page

Author: [aglone](#) Version: [1.1](#) Last Edited By: [aglone3](#) Modified: 27 - days ago

Información de contacto

servicios@iso27002.es

Quick Search

Navigate pages | Site Map

10 8 Intercambio de información y software

- 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

Site Home » 10. Gestión de Comunicaciones y Operaciones » 10 8 Intercambio de información y software » 10. 8. 3. Soportes físicos en tránsito

10. 8. 3. Soportes físicos en tránsito



Control:

Se deberían proteger los medios que contienen información contra acceso no autorizado, mal uso o corrupción durante el transporte fuera de los limites físicos de la organización.

Posibles Soluciones a este control:

	Free Open-Source Disk Encryption Software	Truecrypt
	Rohos Mini Drive es una aplicación gratuita que permite crear particiones con cifrado, ocultarlas y protegerlas con contraseña en cualquier unidad USB flash. Con los datos cifrados puede trabajar en cualquier ordenador aún sin derechos administrativos. El programa crea una partición protegida con el estándar AES 256 bits accesible sólo con la clave secreta que elijas.	Rohos

0 Comments [Show recent to old](#)
[Post a comment](#)

RSS of this page

Author: [aglone](#) Version: [1.1](#) Last Edited By: [aglone3](#) Modified: 27 - days ago

Información de contacto

servicios@iso27002.es

Quick Search

- Navigate pages | Site Map
- 10 8 Intercambio de información y software
 - 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

 [Site Home](#) » [10. Gestión de Comunicaciones y Operaciones](#) » [10 8 Intercambio de información y software](#) » 10. 8. 4. Mensajería electrónica


10. 8. 4. Mensajería electrónica



Control:

Se debería proteger adecuadamente la información contenida en la mensajería electrónica.

Posibles Soluciones a este control:

	Herramienta gratuita y genera firmas codificadas según el formato PKCS#7 o CMS (Cryptographic Message Syntax)	AlbaliaFirma.zip
---	---	----------------------------------

0 Comments [Show recent to old](#)
[Post a comment](#)

 [RSS of this page](#)

Author: [aglone](#) Version: [1.1](#) Last Edited By: [aglone3](#) Modified: 27 - days ago

Información de contacto

servicios@iso27002.es

Quick Search

- Navigate pages | Site Map
- 10 8 Intercambio de información y software

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

Site Home » 10. Gestión de Comunicaciones y Operaciones » 10 8 Intercambio de información y software » 10. 8. 5. Sistemas de información empresariales

10. 8. 5. Sistemas de información empresariales



Control:

Se deberían desarrollar e implementar políticas y procedimientos con el fin de proteger la información asociada con la interconexión de sistemas de información del negocio.

(consultar 7.2)

(consultar 6.2)

(consultar 10.5.1)

(consultar 14)

Posibles Soluciones a este control:

Espacio pendiente de posibles aportaciones.

0 Comments

Show recent to old

Post a comment

RSS of this page

Author: [aglone](#)

Version: [1.1](#)

Last Edited By: [aglone3](#)

Modified: 27 - days ago

Información de contacto

servicios@iso27002.es

Quick Search

- Navigate pages | Site Map
- ISO 27002

05. Política de Seguridad

06. Organización de la Seguridad de Información

07. Gestión de Activos

08. Seguridad ligada a los Recursos Humanos

09. Seguridad Física y del Entorno

10. Gestión de Comunicaciones y Operaciones

10 1 Procedimientos y responsabilidades de operación

10 2 Supervisión de los servicios contratados a terceros

10 3 Planificación y aceptación del sistema

10 4 Protección contra software malicioso y código móvil

10 5 Gestión interna de soportes y recuperación

10 6 Gestión de redes

10 7 Utilización y seguridad de los soportes de información

10 8 Intercambio de información y software

10 9 Servicios de comercio electrónico

10. 9. 1. Seguridad en comercio electrónico

10. 9. 2. Seguridad en transacciones en línea

10 9 3 Seguridad en información pública

10 10 Monitorización

11. Control de Accesos

12. Adquisición, Desarrollo y Mantenimiento de Sistemas de Información

13. Gestión de Incidentes de Seguridad de la Información

14. Gestión de Continuidad del Negocio

15. Conformidad





Objetivos

Contacto

Aviso Legal

10 9 Servicios de comercio electrónico



	Asegurar la seguridad de los servicios de comercio electrónico y de su uso seguro.
	<p>Se deberían considerar las implicaciones de seguridad asociadas con el uso de servicios de comercio electrónico, incluyendo transacciones en línea y los requisitos para los controles.</p> <p>La integridad y disponibilidad de la información electrónica publicada a través de sistemas disponibles de publicidad deberían ser también consideradas.</p>
	Trabaje estrechamente con las unidades de negocio para desarrollar un eBusiness seguro, incorporando requisitos de seguridad de la información en los proyectos, y con ello en los sistemas de eCommerce, desde el principio (también en cualquier cambio/actualización posterior). Insista en el valor añadido de la seguridad en la reducción de riesgos comerciales, legales y operativos asociados al eBusiness. Trabaje los 3 aspectos clave de la seguridad: confidencialidad, integridad y disponibilidad
	"Estado de la eSeguridad", es decir, un informe sobre el nivel global de confianza de la dirección, basado en el análisis de los últimos tests de penetración, incidentes actuales o recientes, vulnerabilidades actuales conocidas, cambios planificados, etc..

0 Comments [Show recent to old](#)
[Post a comment](#)

Attachments (4)

 RSS of this page

Author: [aglone](#) Version: [1.4](#) Last Edited By: [aglone3](#) Modified: 26 - days ago

Información de contacto

servicios@iso27002.es

Quick Search

Navigate pages | Site Map

10 9 Servicios de comercio electrónico

- 10. 9. 1. Seguridad en comercio electrónico
- 10. 9. 2. Seguridad en transacciones en línea
- 10 9 3 Seguridad en información pública

Site Home » 10. Gestión de Comunicaciones y Operaciones » 10 9 Servicios de comercio electrónico » 10. 9. 1. Seguridad en comercio electrónico

10. 9. 1. Seguridad en comercio electrónico



Control:

Se debería proteger la información involucrada en el comercio electrónico que pasa por redes publicas contra actividades fraudulentas, disputas por contratos y divulgación o modificación no autorizadas.



([consultar 12.3](#))

([consultar 15.1](#), [15.1.6](#))

([consultar 11.4.6](#))

([consultar 12.3](#))

Posibles Soluciones a este control:

	Herramienta gratuita y genera firmas codificadas según el formato PKCS#7 o CMS (Cryptographic Message Syntax)	AlbaliaFirma.zip
	Many European identity cards now contain a smart-card chip, equipped with functionalities for online authentication. They are usually called 'electronic identity cards' (eID cards). This report focuses on authentication using smart cards and compares this approach with other common means of authentication.	ENISA report

0 Comments [Show recent to old](#)
[Post a comment](#)

 RSS of this page

Author: [aglone](#) Version: [1.1](#) Last Edited By: [aglone3](#) Modified: 27 - days ago

Información de contacto

servicios@iso27002.es

Quick Search

Navigate pages | Site Map

10 9 Servicios de comercio electrónico

10. 9. 1. Seguridad en comercio electrónico

10. 9. 2. Seguridad en transacciones en línea

10 9 3 Seguridad en información pública

Site Home » 10. Gestión de Comunicaciones y Operaciones » 10 9 Servicios de comercio electrónico » 10. 9. 2. Seguridad en transacciones en línea



10. 9. 2. Seguridad en transacciones en línea



Control:

Se debería proteger la información implicada en las transacciones en línea para prevenir la transmisión incompleta, enrutamiento equivocado, alteración, divulgación, duplicación o repetición no autorizada del mensaje.

Posibles Soluciones a este control:

	Herramienta gratuita y genera firmas codificadas según el formato PKCS#7 o CMS (Cryptographic Message Syntax)	AlbaliaFirma.zip
	Many European identity cards now contain a smart-card chip, equipped with functionalities for online authentication. They are usually called 'electronic identity cards' (eID cards). This report focuses on authentication using smart cards and compares this approach with other common means of authentication.	ENISA report

0 Comments Show recent to old
Post a comment

 RSS of this page

Author: [aglone](#) Version: [1.1](#) Last Edited By: [aglone3](#) Modified: 27 - days ago

Información de contacto

servicios@iso27002.es

Quick Search

Navigate pages | Site Map

10 9 Servicios de comercio electrónico

10. 9. 1. Seguridad en comercio electrónico

10. 9. 2. Seguridad en transacciones en línea

10 9 3 Seguridad en información pública

Site Home » 10. Gestión de Comunicaciones y Operaciones » 10 9 Servicios de comercio electrónico » 10 9 3 Seguridad en información pública

10 9 3 Seguridad en información pública



Control:

Se debería proteger la integridad de la información que pone a disposición en un sistema de acceso público para prevenir modificaciones no autorizadas.

(consultar 12.3)

(consultar 15.1.4)

Posibles Soluciones a este control:

	Herramienta gratuita y genera firmas codificadas según el formato PKCS#7 o CMS (Cryptographic Message Syntax)	AlbaliaFirma.zip
	iScanner is free open source tool lets you detect and remove malicious codes and web pages viruses from your Linux/Unix server easily and automatically.	iScanner
	MANDIANT Web Historian helps users review the list of websites (URLs) that are stored in the history files of the most commonly used browsers, including: Internet Explorer, Firefox and Chrome.	Mandiant WEB Historian

0 Comments [Show recent to old](#)
[Post a comment](#)

[Attachments](#) (1)

RSS of this page

Author: [aglone](#) Version: [1.2](#) Last Edited By: [aglone3](#) Modified: 27 - days ago


Información de contacto

servicios@iso27002.es





Quick Search

- Navigate pages | Site Map
- ISO 27002
 - 05. Política de Seguridad
 - 06. Organización de la Seguridad de Información
 - 07. Gestión de Activos
 - 08. Seguridad ligada a los Recursos Humanos
 - 09. Seguridad Física y del Entorno
 - 10. Gestión de Comunicaciones y Operaciones
 - 10 1 Procedimientos y responsabilidades de operación
 - 10 2 Supervisión de los servicios contratados a terceros
 - 10 3 Planificación y aceptación del sistema
 - 10 4 Protección contra software malicioso y código móvil
 - 10 5 Gestión interna de soportes y recuperación
 - 10 6 Gestión de redes
 - 10 7 Utilización y seguridad de los soportes de información
 - 10 8 Intercambio de información y software
 - 10 9 Servicios de comercio electrónico
 - 10 10 Monitorización**
 - 10. 10. 1. Registro de incidencias
 - 10. 10. 2. Supervisión del uso de los sistemas
 - 10. 10. 3. Protección de los registros de incidencias
 - 10. 10. 4. Diarios de operación del administrador y operador
 - 10. 10. 5. Registro de fallos
 - 10. 10. 6. Sincronización del reloj
 - 11. Control de Accesos
 - 12. Adquisición, Desarrollo y Mantenimiento de Sistemas de Información
 - 13. Gestión de Incidentes de Seguridad de la Información
 - 14. Gestión de Continuidad del Negocio
 - 15. Conformidad
 - Objetivos
 - Contacto
 - Aviso Legal

10 10 Monitorización



Espacio de Patrocinio disponible

 Objetivo	Detectar actividades de procesamiento de la información no autorizadas.
 Principios	<p>Los sistemas deberían ser monitoreados y los eventos de la seguridad de información registrados. El registro de los operadores y el registro de fallos debería ser usado para garantizar la identificación de los problemas del sistema de información.</p> <p>La organización debería cumplir con todos los requerimientos legales aplicables para el monitoreo y el registro de actividades.</p> <p>El monitoreo del sistema debería ser utilizado para verificar la efectividad de los controles adoptados y para verificar la conformidad del modelo de política de acceso.</p>
	<p>El viejo axioma del aseguramiento de la calidad "no puedes controlar lo que no puedes medir o monitorizar" es también válido para la seguridad de la información.</p> <p>La necesidad de implantar procesos de supervisión es más evidente ahora que la medición de la eficacia de los controles se ha convertido en un requisito específico.</p> <p>Analice la criticidad e importancia de los datos que va a monitorizar y cómo esto afecta a los objetivos globales de negocio de la organización en relación a la seguridad de la información.</p>
	Porcentaje de sistemas cuyos logs de seguridad (a) están adecuadamente configurados, (b) son transferidos con seguridad a un sistema de gestión centralizada de logs y (c) son monitorizados/revisados/evaluados regularmente. Tendencia en el número de entradas en los logs de seguridad que (a) han sido registradas, (b) han sido analizadas y (c) han conducido a actividades de seguimiento.

0 Comments [Show recent to old](#)
[Post a comment](#)

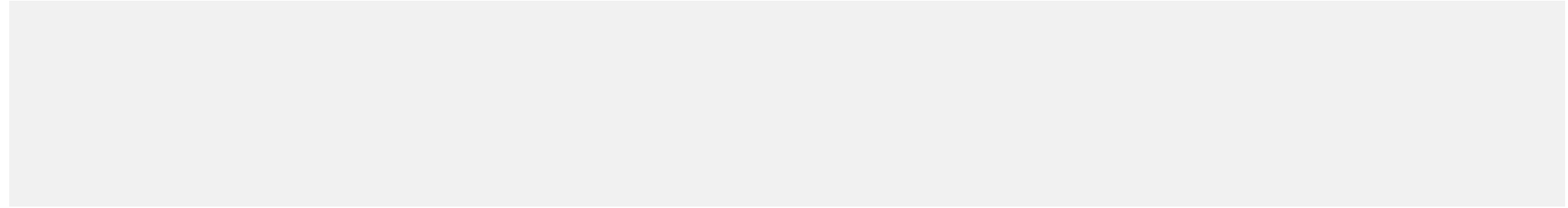
[Attachments](#) (2)

 [RSS of this page](#)

Author: [aglone](#) Version: [1.3](#) Last Edited By: [aglone3](#) Modified: 26 - days ago

Información de contacto

servicios@iso27002.es



Quick Search

- Navigate pages | Site Map
- 10 10 Monitorización

10. 10. 1. Registro de incidencias

10. 10. 2. Supervisión del uso de los sistemas

10. 10. 3. Protección de los registros de incidencias

10. 10. 4. Diarios de operación del administrador y operador

10. 10. 5. Registro de fallos

10. 10. 6. Sincronización del reloj

Site Home » 10. Gestión de Comunicaciones y Operaciones » 10 10 Monitorización » 10. 10. 1. Registro de incidencias

10. 10. 1. Registro de incidencias






Control:

Se deberían producir y mantener durante un periodo establecido los registros de auditoria con la grabación de las actividades de los usuarios, excepciones y eventos de la seguridad de información, con el fin de facilitar las investigaciones futuras y el monitoreo de los controles de acceso.

(consultar 15.1.4)

(consultar 10.1.3)

Posibles Soluciones a este control:

	Solutions from Q1 Labs are quickly becoming the standard for centralized management of enterprise network and security information.	Q1labs
	Splunk is an IT search and analysis engine. It's software that lets you index, search, alert and report on live and historical IT data – giving you visibility across your entire IT infrastructure from one location in real time. Reduce the time to troubleshoot IT problems and security incidents to minutes or seconds instead of hours or days.	Splunk
	The Samhain host-based intrusion detection system (HIDS) provides file integrity checking and log file monitoring/analysis, as well as rootkit detection, port monitoring, detection of rogue SUID executables, and hidden processes. Samhain been designed to monitor multiple hosts with potentially different operating systems, providing centralized logging and maintenance, although it can also be used as standalone application on a single host.	Samhain

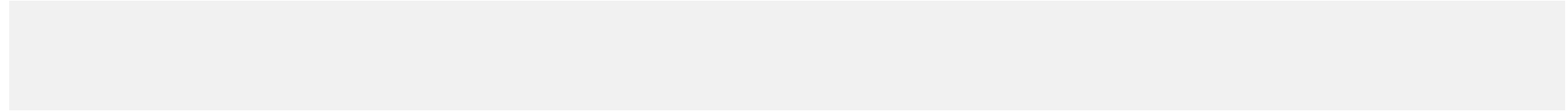
0 Comments [Show recent to old](#)
[Post a comment](#)

 RSS of this page

Author: [aglone](#) Version: [1.1](#) Last Edited By: [aglone3](#) Modified: 27 - days ago

Información de contacto

servicios@iso27002.es



Quick Search

- Navigate pages | Site Map
- 10 10 Monitorización

10. 10. 1. Registro de incidencias

10. 10. 2. Supervisión del uso de los sistemas

10. 10. 3. Protección de los registros de incidencias

10. 10. 4. Diarios de operación del administrador y operador

10. 10. 5. Registro de fallos

10. 10. 6. Sincronización del reloj

Site Home » 10. Gestión de Comunicaciones y Operaciones » 10 10 Monitorización » 10. 10. 2. Supervisión del uso de los sistemas

10. 10. 2. Supervisión del uso de los sistemas



Control:

Se deberían establecer procedimientos para el uso del monitoreo de las instalación de procesamiento de información y revisar regularmente los resultados de las actividades de monitoreo.

(Consultar 13.1.1)

Posibles Soluciones a este control:

	Uniblue libre y la biblioteca en línea comprensiva de procesos está para cada uno que necesite saber la naturaleza y el propósito exactos de cada proceso que debe, y no deba, funcionar en su PC	Processlibrary
	Spiceworks is the complete network management & monitoring, helpdesk, PC inventory & software reporting solution to manage Everything IT in small and medium businesses.	Spiceworks
	Paglo is on-demand tool. Businesses can discover all their IT information and get instant answers to their computer, network, and security questions.	Paglo
	Snort® is an open source network intrusion prevention and detection system (IDS/IPS) developed by Sourcefire. Combining the benefits of signature, protocol and anomaly-based inspection, Snort is the most widely deployed IDS/IPS technology worldwide.	Snort
	Open Source Host-based Intrusion Detection System. It performs log analysis, file integrity checking, policy monitoring, rootkit detection, real-time alerting and active response. It runs on most operating systems, including Linux, MacOS, Solaris, HP-UX, AIX and Windows.	OSSEC
	The software-based solution captures user activity in any user session, including Terminal, Remote Desktop, Citrix, VMWare, VNC, NetOP and PC Anywhere. ObserveIT Xpress is a completely free version of the ObserveIT product, with no time limit. The free version can monitor a maximum of 5 servers	ObserveIT Xpress

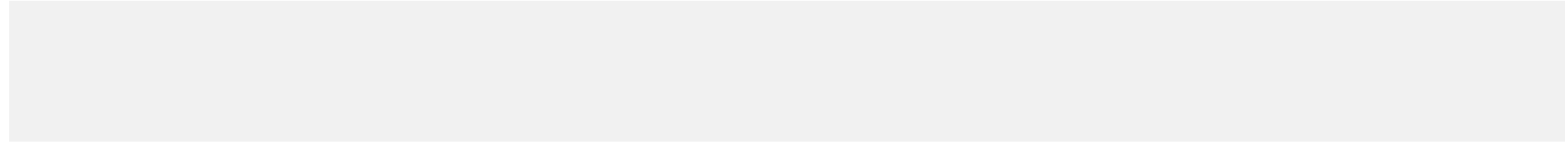
0 Comments Show recent to old
Post a comment

RSS of this page

Author: [aglone](#) Version: [1.1](#) Last Edited By: [aglone3](#) Modified: 27 - days ago

Información de contacto

servicios@iso27002.es



Quick Search

- Navigate pages | Site Map
- 10 10 Monitorización

10. 10. 1. Registro de incidencias

10. 10. 2. Supervisión del uso de los sistemas

10. 10. 3. Protección de los registros de incidencias

10. 10. 4. Diarios de operación del administrador y operador

10. 10. 5. Registro de fallos

10. 10. 6. Sincronización del reloj

Site Home » 10. Gestión de Comunicaciones y Operaciones » 10 10 Monitorización » 10. 10. 3. Protección de los registros de incidencias

10. 10. 3. Protección de los registros de incidencias



Control:

Se deberían proteger los servicios y la información de registro de la actividad contra acciones forzosas o accesos no autorizados.

(consultar 13.2.3)

Posibles Soluciones a este control:

Espacio pendiente de posibles aportaciones.

0 Comments [Show recent to old](#)
[Post a comment](#)

RSS of this page

Author: [aglone](#) Version: [1.1](#) Last Edited By: [aglone3](#) Modified: 27 - days ago

Información de contacto

servicios@iso27002.es

Quick Search

- Navigate pages | Site Map
- 10 10 Monitorización

10. 10. 1. Registro de incidencias

10. 10. 2. Supervisión del uso de los sistemas

10. 10. 3. Protección de los registros de incidencias

10. 10. 4. Diarios de operación del administrador y operador

10. 10. 5. Registro de fallos

10. 10. 6. Sincronización del reloj

Site Home » 10. Gestión de Comunicaciones y Operaciones » 10 10 Monitorización » 10. 10. 4. Diarios de operación del administrador y operador


10. 10. 4. Diarios de operación del administrador y operador



Control:

Se deberían registrar las actividades del administrador y de los operadores del sistema.

Posibles Soluciones a este control:

logo.gif 	The software-based solution captures user activity in any user session, including Terminal, Remote Desktop, Citrix, VMWare, VNC, NetOP and PC Anywhere. ObserveIT Xpress is a completely free version of the ObserveIT product, with no time limit. The free version can monitor a maximum of 5 servers	ObserveIT Xpress
--	---	----------------------------------

0 Comments [Show recent to old](#)
[Post a comment](#)

 RSS of this page

Author: [aglone](#) Version: [1.1](#) Last Edited By: [aglone3](#) Modified: 27 - days ago

Información de contacto

servicios@iso27002.es

Quick Search

- Navigate pages | Site Map
- 10 10 Monitorización

10. 10. 1. Registro de incidencias

10. 10. 2. Supervisión del uso de los sistemas

10. 10. 3. Protección de los registros de incidencias

10. 10. 4. Diarios de operación del administrador y operador

10. 10. 5. Registro de fallos

10. 10. 6. Sincronización del reloj



10. 10. 5. Registro de fallos



Control:

Se deberían registrar, analizar y tomar acciones apropiadas de las averías.

Posibles Soluciones a este control:

	Splunk is an IT search and analysis engine. It's software that lets you index, search, alert and report on live and historical IT data – giving you visibility across your entire IT infrastructure from one location in real time. Reduce the time to troubleshoot IT problems and security incidents to minutes or seconds instead of hours or days.	Splunk
	dradis is an open source framework to enable effective information sharing. dradis is a self-contained web application that provides a centralised repository of information to keep track of what has been done so far, and what is still ahead.	dradis

0 Comments [Show recent to old](#)
[Post a comment](#)

 RSS of this page

Author: [aglone](#) Version: [1.1](#) Last Edited By: [aglone3](#) Modified: 27 - days ago

Información de contacto

servicios@iso27002.es

Quick Search

- Navigate pages | Site Map
- 10 10 Monitorización

10. 10. 1. Registro de incidencias

10. 10. 2. Supervisión del uso de los sistemas

10. 10. 3. Protección de los registros de incidencias

10. 10. 4. Diarios de operación del administrador y operador

10. 10. 5. Registro de fallos

10. 10. 6. Sincronización del reloj

Site Home » 10. Gestión de Comunicaciones y Operaciones » 10 10 Monitorización » 10. 10. 6. Sincronización del reloj



10. 10. 6. Sincronización del reloj



Control:

Se deberían sincronizar los relojes de todos los sistemas de procesamiento de información dentro de la organización o en el dominio de seguridad, con una fuente acordada y exacta de tiempo.

Posibles Soluciones a este control:

	Servidores de hora NTP para todo el mundo	pool.ntp.org
	Enlace con información completa de protocolos y enlaces	Wikipedia

0 Comments [Show recent to old](#)
[Post a comment](#)

 [RSS of this page](#)

Author: [aglone](#) Version: [1.1](#) Last Edited By: [aglone3](#) Modified: 27 - days ago

Información de contacto

servicios@iso27002.es

Quick Search

- Navigate pages | Site Map
- ISO 27002

05. Política de Seguridad

06. Organización de la Seguridad de Información

07. Gestión de Activos

08. Seguridad ligada a los Recursos Humanos

09. Seguridad Física y del Entorno

10. Gestión de Comunicaciones y Operaciones

11. Control de Accesos

11 1 Requerimientos de negocio para el control de accesos

11.1.1. Política de control de accesos

11 2 Gestión de acceso de usuario

11 3 Responsabilidades del usuario

11 4 Control de acceso en red

11 5 Control de acceso al sistema operativo

11 6 Control de acceso a las aplicaciones

11 7 Informática móvil y tele trabajo

12. Adquisición, Desarrollo y Mantenimiento de Sistemas de Información

13. Gestión de Incidentes de Seguridad de la Información

14. Gestión de Continuidad del Negocio


15. Conformidad

Objetivos





Contacto

Aviso Legal

11 1 Requerimientos de negocio para el control de accesos



Espacio de Patrocinio disponible

 <div>Objetivo</div>	Controlar los accesos a la información.
 <div>Principios</div>	<p>Se deberían controlar los accesos a la información, los recursos de tratamiento de la información y los procesos de negocio en base a las necesidades de seguridad y de negocio de la Organización.</p> <p>Las regulaciones para el control de los accesos deberían considerar las políticas de distribución de la información y de autorizaciones.</p>
	<p>Los propietarios de activos de información que son responsables ante la dirección de la protección "sus" activos deberían tener la capacidad de definir y/o aprobar las reglas de control de acceso y otros controles de seguridad.</p> <p>Asegúrese de que se les responsabiliza de incumplimientos, no conformidades y otros incidentes.</p>
	Porcentaje de sistemas y aplicaciones corporativas para los que los "propietarios" adecuados han: (a) sido identificados, (b) aceptado formalmente sus responsabilidades, (c) llevado a cabo -o encargado- revisiones de accesos y seguridad de aplicaciones, basadas en riesgo y (d) definido las reglas de control de acceso basadas en roles.

0 Comments [Show recent to old](#)
[Post a comment](#)

Attachments (2)

 [RSS of this page](#)

Author: [aglone](#) Version: [1.3](#) Last Edited By: [aglone3](#) Modified: 26 - days ago

Información de contacto

servicios@iso27002.es

Quick Search

Navigate pages | Site Map

11 1 Requerimientos de negocio para el control de accesos

11.1.1. Política de control de accesos

Site Home » 11. Control de Accesos » 11 1 Requerimientos de negocio para el control de accesos » 11.1.1. Política de control de accesos

11.1.1. Política de control de accesos



Control:

Se debería establecer, documentar y revisar una política de control de accesos en base a las necesidades de seguridad y de negocio de la Organización.

(consultar también [sección 9](#))

([consultar 7.2](#))

([consultar 15.1](#))

([consultar 11.2.1](#))

([consultar 11.2.4](#))

([consultar 8.3.3](#))

Posibles Soluciones a este control:

Espacio pendiente de posibles aportaciones.

0 Comments [Show recent to old](#)
[Post a comment](#)

RSS of this page

Author: [aglone](#) Version: [1.1](#) Last Edited By: [aglone3](#) Modified: 27 - days ago

Información de contacto

servicios@iso27002.es

Quick Search

- Navigate pages | Site Map
- ISO 27002
- ⊞

 05. Política de Seguridad
- ⊞

 06. Organización de la Seguridad de Información
- ⊞

 07. Gestión de Activos
- ⊞

 08. Seguridad ligada a los Recursos Humanos
- ⊞

 09. Seguridad Física y del Entorno
- ⊞

 10. Gestión de Comunicaciones y Operaciones
- ⊞

 11. Control de Accesos

⊞

 11 1 Requerimientos de negocio para el control de accesos

⊞

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 los usuarios
- ⊞

 11 3 Responsabilidades del usuario
- ⊞

 11 4 Control de acceso en red
- ⊞

 11 5 Control de acceso al sistema operativo
- ⊞

 11 6 Control de acceso a las aplicaciones
- ⊞

 11 7 Informática móvil y tele trabajo

⊞

 12. Adquisición, Desarrollo y Mantenimiento de Sistemas de Información

⊞

 13. Gestión de Incidentes de Seguridad de la Información

⊞

 14. Gestión de Continuidad del Negocio

⊞

 15. Conformidad

●

 Objetivos






●

 Contacto

●

 Aviso Legal

11 2 Gestión de acceso de usuario

	Espacio de Patrocinio disponible
	Garantizar el acceso a los usuarios autorizados e impedir los accesos no autorizados a los sistemas de información.
	<p>Se deberían establecer procedimientos formales para controlar la asignación de los permisos de acceso a los sistemas y servicios de información.</p> <p>Los procedimientos deberían cubrir todas la etapas del ciclo de vida del acceso de los usuarios, desde del registro inicial de los nuevos usuarios hasta su baja cuando ya no sea necesario su acceso a los sistemas y servicios de información.</p> <p>Se debería prestar especial atención, si fuera oportuno, a la necesidad de controlar la asignación de permisos de acceso con privilegios que se salten y anulen la eficacia de los controles del sistema.</p>
	<p>Cree la función diferenciada de "administrador de seguridad", con responsabilidades operativas para aplicar las reglas de control de acceso definidas por los propietarios de las aplicaciones y la dirección de seguridad de la información.</p> <p>Invierta en proporcionar al administrador de seguridad herramientas para realizar sus tareas lo más eficientemente posible.</p>
	Tiempo medio transcurrido entre la solicitud y la realización de peticiones de cambio de accesos y número de solicitudes de cambio de acceso cursadas en el mes anterior (con análisis de tendencias y comentarios acerca de cualquier pico / valle (p. ej., "Implantada nueva aplicación financiera este mes")).

0 Comments

Show recent to old

Post a comment

Attachments (2)

 RSS of this page

Author: [aglone](#)

Version: [1.3](#)

Last Edited By: [aglone3](#)

Modified: 26 - days ago

Información de contacto

servicios@iso27002.es

Quick Search

- Navigate pages | Site Map
- 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 los usuarios

Site Home » 11. Control de Accesos » 11 2 Gestión de acceso de usuario » 11.2.1. Registro de usuario

11.2.1. Registro de usuario



Control:


Debería existir un procedimiento formal de alta y baja de usuarios con objeto de garantizar y cancelar los accesos a todos los sistemas y servicios de información.

(consultar 11.1)

(consultar 10.1.3)

(consultar 11.2.4)

Posibles Soluciones a este control:

 Professional Learn more. Do more.	Documento con modelos y técnicas de control de accesos (inglés)	http://shop.osborne.com
---	---	---

0 Comments [Show recent to old](#)
[Post a comment](#)

 RSS of this page

Author: [aglone](#) Version: [1.1](#) Last Edited By: [aglone3](#) Modified: 27 - days ago

Información de contacto

servicios@iso27002.es

Quick Search

- Navigate pages | Site Map
- 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 los usuarios

Site Home » 11. Control de Accesos » 11 2 Gestión de acceso de usuario » 11.2.2. Gestión de privilegios

11.2.2. Gestión de privilegios



Control:

Se debería restringir y controlar la asignación y uso de los privilegios.

(consultar 11.1.1)

Posibles Soluciones a este control:

	Solución web (free trial 30 days) que permite realizar las tareas más comunes, como las altas y bajas de usuarios y la aplicación de políticas de grupo, a través de un interfaz intuitivo y fácil de aprender. A través de sus informes detallados, ofrece visibilidad completa sobre todos los objetivos en el Directorio Activo.	Manageengine.com
	DB Audit is a complete out-of-the-box database security & auditing solution for Oracle, Sybase, MySQL, DB2 and MS SQL Server. DB Audit allows database and system administrators, security administrators, auditors and operators to track and analyze any database activity including database access and usage, data creation, change or deletion; mananage database users; quickly discover uprotected PCI and PII data; enforce SOX, PCI/CISP, HIPAA, GLBA compliance; and more.	DB Audit
	Once it detects one or more SQL injections on the target host, the user can choose among a variety of options to perform an extensive back-end database management system fingerprint, retrieve DBMS session user and database, enumerate users, password hashes, privileges, databases, dump entire or user's specific DBMS tables/columns, run his own SQL statement, read specific files on the file system and more.	Pangolin audit tool
	UserLock® permite proteger el acceso a las redes de Windows®, impidiendo las conexiones simultáneas, al dar la posibilidad de limitar las conexiones de los usuarios y proporcionando a los administradores el control remoto de las sesiones, de las funcionalidades de alerta, de informes y análisis sobre todas las conexiones/desconexiones efectuadas en sus redes.La versión de evaluación de UserLock es válida durante 180 días. No comporta ninguna limitación en términos de funcionalidades.	Userlock

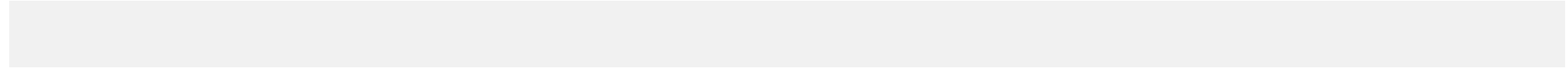
0 Comments Show recent to old
Post a comment

 RSS of this page

Author: [aglone](#) Version: [1.1](#) Last Edited By: [aglone3](#) Modified: 27 - days ago

Información de contacto

servicios@iso27002.es



Quick Search

- Navigate pages | Site Map
- 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 los usuarios

 [Site Home](#) » [11. Control de Accesos](#) » [11 2 Gestión de acceso de usuario](#) » 11.2.3. Gestión de contraseñas de usuario

11.2.3. Gestión de contraseñas de usuario



Control:

Se debería controlar la asignación de contraseñas mediante un proceso de gestión formal.

([consultar 8.1.3](#))

([consultar 11.3.1](#))

Posibles Soluciones a este control:

Espacio pendiente de posibles aportaciones.

0 Comments [Show recent to old](#)
[Post a comment](#)

 [RSS of this page](#)

Author: [aglone](#) Version: [1.1](#) Last Edited By: [aglone3](#) Modified: 27 - days ago

Información de contacto

servicios@iso27002.es

Quick Search

- Navigate pages | Site Map
- 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 los usuarios

Site Home » 11. Control de Accesos » 11 2 Gestión de acceso de usuario » 11.2.4. Revisión de los derechos de acceso de los usuarios

11.2.4. Revisión de los derechos de acceso de los usuarios



Control:

El órgano de Dirección debería revisar con regularidad los derechos de acceso de los usuarios, siguiendo un procedimiento formal.

(consultar 11.2.1)

(consultar 11.2.2)

Posibles Soluciones a este control:

Espacio pendiente de posibles aportaciones.

0 Comments Show recent to old
Post a comment

RSS of this page

Author: aglone Version: 1.1 Last Edited By: aglone3 Modified: 27 - days ago

Información de contacto

servicios@iso27002.es

Quick Search

- Navigate pages | Site Map
- ISO 27002

05. Política de Seguridad

06. Organización de la Seguridad de Información

07. Gestión de Activos

08. Seguridad ligada a los Recursos Humanos

09. Seguridad Física y del Entorno

10. Gestión de Comunicaciones y Operaciones

11. Control de Accesos

11 1 Requerimientos de negocio para el control de accesos

11 2 Gestión de acceso de usuario

11 3 Responsabilidades del usuario

11.3.1. Uso de contraseña

11.3.2. Equipo informático de usuario desatendido

11.3.3. Políticas para escritorios y monitores sin información

11 4 Control de acceso en red

11 5 Control de acceso al sistema operativo

11 6 Control de acceso a las aplicaciones

11 7 Informática móvil y tele trabajo

12. Adquisición, Desarrollo y Mantenimiento de Sistemas de Información

13. Gestión de Incidentes de Seguridad de la Información

14. Gestión de Continuidad del Negocio



15. Conformidad

Objetivos

Contacto

Aviso Legal
- Site Home » 11. Control de Accesos » 11 3 Responsabilidades del usuario
- 11 3 Responsabilidades del usuario
- 

Espacio de Patrocinio disponible

 <div>Objetivo</div>	Impedir el acceso de usuarios no autorizados y el compromiso o robo de información y recursos para el tratamiento de la información.
 <div>Principios</div>	<p>La cooperación de los usuarios autorizados es esencial para una seguridad efectiva.</p> <p>Los usuarios deberían ser conscientes de sus responsabilidades en el mantenimiento de controles de acceso eficaces, en particular respecto al uso de contraseñas y seguridad en los equipos puestos a su disposición.</p> <p>Se debería implantar una política para mantener mesas de escritorio y monitores libres de cualquier información con objeto de reducir el riesgo de accesos no autorizados o el deterioro de documentos, medios y recursos para el tratamiento de la información.</p>
 <div></div>	<p>Asegúrese de que se establecen las responsabilidades de seguridad y que son entendidas por el personal afectado.</p> <p>Una buena estrategia es definir y documentar claramente las responsabilidades relativas a seguridad de la información en las descripciones o perfiles de los puestos de trabajo.</p> <p>Son imprescindibles las revisiones periódicas para incluir cualquier cambio.</p> <p>Comunique regularmente a los empleados los perfiles de sus puestos (p. ej., en la revisión anual de objetivos), para recordarles sus responsabilidades y recoger cualquier cambio.</p>
 <div></div>	Porcentaje de descripciones de puesto de trabajo que incluyen responsabilidades en seguridad de la información (a) totalmente documentadas y (b) formalmente aceptadas.
- 0 Comments [Show recent to old](#)
[Post a comment](#)
- [Attachments](#) (2)
-  [RSS of this page](#)
- Author: [aglone](#) Version: [1.4](#) Last Edited By: [aglone3](#) Modified: 26 - days ago
- Información de contacto
- servicios@iso27002.es
- Powered by [Zoho Wiki](#) | [Zoho](#) | [Report Abuse](#) | [Wiki Index](#) | [Site Map](#) | [Help](#) | [Feedback](#) | [Jump Start with 2 Free Wikis](#) | [Sign in](#)
- http://iso27002.wiki.zoho.com/11-3-Responsabilidades-del-usuario.html[28/01/2011 08:31:21 p.m.]

Quick Search

Navigate pages | Site Map

11 3 Responsabilidades del usuario

- 11.3.1. Uso de contraseña
- 11.3.2. Equipo informático de usuario desatendido
- 11.3.3. Políticas para escritorios y monitores sin información

11.3.1. Uso de contraseña



Control:

Se debería exigir a los usuarios el uso de las buenas prácticas de seguridad en la selección y uso de las contraseñas.

Posibles Soluciones a este control:

	Random Password Generator (freeware) is designed to help you create secure Random passwords that are extremely difficult to crack or guess, with a combination of random lower and upper case letters, numbers and punctuation symbols. And these random generated passwords will be saved for memo. You can give a mark to the generated random password for later check.	Password generator
	Generador on-line de contraseñas.	Password.es
	Ophcrack is a free Windows password cracker based on rainbow tables. It is a very efficient implementation of rainbow tables done by the inventors of the method. It comes with a Graphical User Interface and runs on multiple platforms.	ophcrack
	Cain & Abel is a password recovery tool for Microsoft Operating Systems. It allows easy recovery of various kind of passwords by sniffing the network, cracking encrypted passwords using Dictionary, Brute-Force and Cryptanalysis attacks, recording VoIP conversations, decoding scrambled passwords, recovering wireless network keys, revealing password boxes, uncovering cached passwords and analyzing routing protocols.	Cain & Abel
	John the Ripper is free and Open Source software, distributed primarily in source code form. If you would rather use a commercial product tailored for your specific operating system, please consider John the Ripper Pro, which is distributed primarily in the form of "native" packages for the target operating systems and in general is meant to be easier to install and use while delivering optimal performance. td>	John the Ripper

0 Comments [Show recent to old](#)
[Post a comment](#)

RSS of this page

Author: [aglone](#) Version: [1.1](#) Last Edited By: [aglone3](#) Modified: 27 - days ago

Información de contacto

servicios@iso27002.es

Quick Search

Navigate pages | Site Map

11 3 Responsabilidades del usuario

11.3.1. Uso de contraseña

11.3.2. Equipo informático de usuario desatendido

11.3.3. Políticas para escritorios y monitores sin información

Site Home » 11. Control de Accesos » 11 3 Responsabilidades del usuario » 11.3.2. Equipo informático de usuario desatendido

11.3.2. Equipo informático de usuario desatendido



Espacio de Patrocinio disponible

Control:

Los usuarios deberían garantizar que los equipos desatendidos disponen de la protección apropiada.

(consultar también 11.3.3)

Posibles Soluciones a este control:

Espacio pendiente de posibles aportaciones.

0 Comments Show recent to old Post a comment

 RSS of this page

Author: [aglone](#) Version: [1.1](#) Last Edited By: [aglone3](#) Modified: 27 - days ago

Información de contacto

servicios@iso27002.es

Powered by [Zoho Wiki](#) | [Zoho](#) | [Report Abuse](#) | [Wiki Index](#) | [Site Map](#) | [Help](#) | [Feedback](#) | [Jump Start with 2 Free Wikis](#) | [Sign in](#)

http://iso27002.wiki.zoho.com/11-3-2-Equipo-informático-de-usuario-desatendido.html[28/01/2011 08:31:47 p.m.]

Quick Search

- Navigate pages | Site Map
- 11 3 Responsabilidades del usuario
 - 11.3.1. Uso de contraseña
 - 11.3.2. Equipo informático de usuario desatendido
 - 11.3.3. Políticas para escritorios y monitores sin información**

Site Home » 11. Control de Accesos » 11 3 Responsabilidades del usuario » 11.3.3. Políticas para escritorios y monitores sin información

11.3.3. Políticas para escritorios y monitores sin información



Control:

Políticas para escritorios y monitores limpios de información

(consultar 7.2)

(consultar 15.1)

Posibles Soluciones a este control:

	Posters are utilized to efficiently and effectively educate numerous staff on new security topics each and every month. Our eye-catching, entertaining, posters will help increase the security awareness level in your workplace.	OISSG
--	--	-----------------------

0 Comments [Show recent to old](#)
[Post a comment](#)

RSS of this page

Author: [aglone](#) Version: [1.1](#) Last Edited By: [aglone3](#) Modified: 27 - days ago

Información de contacto

servicios@iso27002.es

Quick Search

- Navigate pages | Site Map
- ISO 27002

⊞ 05. Política de Seguridad

⊞ 06. Organización de la Seguridad de Información

⊞ 07. Gestión de Activos

⊞ 08. Seguridad ligada a los Recursos Humanos

⊞ 09. Seguridad Física y del Entorno

⊞ 10. Gestión de Comunicaciones y Operaciones

⊞ 11. Control de Accesos

⊞ 11 1 Requerimientos de negocio para el control de accesos

⊞ 11 2 Gestión de acceso de usuario

⊞ 11 3 Responsabilidades del usuario

⊞ 11 4 Control de acceso en red

● 11.4.1. Política de uso de los servicios de red

● 11.4.2. Autenticación de usuario para conexiones externas

● 11.4.3. Autenticación de nodos de la red

● 11.4.4. Protección a puertos de diagnóstico remoto

● 11.4.5. Segregación en las redes

● 11.4.6. Control de conexión a las redes

● 11.4.7. Control de encaminamiento en la red

⊞ 11 5 Control de acceso al sistema operativo

⊞ 11 6 Control de acceso a las aplicaciones

⊞ 11 7 Informática móvil y tele trabajo

⊞ 12. Adquisición, Desarrollo y Mantenimiento de Sistemas de Información

⊞ 13. Gestión de Incidentes de Seguridad de la Información

⊞ 14. Gestión de Continuidad del Negocio

⊞ 15. Conformidad

● Objetivos





● Contacto

● Aviso Legal

 [Site Home](#) >> [11. Control de Accesos](#) >> 11 4 Control de acceso en red

11 4 Control de acceso en red



 Objetivo	Impedir el acceso no autorizado a los servicios en red.
 Principios	<p>Se deberían controlar los accesos a servicios internos y externos conectados en red.</p> <p>El acceso de los usuarios a redes y servicios en red no debería comprometer la seguridad de los servicios en red si se garantizan:</p> <p>a) que existen interfaces adecuadas entre la red de la Organización y las redes públicas o privadas de otras organizaciones;</p> <p>b) que los mecanismos de autenticación adecuados se aplican a los usuarios y equipos;</p> <p>c) el cumplimiento del control de los accesos de los usuarios a los servicios de información.</p>
	Mantenga el equilibrio entre controles de seguridad perimetrales (LAN/WAN) e internos (LAN/LAN), frente a controles de seguridad en aplicaciones (defensa en profundidad).
	Estadísticas de cortafuegos, tales como porcentaje de paquetes o sesiones salientes que han sido bloqueadas (p. ej., intentos de acceso a páginas web prohibidas; número de ataques potenciales de hacking repelidos, clasificados en insignificantes/preocupantes/críticos).

0 Comments [Show recent to old](#)
Post a comment

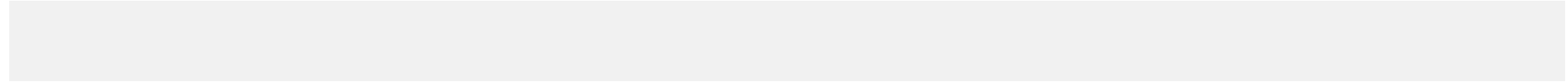
Attachments (2)

 [RSS of this page](#)

Author: [aglone](#) **Version:** [1.3](#) **Last Edited By:** [aglone3](#) **Modified:** 26 - days ago

Información de contacto

servicios@iso27002.es



Quick Search

- Navigate pages | Site Map
- 11 4 Control de acceso en red

 - 11.4.1. Política de uso de los servicios de red
 - 11.4.2. Autenticación de usuario para conexiones externas
 - 11.4.3. Autenticación de nodos de la red
 - 11.4.4. Protección a puertos de diagnóstico remoto
 - 11.4.5. Segregación en las redes
 - 11.4.6. Control de conexión a las redes
 - 11.4.7. Control de encaminamiento en la red

Site Home » 11. Control de Accesos » 11 4 Control de acceso en red » 11.4.1. Política de uso de los servicios de red

11.4.1. Política de uso de los servicios de red



Control:

Se debería proveer a los usuarios de los accesos a los servicios para los que han sido expresamente autorizados a utilizar.

(consultar 11.1)

Posibles Soluciones a este control:

Espacio pendiente de posibles aportaciones.

0 Comments [Show recent to old](#)
[Post a comment](#)

RSS of this page

Author: [aglone](#) Version: [1.1](#) Last Edited By: [aglone3](#) Modified: 27 - days ago

Información de contacto

servicios@iso27002.es

Quick Search

- Navigate pages | Site Map
- 11 4 Control de acceso en red

 - 11.4.1. Política de uso de los servicios de red
 - 11.4.2. Autenticación de usuario para conexiones externas**
 - 11.4.3. Autenticación de nodos de la red
 - 11.4.4. Protección a puertos de diagnóstico remoto
 - 11.4.5. Segregación en las redes
 - 11.4.6. Control de conexión a las redes
 - 11.4.7. Control de encaminamiento en la red

 [Site Home](#) » [11. Control de Accesos](#) » [11 4 Control de acceso en red](#) » 11.4.2. Autenticación de usuario para conexiones externas

11.4.2. Autenticación de usuario para conexiones externas



Control:

Se deberían utilizar métodos de autenticación adecuados para el control del acceso remoto de los usuarios.

Posibles Soluciones a este control:

Espacio pendiente de posibles aportaciones.

0 Comments [Show recent to old](#)
[Post a comment](#)



RSS of this page

Author: [aglone](#) **Version:** [1.1](#) **Last Edited By:** [aglone3](#) **Modified:** 27 - days ago

Información de contacto

servicios@iso27002.es

Quick Search

- Navigate pages | Site Map
- 11 4 Control de acceso en red

11.4.1. Política de uso de los servicios de red

11.4.2. Autenticación de usuario para conexiones externas

11.4.3. Autenticación de nodos de la red

11.4.4. Protección a puertos de diagnóstico remoto

11.4.5. Segregación en las redes

11.4.6. Control de conexión a las redes

11.4.7. Control de encaminamiento en la red



11.4.3. Autenticación de nodos de la red



Control:

Se debería considerar la identificación automática de los equipos como un medio de autenticación de conexiones procedentes de lugares y equipos específicos.

Posibles Soluciones a este control:

	Spiceworks is the complete network management & monitoring, helpdesk, PC inventory & software reporting solution to manage Everything IT in small and medium businesses.	Spiceworks
logo.png 	Paglo is on-demand tool. Businesses can discover all their IT information and get instant answers to their computer, network, and security questions.	Paglo

0 Comments [Show recent to old](#)
[Post a comment](#)

 RSS of this page

Author: [aglone](#) Version: [1.1](#) Last Edited By: [aglone3](#) Modified: 27 - days ago

Información de contacto

servicios@iso27002.es

Quick Search

- Navigate pages | Site Map
- 11 4 Control de acceso en red

 - 11.4.1. Política de uso de los servicios de red
 - 11.4.2. Autenticación de usuario para conexiones externas
 - 11.4.3. Autenticación de nodos de la red
 - 11.4.4. Protección a puertos de diagnóstico remoto**
 - 11.4.5. Segregación en las redes
 - 11.4.6. Control de conexión a las redes
 - 11.4.7. Control de encaminamiento en la red

11.4.4. Protección a puertos de diagnóstico remoto



Control:

Se debería controlar la configuración y el acceso físico y lógico a los puertos de diagnóstico.

Posibles Soluciones a este control:

Espacio pendiente de posibles aportaciones.

0 Comments [Show recent to old](#)
[Post a comment](#)

RSS of this page

Author: [aglone](#) Version: [1.1](#) Last Edited By: [aglone3](#) Modified: 27 - days ago

Información de contacto

servicios@iso27002.es

Quick Search

- Navigate pages | Site Map
- 11 4 Control de acceso en red

 - 11.4.1. Política de uso de los servicios de red
 - 11.4.2. Autenticación de usuario para conexiones externas
 - 11.4.3. Autenticación de nodos de la red
 - 11.4.4. Protección a puertos de diagnóstico remoto
 - 11.4.5. Segregación en las redes**
 - 11.4.6. Control de conexión a las redes
 - 11.4.7. Control de encaminamiento en la red

Site Home » 11. Control de Accesos » 11 4 Control de acceso en red » 11.4.5. Segregación en las redes

11.4.5. Segregación en las redes



Control:

Se deberían segregar los grupos de usuarios, servicios y sistemas de información en las redes.

(consultar 11.4.6 y 11.4.7)

(consultar 11.1)

(consultar 10.1)

Posibles Soluciones a este control:

Espacio pendiente de posibles aportaciones.

0 Comments Show recent to old
Post a comment

RSS of this page

Author: [aglone](#) Version: [1.1](#) Last Edited By: [aglone3](#) Modified: 27 - days ago

Información de contacto

servicios@iso27002.es

Quick Search

- Navigate pages | Site Map
- 11 4 Control de acceso en red

 - 11.4.1. Política de uso de los servicios de red
 - 11.4.2. Autenticación de usuario para conexiones externas
 - 11.4.3. Autenticación de nodos de la red
 - 11.4.4. Protección a puertos de diagnóstico remoto
 - 11.4.5. Segregación en las redes
 - 11.4.6. Control de conexión a las redes**
 - 11.4.7. Control de encaminamiento en la red

11.4.6. Control de conexión a las redes



Control:

En el caso de las redes compartidas, especialmente aquellas que se extienden más allá de los límites de la propia Organización, se deberían restringir las competencias de los usuarios para conectarse en red según la política de control de accesos y necesidad de uso de las aplicaciones de negocio.

(consultar 11.1)

(consultar 11.1.1)

Posibles Soluciones a este control:

Espacio pendiente de posibles aportaciones.

0 Comments [Show recent to old](#)
[Post a comment](#)

RSS of this page

Author: [aglone](#) Version: [1.1](#) Last Edited By: [aglone3](#) Modified: 27 - days ago

Información de contacto

servicios@iso27002.es

Quick Search

- Navigate pages | Site Map
- 11 4 Control de acceso en red

11.4.1. Política de uso de los servicios de red

11.4.2. Autenticación de usuario para conexiones externas

11.4.3. Autenticación de nodos de la red

11.4.4. Protección a puertos de diagnóstico remoto

11.4.5. Segregación en las redes

11.4.6. Control de conexión a las redes

11.4.7. Control de encaminamiento en la red

Site Home » 11. Control de Accesos » 11 4 Control de acceso en red » 11.4.7. Control de encaminamiento en la red

11.4.7. Control de encaminamiento en la red





Control:

Se deberían establecer controles de enrutamiento en las redes para asegurar que las conexiones de los ordenadores y flujos de información no incumplen la política de control de accesos a las aplicaciones de negocio.

(consultar 11.1)

Posibles Soluciones a este control:

 Network-Tools.com	Freeware employee monitoring. Network-Tools owner sues Microsoft, Cisco, Comcast and TRUSTe over IP Address Blacklisting. Suit alleges eavdropping, privacy policy fraud, breach of contract and defamation.	NetworkTools
 Backscatterer.org <small>powered by UCEPROTECT</small>	Simply use this list via DNS at ips.backscatterer.org for scoring or rejecting bounces and sender callouts from abusive systems.	Backscatterer

0 Comments [Show recent to old](#)
[Post a comment](#)

 RSS of this page

Author: [aglone](#) Version: [1.1](#) Last Edited By: [aglone3](#) Modified: 27 - days ago

Información de contacto

servicios@iso27002.es

Quick Search

- Navigate pages | Site Map
- ISO 27002

05. Política de Seguridad

06. Organización de la Seguridad de Información

07. Gestión de Activos

08. Seguridad ligada a los Recursos Humanos

09. Seguridad Física y del Entorno

10. Gestión de Comunicaciones y Operaciones

11. Control de Accesos

11 1 Requerimientos de negocio para el control de accesos

11 2 Gestión de acceso de usuario

11 3 Responsabilidades del usuario

11 4 Control de acceso en red

11 5 Control de acceso al sistema operativo

11.5.1. Procedimientos de conexión de terminales

11.5.2. Identificación y autenticación de usuario

11.5.3. Sistema de gestión de contraseñas

11.5.4. Uso de los servicios del sistema

11.5.5. Desconexión automática de terminales

11.5.6. Limitación del tiempo de conexión

11 6 Control de acceso a las aplicaciones

11 7 Informática móvil y tele trabajo

12. Adquisición, Desarrollo y Mantenimiento de Sistemas de Información

13. Gestión de Incidentes de Seguridad de la Información

14. Gestión de Continuidad del Negocio






15. Conformidad

Objetivos

Contacto

Aviso Legal

11 5 Control de acceso al sistema operativo

	Espacio de Patrocinio disponible
	Impedir el acceso no autorizado al sistema operativo de los sistemas.
	<p>Se deberían utilizar las prestaciones de seguridad del sistema operativo para permitir el acceso exclusivo a los usuarios autorizados.</p> <p>Las prestaciones deberían ser capaces de:</p> <div>a) la autenticación de los usuarios autorizados, de acuerdo a la política de control de accesos definida;</div> <div>b) registrar los intentos de autenticación correctos y fallidos del sistema;</div> <div>c) registrar el uso de privilegios especiales del sistema;</div> <div>d) emitir señales de alarma cuando se violan las políticas de seguridad del sistema;</div> <div>e) disponer los recursos adecuados para la autenticación;</div> <div>f) restringir los horarios de conexión de los usuarios cuando sea necesario.</div>
	Implante estándares de seguridad básica para todas las plataformas informáticas y de comunicaciones, recogiendo las mejores prácticas de CIS , NIST , fabricantes de sistemas, etc.
	Estadísticas de vulnerabilidad de sistemas y redes, como nº de vulnerabilidades conocidas cerradas, abiertas y nuevas; velocidad media de parcheo de vulnerabilidades (analizadas por prioridades/categorías del fabricante o propias).

0 Comments

Show recent to old

Post a comment

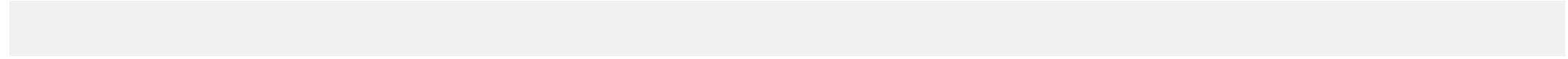
Attachments (2)

 RSS of this page

Author: [aglone](#) Version: [1.3](#) Last Edited By: [aglone3](#) Modified: 26 - days ago

Información de contacto

servicios@iso27002.es



Quick Search

- Navigate pages | Site Map
- 11 5 Control de acceso al sistema operativo

 - 11.5.1. Procedimientos de conexión de terminales
 - 11.5.2. Identificación y autenticación de usuario
 - 11.5.3. Sistema de gestión de contraseñas
 - 11.5.4. Uso de los servicios del sistema
 - 11.5.5. Desconexión automática de terminales
 - 11.5.6. Limitación del tiempo de conexión

Site Home » 11. Control de Accesos » 11 5 Control de acceso al sistema operativo » 11.5.1. Procedimientos de conexión de terminales

11.5.1. Procedimientos de conexión de terminales



Control:

Debería controlarse el acceso al sistema operativo mediante procedimientos seguros de conexión.

Posibles Soluciones a este control:

Espacio pendiente de posibles aportaciones.

0 Comments Show recent to old
Post a comment

RSS of this page

Author: aglone Version: 1.1 Last Edited By: aglone3 Modified: 27 - days ago

Información de contacto

servicios@iso27002.es

Quick Search

- Navigate pages | Site Map
- 11 5 Control de acceso al sistema operativo
 - 11.5.1. Procedimientos de conexión de terminales
 - 11.5.2. Identificación y autenticación de usuario**
 - 11.5.3. Sistema de gestión de contraseñas
 - 11.5.4. Uso de los servicios del sistema
 - 11.5.5. Desconexión automática de terminales
 - 11.5.6. Limitación del tiempo de conexión

 [Site Home](#) » [11. Control de Accesos](#) » [11 5 Control de acceso al sistema operativo](#) » 11.5.2. Identificación y autenticación de usuario

11.5.2. Identificación y autenticación de usuario



Control:

Todos los usuarios deberían disponer de un único identificador propio para su uso personal y exclusivo. Se debería elegir una técnica de autenticación adecuada que verifique la identidad reclamada por un usuario.

Posibles Soluciones a este control:

Espacio pendiente de posibles aportaciones.

0 Comments [Show recent to old](#)
[Post a comment](#)

 [RSS of this page](#)

Author: [aglone](#) Version: [1.1](#) Last Edited By: [aglone3](#) Modified: 27 - days ago

Información de contacto

servicios@iso27002.es

Quick Search

- Navigate pages | Site Map
- 11 5 Control de acceso al sistema operativo

11.5.1. Procedimientos de conexión de terminales

11.5.2. Identificación y autenticación de usuario

11.5.3. Sistema de gestión de contraseñas

11.5.4. Uso de los servicios del sistema

11.5.5. Desconexión automática de terminales

11.5.6. Limitación del tiempo de conexión

11.5.3. Sistema de gestión de contraseñas



Control:

Los sistemas de gestión de contraseñas deberían ser interactivos y garantizar la calidad de las contraseñas.

(consultar 11.3.1)

(consultar 11.2.3)

Posibles Soluciones a este control:

Espacio pendiente de posibles aportaciones.

0 Comments Show recent to old
Post a comment

RSS of this page

Author: aglone Version: 1.1 Last Edited By: aglone3 Modified: 27 - days ago

Información de contacto

servicios@iso27002.es

Quick Search

- Navigate pages | Site Map
- 11 5 Control de acceso al sistema operativo

11.5.1. Procedimientos de conexión de terminales

11.5.2. Identificación y autenticación de usuario

11.5.3. Sistema de gestión de contraseñas

11.5.4. Uso de los servicios del sistema

11.5.5. Desconexión automática de terminales

11.5.6. Limitación del tiempo de conexión

11.5.4. Uso de los servicios del sistema



Control:

Se debería restringir y controlar muy de cerca el uso de programas de utilidad del sistema que pudieran ser capaces de eludir los controles del propio sistema y de las aplicaciones.

(consultar también 11.2.2)

Posibles Soluciones a este control:

Espacio pendiente de posibles aportaciones.

0 Comments [Show recent to old](#)
[Post a comment](#)

RSS of this page


Author: [aglone](#) Version: [1.1](#) Last Edited By: [aglone3](#) Modified: 27 - days ago

Información de contacto

servicios@iso27002.es

Quick Search

- Navigate pages | Site Map
- 11 5 Control de acceso al sistema operativo
 - 11.5.1. Procedimientos de conexión de terminales
 - 11.5.2. Identificación y autenticación de usuario
 - 11.5.3. Sistema de gestión de contraseñas
 - 11.5.4. Uso de los servicios del sistema
 - 11.5.5. Desconexión automática de terminales**
 - 11.5.6. Limitación del tiempo de conexión

 [Site Home](#) » [11. Control de Accesos](#) » [11 5 Control de acceso al sistema operativo](#) » 11.5.5. Desconexión automática de terminales

11.5.5. Desconexión automática de terminales



Control:

Se deberían desconectar las sesiones tras un determinado periodo de inactividad.

Posibles Soluciones a este control:

Espacio pendiente de posibles aportaciones.

0 Comments [Show recent to old](#)
[Post a comment](#)

 [RSS of this page](#)

Author: [aglone](#) Version: [1.1](#) Last Edited By: [aglone3](#) Modified: 27 - days ago

Información de contacto

servicios@iso27002.es

Quick Search

- Navigate pages | Site Map
- 11 5 Control de acceso al sistema operativo

11.5.1. Procedimientos de conexión de terminales

11.5.2. Identificación y autenticación de usuario

11.5.3. Sistema de gestión de contraseñas

11.5.4. Uso de los servicios del sistema

11.5.5. Desconexión automática de terminales

11.5.6. Limitación del tiempo de conexión

11.5.6. Limitación del tiempo de conexión



Control:

Se deberían utilizar limitaciones en el tiempo de conexión que proporcionen un nivel de seguridad adicional a las aplicaciones de alto riesgo.

Posibles Soluciones a este control:

Espacio pendiente de posibles aportaciones.

0 Comments Show recent to old
Post a comment

RSS of this page

Author: aglone Version: 1.1 Last Edited By: aglone3 Modified: 27 - days ago

Información de contacto

servicios@iso27002.es

Quick Search

- Navigate pages | Site Map
- ISO 27002

05. Política de Seguridad

06. Organización de la Seguridad de Información

07. Gestión de Activos

08. Seguridad ligada a los Recursos Humanos

09. Seguridad Física y del Entorno

10. Gestión de Comunicaciones y Operaciones

11. Control de Accesos

11 1 Requerimientos de negocio para el control de accesos

11 2 Gestión de acceso de usuario

11 3 Responsabilidades del usuario

11 4 Control de acceso en red

11 5 Control de acceso al sistema operativo

11 6 Control de acceso a las aplicaciones

11.6.1. Restricción de acceso a la información

11 6 2 Aislamiento de sistemas sensibles

11 7 Informática móvil y tele trabajo

12. Adquisición, Desarrollo y Mantenimiento de Sistemas de Información

13. Gestión de Incidentes de Seguridad de la Información

14. Gestión de Continuidad del Negocio

15. Conformidad

Objetivos

Contacto

Aviso Legal
- Site Home


>>

11. Control de Accesos

>>

11 6 Control de acceso a las aplicaciones
- ## 11 6 Control de acceso a las aplicaciones
-
- | | |
|---|---|
|  <div>Objetivo</div> | <p>Impedir el acceso no autorizado a la información mantenida por los sistemas de las aplicaciones.</p> |
|  <div>Principios</div> | <p>Se deberían utilizar dispositivos de seguridad con objeto de restringir el acceso a las aplicaciones y sus contenidos.</p> <p>Se debería restringir el acceso lógico a las aplicaciones software y su información únicamente a usuarios autorizados.</p> <p>Los sistemas de aplicación deberían:</p> <p>a) controlar el acceso de los usuarios a la información y funciones de los sistemas de aplicaciones, en relación a la política de control de accesos definida;</p> <p>b) proporcionar protección contra accesos no autorizados derivados del uso de cualquier utilidad, software del sistema operativo y software malicioso que puedan traspasar o eludir los controles del sistema o de las aplicaciones;</p> <p>c) no comprometer otros sistemas con los que se compartan recursos de información.</p> |
|  | <p>Implante estándares de seguridad básica para todas las aplicaciones y middleware, recogiendo las mejores prácticas y checklists de CIS, NIST, fabricantes de software, etc.</p> |
|  | <p>Porcentaje de plataformas totalmente conformes con los estándares de seguridad básica (comprobado mediante pruebas independientes), con anotaciones sobre los sistemas no conformes (p. ej., "Sistema de finanzas será actualizado para ser conforme en cuarto trimestre)".</p> |
- 0 Comments

Show recent to old

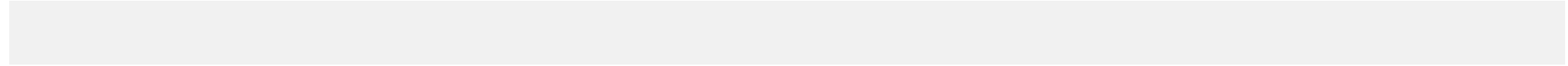
Post a comment
- Attachments (2)
- 

RSS of this page
- Author: [aglone](#)

Version: [1.3](#)

Last Edited By: [aglone3](#)

Modified: 26 - days ago
- ### Información de contacto
- servicios@iso27002.es
- Powered by [Zoho Wiki](#) | [Zoho](#) | [Report Abuse](#) | [Wiki Index](#) | [Site Map](#) | [Help](#) | [Feedback](#) | [Jump Start with 2 Free Wikis](#) | [Sign in](#)
- http://iso27002.wiki.zoho.com/11-6-Control-de-acceso-a-las-aplicaciones.html[28/01/2011 08:34:39 p.m.]



Quick Search

Navigate pages | Site Map

11 6 Control de acceso a las aplicaciones

- 11.6.1. Restricción de acceso a la información
- 11 6 2 Aislamiento de sistemas sensibles

11.6.1. Restricción de acceso a la información



Control:

Se debería restringir el acceso de los usuarios y el personal de mantenimiento a la información y funciones de los sistemas de aplicaciones, en relación a la política de control de accesos definida.

(consultar 11.1)

Posibles Soluciones a este control:

Espacio pendiente de posibles aportaciones.

0 Comments [Show recent to old](#)
[Post a comment](#)

RSS of this page

Author: [aglone](#) Version: [1.1](#) Last Edited By: [aglone3](#) Modified: 27 - days ago

Información de contacto

servicios@iso27002.es

Quick Search

- Navigate pages | Site Map
- 11 6 Control de acceso a las aplicaciones

11.6.1. Restricción de acceso a la información

11 6 2 Aislamiento de sistemas sensibles

Site Home » 11. Control de Accesos » 11 6 Control de acceso a las aplicaciones » 11 6 2 Aislamiento de sistemas sensibles

11 6 2 Aislamiento de sistemas sensibles



Control:

Los sistemas sensibles deberían disponer de un entorno informático dedicado (propio).

(consultar 7.1.2)

Posibles Soluciones a este control:

	La biblioteca TechNet Library es un recurso esencial para los profesionales de TI que usan los productos, herramientas y tecnología de Microsoft.	technet library
--	---	---------------------------------

0 Comments [Show recent to old](#)
[Post a comment](#)

[Attachments](#) (1)

[RSS of this page](#)

Author: [aglone](#) Version: [1.2](#) Last Edited By: [aglone3](#) Modified: 27 - days ago

Información de contacto

servicios@iso27002.es

Quick Search

- Navigate pages | Site Map
- ISO 27002

05. Política de Seguridad

06. Organización de la Seguridad de Información

07. Gestión de Activos

08. Seguridad ligada a los Recursos Humanos

09. Seguridad Física y del Entorno

10. Gestión de Comunicaciones y Operaciones

11. Control de Accesos

11 1 Requerimientos de negocio para el control de accesos

11 2 Gestión de acceso de usuario

11 3 Responsabilidades del usuario

11 4 Control de acceso en red

11 5 Control de acceso al sistema operativo

11 6 Control de acceso a las aplicaciones

11 7 Informática móvil y tele trabajo

11 7 1 Informática móvil

11.7.2. Tele trabajo

12. Adquisición, Desarrollo y Mantenimiento de Sistemas de Información

13. Gestión de Incidentes de Seguridad de la Información

14. Gestión de Continuidad del Negocio

15. Conformidad

Objetivos


Contacto

Aviso Legal
- Site Home





>>

11. Control de Accesos

>>

11 7 Informática móvil y tele trabajo
- 11 7 Informática móvil y tele trabajo
- 

Espacio de Patrocinio disponible

 <div>Objetivo</div>	Garantizar la seguridad de la información en el uso de recursos de informática móvil y teletrabajo.
 <div>Principios</div>	<p>La protección exigible debería estar en relación a los riesgos específicos que ocasionan estas formas específicas de trabajo. En el uso de la informática móvil deberían considerarse los riesgos de trabajar en entornos desprotegidos y aplicar la protección conveniente.</p> <p>En el caso del teletrabajo, la Organización debería aplicar las medidas de protección al lugar remoto y garantizar que las disposiciones adecuadas estén disponibles para esta modalidad de trabajo.</p>
	<p>Tenga políticas claramente definidas para la protección, no sólo de los propios equipos informáticos portátiles (es decir, laptops, PDAs, etc.), sino, en mayor medida, de la información almacenada en ellos.</p> <p>Por lo general, el valor de la información supera con mucho el del hardware.</p> <p>Asegúrese de que el nivel de protección de los equipos informáticos utilizados dentro de las instalaciones de la organización tiene su correspondencia en el nivel de protección de los equipos portátiles, en aspectos tales como antivirus, parches, actualizaciones, software cortafuegos, etc.</p>
	"Estado de la seguridad en entorno portátil / teletrabajo", es decir, un informe sobre el estado actual de la seguridad de equipos informáticos portátiles (laptops, PDAs, teléfonos móviles, etc.), y de teletrabajo (en casa de los empleados, fuerza de trabajo móvil), con comentarios sobre incidentes recientes/actuales, vulnerabilidades actuales de seguridad conocidas y pronósticos sobre cualquier riesgo creciente, despliegue de configuraciones seguras, antivirus, firewalls personales, etc.
- 0 Comments [Show recent to old](#)
[Post a comment](#)
- [Attachments](#) (2)
-  [RSS of this page](#)
- Author: [aglone](#) Version: [1.5](#) Last Edited By: [aglone3](#) Modified: 26 - days ago
- Información de contacto
- servicios@iso27002.es
- Powered by [Zoho Wiki](#) | [Zoho](#) | [Report Abuse](#) | [Wiki Index](#) | [Site Map](#) | [Help](#) | [Feedback](#) | [Jump Start with 2 Free Wikis](#) | [Sign in](#)
- http://iso27002.wiki.zoho.com/11-7-Informática-móvil-y-tele-trabajo.html[28/01/2011 08:35:08 p.m.]

Quick Search

- Navigate pages | Site Map
- 11 7 Informática móvil y tele trabajo

11 7 1 Informática móvil

11.7.2. Tele trabajo

Site Home » 11. Control de Accesos » 11 7 Informática móvil y tele trabajo » 11 7 1 Informática móvil

11 7 1 Informática móvil



Control:

Se debería establecer una política formal y se deberían adoptar las medidas de seguridad adecuadas para la protección contra los riesgos derivados del uso de los recursos de informática móvil y las telecomunicaciones.

(consultar 12.3)

(consultar 10.4)

(consultar 11.4)

(consultar 9.2.5)

Posibles Soluciones a este control:

	Checklist de revisión de controles para equipos portátiles, trabajo en movilidad, teletrabajo y redes inalámbricas (inglés)	http://tinyurl.com/PortableITchecklist
	Guía para proteger y usar de forma segura su móvil	Guía INTECO

0 Comments Show recent to old
Post a comment

Attachments (1)

RSS of this page

Author: [aglone](#) Version: [1.2](#) Last Edited By: [aglone3](#) Modified: 27 - days ago

Información de contacto

servicios@iso27002.es

Quick Search

Navigate pages | Site Map

11 7 Informática móvil y tele trabajo

11 7 1 Informática móvil

11.7.2. Tele trabajo

Site Home » 11. Control de Accesos » 11 7 Informática móvil y tele trabajo » 11.7.2. Tele trabajo


11.7.2. Tele trabajo



Control:

Se debería desarrollar e implantar una política, planes operacionales y procedimientos para las actividades de teletrabajo.

Posibles Soluciones a este control:

menu-oswa.gif 	The OSWA-Assistant™ is a freely-downloadable, self-contained, wireless-auditing toolkit for both IT-security professionals and End-users alike.	OSWA
--	---	----------------------

0 Comments [Show recent to old](#)
[Post a comment](#)

 [RSS of this page](#)

Author: [aglone](#) Version: [1.1](#) Last Edited By: [aglone3](#) Modified: 27 - days ago

Información de contacto

servicios@iso27002.es

Quick Search

Navigate pages | Site Map

ISO 27002

05. Política de Seguridad

06. Organización de la Seguridad de Información

07. Gestión de Activos

08. Seguridad ligada a los Recursos Humanos

09. Seguridad Física y del Entorno

10. Gestión de Comunicaciones y Operaciones

11. Control de Accesos

12. Adquisición, Desarrollo y Mantenimiento de Sistemas de Información

12 1 Requisitos de seguridad de los sistemas

12.1.1. Análisis y especificación de los requisitos de seguridad

12 2 Seguridad de las aplicaciones del sistema

12 3 Controles criptográficos

12 4 Seguridad de los ficheros del sistema

12 5 Seguridad en los procesos de desarrollo y soporte

12 6 Gestión de las vulnerabilidades técnicas

13. Gestión de Incidentes de Seguridad de la Información

14. Gestión de Continuidad del Negocio

15. Conformidad





Objetivos

Contacto

Aviso Legal

12 1 Requisitos de seguridad de los sistemas



 Objetivo	Garantizar que la seguridad es parte integral de los sistemas de información.
 Principios	<p>Dentro de los sistemas de información se incluyen los sistemas operativos, infraestructuras, aplicaciones de negocio, aplicaciones estándar o de uso generalizado, servicios y aplicaciones desarrolladas por los usuarios.</p> <p>El diseño e implantación de los sistemas de información que sustentan los procesos de negocio pueden ser cruciales para la seguridad. Los requisitos de seguridad deberían ser identificados y consensuados previamente al desarrollo y/o implantación de los sistemas de información.</p> <p>Todos los requisitos de seguridad deberían identificarse en la fase de recogida de requisitos de un proyecto y ser justificados, aceptados y documentados como parte del proceso completo para un sistema de información.</p>
	<p>Involucre a los "propietarios de activos de información" en evaluaciones de riesgos a alto nivel y consiga su aprobación de los requisitos de seguridad que surjan.</p> <p>Si son realmente responsables de proteger sus activos, es en interés suyo el hacerlo bien.</p> <p>Esté al tanto de las novedades sobre vulnerabilidades comunes o actuales en aplicaciones e identifique e implemente las medidas protectoras o defensivas apropiadas. Numerosas referencias ofrecen orientación sobre la implementación, como, p. ej., OWASP.</p>
	Similar a 11.1

0 Comments [Show recent to old](#)
[Post a comment](#)

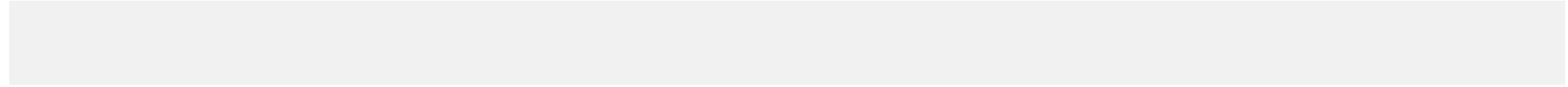
[Attachments \(2\)](#)

 [RSS of this page](#)

Author: [aglone](#) Version: [1.3](#) Last Edited By: [aglone3](#) Modified: 26 - days ago

Información de contacto

servicios@iso27002.es



Quick Search

- Navigate pages | [Site Map](#)
- 12 1 Requisitos de seguridad de los sistemas

12.1.1. Análisis y especificación de los requisitos de seguridad

[Site Home](#) » [12. Adquisición, Desarrollo y Mantenimiento de Sistemas de Información](#) » [12 1 Requisitos de seguridad de los sistemas](#) » 12.1.1. Análisis y especificación de los requisitos de seguridad

12.1.1. Análisis y especificación de los requisitos de seguridad



Control:

Las demandas de nuevos sistemas de información para el negocio o mejoras de los sistemas ya existentes deberían especificar los requisitos de los controles de seguridad.

([consultar también 7.2](#))

Posibles Soluciones a este control:

	ISO/IEC 21827 specifies the Systems Security Engineering - Capability Maturity Model, which describes the characteristics essential to the success of an organization's security engineering process, and is applicable to all security engineering organizations including government, commercial, and academic. ISO/IEC 21827 does not prescribe a particular process or sequence, but captures practices generally observed in industry	ISO/IEC 21827
--	--	-------------------------------

0 Comments [Show recent to old](#)
[Post a comment](#)

[RSS of this page](#)

Author: [aglone](#) Version: [1.1](#) Last Edited By: [aglone3](#) Modified: 27 - days ago

Información de contacto


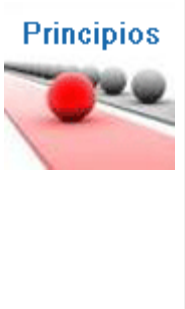


servicios@iso27002.es

Quick Search

- Navigate pages | Site Map
- ISO 27002
 - 05. Política de Seguridad
 - 06. Organización de la Seguridad de Información
 - 07. Gestión de Activos
 - 08. Seguridad ligada a los Recursos Humanos
 - 09. Seguridad Física y del Entorno
 - 10. Gestión de Comunicaciones y Operaciones
 - 11. Control de Accesos
 - 12. Adquisición, Desarrollo y Mantenimiento de Sistemas de Información
 - 12 1 Requisitos de seguridad de los sistemas
 - 12 2 Seguridad de las aplicaciones del sistema**
 - 12.2.1. Validación de los datos de entrada
 - 12.2.2. Control del proceso interno
 - 12.2.3. Autenticación de mensajes
 - 12.2.4. Validación de los datos de salida
 - 12 3 Controles criptográficos
 - 12 4 Seguridad de los ficheros del sistema
 - 12 5 Seguridad en los procesos de desarrollo y soporte
 - 12 6 Gestión de las vulnerabilidades técnicas
 - 13. Gestión de Incidentes de Seguridad de la Información
 - 14. Gestión de Continuidad del Negocio
 - 15. Conformidad
 - Objetivos
 - Contacto
 - Aviso Legal

12 2 Seguridad de las aplicaciones del sistema



 Objetivo	Evitar errores, pérdidas, modificaciones no autorizadas o mal uso de la información en las aplicaciones.
 Principios	<p>Se deberían diseñar controles apropiados en las propias aplicaciones, incluidas las desarrolladas por los propios usuarios, para asegurar el procesamiento correcto de la información. Estos controles deberían incluir la validación de los datos de entrada, el tratamiento interno y los datos de salida.</p> <p>Podrían ser requeridos controles adicionales para los sistemas que procesan o tienen algún efecto en activos de información de carácter sensible, valioso o crítico. Dichos controles deberían ser determinados en función de los requisitos de seguridad y la estimación del riesgo.</p>
	<p>Siempre que sea posible, utilice librerías y funciones estándar para necesidades corrientes como validación de datos de entrada, restricciones de rango y tipo, integridad referencial, etc.</p> <p>Para mayor confianza con datos vitales, construya e incorpore funciones adicionales de validación y chequeo cruzado (p. ej., sumas totalizadas de control).</p> <p>Desarrolle y use herramientas -y habilidades- de prueba automatizadas y manuales, para comprobar cuestiones habituales como desbordamientos de memoria, inyección SQL, etc.</p>
	Porcentaje de sistemas para los cuales los controles de validación de datos se han (a) definido y (b) implementado y demostrado eficaces mediante pruebas.

0 Comments [Show recent to old](#)
[Post a comment](#)

[Attachments](#) (2)

 [RSS of this page](#)

Author: [aglone](#) Version: [1.3](#) Last Edited By: [aglone3](#) Modified: 26 - days ago

Información de contacto

servicios@iso27002.es

Quick Search

- Navigate pages | Site Map
- 12 2 Seguridad de las aplicaciones del sistema

12.2.1. Validación de los datos de entrada

12.2.2. Control del proceso interno

12.2.3. Autenticación de mensajes

12.2.4. Validación de los datos de salida

Site Home » 12. Adquisición, Desarrollo y Mantenimiento de Sistemas de Información » 12 2 Seguridad de las aplicaciones del sistema » 12.2.1. Validación de los datos de entrada

12.2.1. Validación de los datos de entrada



Control:

Se deberían validar los datos de entrada utilizados por las aplicaciones para garantizar que estos datos son correctos y apropiados.

(consultar 10.10.1)

Posibles Soluciones a este control:

Espacio pendiente de posibles aportaciones.

0 Comments Show recent to old
Post a comment

RSS of this page

Author: aglone Version: 1.1 Last Edited By: aglone3 Modified: 27 - days ago

Información de contacto

servicios@iso27002.es

Quick Search

Navigate pages | Site Map

12 2 Seguridad de las aplicaciones del sistema

12.2.1. Validación de los datos de entrada

12.2.2. Control del proceso interno

12.2.3. Autenticación de mensajes

12.2.4. Validación de los datos de salida

Site Home » 12. Adquisición, Desarrollo y Mantenimiento de Sistemas de Información » 12 2 Seguridad de las aplicaciones del sistema » 12.2.2. Control del proceso interno

12.2.2. Control del proceso interno



Control:





Se deberían incluir chequeos de validación en las aplicaciones para la detección de una posible corrupción en la información debida a errores de procesamiento o de acciones deliberadas.

(consultar también 10.1.1)

(consultar 12.2.1)

(consultar 10.10.1)

Posibles Soluciones a este control:

	Rough Auditing Tool for Security (RATS) is an automated code review tool, provided originally by Secure Software Inc, who were acquired by Fortify Software Inc. It scans C, C++, Perl, PHP and Python source code and flags common security related programming errors such as buffer overflows and TOCTOU (Time Of Check, Time Of Use) race conditions. The tool performs a rough analysis of the source code.	RATS
	Graudit is a simple script and signature sets that allows you to find potential security flaws in source code using the GNU utility grep. It's comparable to other static analysis applications like RATS, SWAAT and flaw-finder while keeping the technical requirements to a minimum and being very flexible. Graudit supports scanning code written in several languages; asp, jsp, perl, php and python.	GRAudit
	Code Analysis Tool .NET is a binary code analysis tool that helps identify common variants of certain prevailing vulnerabilities that can give rise to common attack vectors such as Cross-Site Scripting (XSS), SQL Injection and XPath Injection.	Microsoft CAT .NET
	The 2010 CWE/SANS Top 25 Most Dangerous Programming Errors is a list of the most widespread and critical programming errors that can lead to serious software vulnerabilities.	CWE

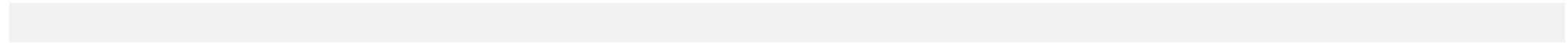
0 Comments [Show recent to old](#)
[Post a comment](#)

 RSS of this page

Author: [aglone](#) Version: [1.1](#) Last Edited By: [aglone3](#) Modified: 27 - days ago

Información de contacto

servicios@iso27002.es



Quick Search

- Navigate pages | Site Map
- 12 2 Seguridad de las aplicaciones del sistema

12.2.1. Validación de los datos de entrada

12.2.2. Control del proceso interno

12.2.3. Autenticación de mensajes

12.2.4. Validación de los datos de salida

Site Home » 12. Adquisición, Desarrollo y Mantenimiento de Sistemas de Información » 12 2 Seguridad de las aplicaciones del sistema » 12.2.3. Autenticación de mensajes

12.2.3. Autenticación de mensajes



Control:

Se deberían identificar los requisitos para asegurar la autenticidad y protección de la integridad del contenido de los mensajes en las aplicaciones, e identificar e implantar los controles apropiados.

Posibles Soluciones a este control:

Espacio pendiente de posibles aportaciones.

0 Comments [Show recent to old](#)
[Post a comment](#)

[RSS of this page](#)

Author: [aglone](#) Version: [1.1](#) Last Edited By: [aglone3](#) Modified: 27 - days ago

Información de contacto

servicios@iso27002.es

Quick Search

- Navigate pages | Site Map
- 12 2 Seguridad de las aplicaciones del sistema
 - 12.2.1. Validación de los datos de entrada
 - 12.2.2. Control del proceso interno
 - 12.2.3. Autenticación de mensajes
 - 12.2.4. Validación de los datos de salida**

 [Site Home](#) >> [12. Adquisición, Desarrollo y Mantenimiento de Sistemas de Información](#) >> [12 2 Seguridad de las aplicaciones del sistema](#) >> 12.2.4. Validación de los datos de salida

12.2.4. Validación de los datos de salida



Control:

Se deberían validar los datos de salida de las aplicaciones para garantizar que el procesamiento de la información almacenada es correcto y apropiado a las circunstancias.

Posibles Soluciones a este control:

Espacio pendiente de posibles aportaciones.

0 Comments [Show recent to old](#)
[Post a comment](#)

 [RSS of this page](#)

Author: [aglone](#) Version: [1.1](#) Last Edited By: [aglone3](#) Modified: 27 - days ago

Información de contacto

servicios@iso27002.es

Quick Search

- Navigate pages | Site Map
- ISO 27002

05. Política de Seguridad

06. Organización de la Seguridad de Información

07. Gestión de Activos

08. Seguridad ligada a los Recursos Humanos

09. Seguridad Física y del Entorno

10. Gestión de Comunicaciones y Operaciones

11. Control de Accesos

12. Adquisición, Desarrollo y Mantenimiento de Sistemas de Información
 - 12 1 Requisitos de seguridad de los sistemas
 - 12 2 Seguridad de las aplicaciones del sistema
 - 12 3 Controles criptográficos
 - 12.3.1. Política de uso de los controles criptográficos
 - 12.3.2. Cifrado
 - 12 4 Seguridad de los ficheros del sistema
 - 12 5 Seguridad en los procesos de desarrollo y soporte
 - 12 6 Gestión de las vulnerabilidades técnicas

13. Gestión de Incidentes de Seguridad de la Información

14. Gestión de Continuidad del Negocio


15. Conformidad

Objetivos





Contacto

Aviso Legal

12 3 Controles criptográficos



Espacio de Patrocinio disponible

 <div>Objetivo</div>	Proteger la confidencialidad, autenticidad o integridad de la información con la ayuda de técnicas criptográficas.
 <div>Principios</div>	Se debería desarrollar una política de uso de controles criptográficos. Se debería establecer una gestión de claves que de soporte al uso de de técnicas criptográficas.
 <div></div>	Utilice estándares formales actuales tales como AES, en lugar de algoritmos de cosecha propia. ¡La implementación es crucial!
 <div></div>	Porcentaje de sistemas que contienen datos valiosos o sensibles para los cuales se han implantado totalmente controles criptográficos apropiados (periodo de reporte de 3 a 12 meses).

0 Comments [Show recent to old](#)
[Post a comment](#)

Attachments (2)

 [RSS of this page](#)

Author: [aglone](#) Version: [1.3](#) Last Edited By: [aglone3](#) Modified: 26 - days ago

Información de contacto

servicios@iso27002.es

Quick Search

- Navigate pages | Site Map
- 12 3 Controles criptográficos
 - 12.3.1. Política de uso de los controles criptográficos
 - 12.3.2. Cifrado

Política de uso de los controles criptográficos

12.3.1. Política de uso de los controles criptográficos



Control:

Se debería desarrollar e implantar una política de uso de controles criptográficos para la protección de la información.







Guías:

([consultar también 5.1.1](#))

([consultar también 12.3.2](#))

([consultar también 15.1.6](#))

Posibles Soluciones a este control:

	Free Open-Source Disk Encryption Software	truecrypt
	Modelo de política de encriptación (inglés)	Sans
	Low cost, easy to use and highly secure encryption and digital signature solutions for every one from big companies to individual users	MXC
	Herramienta gratuita y genera firmas codificadas según el formato PKCS#7 o CMS (Cryptographic Message Syntax)	Albalia
	Implementation of the OpenPGP standard as defined by RFC4880 . GnuPG allows to encrypt and sign your data and communication, features a versatile key managment system as well as access modules for all kind of public key directories. Version 2 of GnuPG also provides support for S/MIME.	GNU project
	Tabla resumen descriptiva de productos y sus funcionalidades de cifrado.	Northwestern

0 Comments

Show recent to old

Post a comment



RSS of this page

Author: [aglone](#)

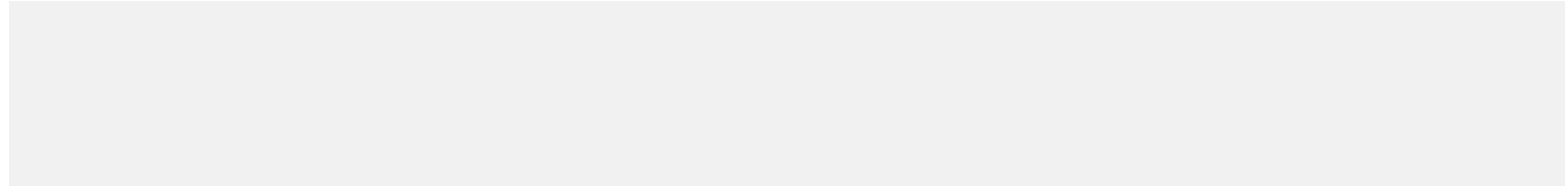
Version: [1.1](#)

Last Edited By: [aglone3](#)

Modified: 27 - days ago

Información de contacto

servicios@iso27002.es



Quick Search

Navigate pages | Site Map

12 3 Controles criptográficos

- 12.3.1. Política de uso de los controles criptográficos
- 12.3.2. Cifrado**

Site Home

»

12. Adquisición, Desarrollo y Mantenimiento de Sistemas de Información

»

12 3 Controles criptográficos

»

12.3.2. Cifrado

12.3.2. Cifrado





Control:

Se debería establecer una gestión de las claves que respalde el uso de las técnicas criptográficas en la Organización.

([consultar 6.2.3](#))

Posibles Soluciones a este control:

	Free Open-Source Disk Encryption Software	http://www.truecrypt.org
	Herramienta gratuita y genera firmas codificadas según el formato PKCS#7 o CMS (Cryptographic Message Syntax)	AlbaliaFirma.zip

0 Comments

[Show recent to old](#)

[Post a comment](#)

 RSS of this page

Author: [aglone](#) Version: [1.1](#) Last Edited By: [aglone3](#) Modified: 27 - days ago

Información de contacto

servicios@iso27002.es

Quick Search

- Navigate pages | Site Map
- ISO 27002

05. Política de Seguridad

06. Organización de la Seguridad de Información

07. Gestión de Activos

08. Seguridad ligada a los Recursos Humanos

09. Seguridad Física y del Entorno

10. Gestión de Comunicaciones y Operaciones

11. Control de Accesos

12. Adquisición, Desarrollo y Mantenimiento de Sistemas de Información

12 1 Requisitos de seguridad de los sistemas

12 2 Seguridad de las aplicaciones del sistema

12 3 Controles criptográficos

12 4 Seguridad de los ficheros del 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 a la librería de programas fuente

12 5 Seguridad en los procesos de desarrollo y soporte

12 6 Gestión de las vulnerabilidades técnicas

13. Gestión de Incidentes de Seguridad de la Información

14. Gestión de Continuidad del Negocio


15. Conformidad

Objetivos





Contacto

Aviso Legal

12 4 Seguridad de los ficheros del sistema



Espacio de Patrocinio disponible

 <div>Objetivo</div>	Garantizar la seguridad de los sistemas de ficheros.
 <div>Principios</div>	Se debería controlar el acceso a los sistemas de ficheros y código fuente de los programas. Los proyectos TI y las actividades de soporte deberían ser dirigidos de un modo seguro. Se debería evitar la exposición de datos sensibles en entornos de prueba.
	Aplique consistentemente estándares de seguridad básica, asegurando que se siguen las recomendaciones de CIS , NIST , fabricantes de sistemas, etc.
	Porcentaje de sistemas evaluados de forma independiente como totalmente conformes con los estándares de seguridad básica aprobados, respecto a aquellos que no han sido evaluados, no son conformes o para los que no se han aprobado dichos estándares.

0 Comments [Show recent to old](#)
[Post a comment](#)

[Attachments \(2\)](#)

 [RSS of this page](#)

Author: [aglone](#) Version: [1.3](#) Last Edited By: [aglone3](#) Modified: 26 - days ago

Información de contacto

servicios@iso27002.es

Quick Search

- Navigate pages | Site Map
- 12 4 Seguridad de los ficheros del 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 a la librería de programas fuente

Site Home » 12. Adquisición, Desarrollo y Mantenimiento de Sistemas de Información » 12 4 Seguridad de los ficheros del sistema » 12.4.1. Control del software en explotación

12.4.1. Control del software en explotación



Control:

Se deberían establecer procedimientos con objeto de controlar la instalación de software en sistemas que estén operativos.

(consultar 12.4.3)

(consultar 10.1.4)

(consultar también 12.6.1)

Posibles Soluciones a este control:

	This document is a guide to patch management, defined as the process of controlling the deployment and maintenance of interim software releases into operational environments.	CPNI
	This document provides guidance on creating a security patch and vulnerability management program and testing the effectiveness of that program.	NIST

0 Comments

Show recent to old

Post a comment

RSS of this page

Author: [aglone](#)

Version: [1.1](#)

Last Edited By: [aglone3](#)

Modified: 27 - days ago

Información de contacto

servicios@iso27002.es

Quick Search

- Navigate pages | Site Map
- 12 4 Seguridad de los ficheros del 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 a la librería de programas fuente

Site Home » 12. Adquisición, Desarrollo y Mantenimiento de Sistemas de Información » 12 4 Seguridad de los ficheros del sistema » 12.4.2. Protección de los datos de prueba del sistema

12.4.2. Protección de los datos de prueba del sistema



Control:

Se deberían seleccionar, proteger y controlar cuidadosamente los datos utilizados para las pruebas.

Posibles Soluciones a este control:

	Guidelines for the Use of Personal Data in System Testing (Second Edition)	http://shop.bsigroup.com
--	--	---

0 Comments [Show recent to old](#)
[Post a comment](#)

RSS of this page

Author: [aglone](#) Version: [1.1](#) Last Edited By: [aglone3](#) Modified: 27 - days ago

Información de contacto

servicios@iso27002.es

Quick Search

Navigate pages | Site Map

12 4 Seguridad de los ficheros del 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 a la librería de programas fuente

Site Home » 12. Adquisición, Desarrollo y Mantenimiento de Sistemas de Información » 12 4 Seguridad de los ficheros del sistema » 12.4.3. Control de acceso a la librería de programas fuente

12.4.3. Control de acceso a la librería de programas fuente



Espacio de Patrocinio disponible

Control:

Se debería restringir el acceso al código fuente de los programas.

(consultar también 11)

(consultar 10.7.4)

(consultar 12.5.1)

Posibles Soluciones a este control:

Espacio pendiente de posibles aportaciones.

0 Comments Show recent to old Post a comment

 RSS of this page

Author: [aglone](#) Version: [1.1](#) Last Edited By: [aglone3](#) Modified: 27 - days ago

Información de contacto

servicios@iso27002.es

Quick Search

Navigate pages | Site Map

ISO 27002

05. Política de Seguridad

06. Organización de la Seguridad de Información

07. Gestión de Activos

08. Seguridad ligada a los Recursos Humanos

09. Seguridad Física y del Entorno

10. Gestión de Comunicaciones y Operaciones

11. Control de Accesos

12. Adquisición, Desarrollo y Mantenimiento de Sistemas de Información

12 1 Requisitos de seguridad de los sistemas

12 2 Seguridad de las aplicaciones del sistema

12 3 Controles criptográficos

12 4 Seguridad de los ficheros del sistema

12 5 Seguridad en los procesos de desarrollo y soporte

12.5.1. Procedimientos de control de cambios

12.5.2. Revisión técnica de los cambios en el sistema operativo

12.5.3. Restricciones en los cambios a los paquetes de software

12.5.4. Canales encubiertos y código Troyano

12.5.5. Desarrollo externalizado del software

12 6 Gestión de las vulnerabilidades técnicas

13. Gestión de Incidentes de Seguridad de la Información

14. Gestión de Continuidad del Negocio

15. Conformidad






Objetivos

Contacto

Aviso Legal


Site Home » 12. Adquisición, Desarrollo y Mantenimiento de Sistemas de Información » 12 5 Seguridad en los procesos de desarrollo y soporte

12 5 Seguridad en los procesos de desarrollo y soporte

	<h1>Espacio de Patrocinio disponible</h1>
	Mantener la seguridad del software del sistema de aplicaciones y la información.
	Se deberían controlar estrictamente los entornos de desarrollo de proyectos y de soporte. Los directivos responsables de los sistemas de aplicaciones deberían ser también responsables de la seguridad del proyecto o del entorno de soporte. Ellos deberían garantizar que todas las propuestas de cambio en los sistemas son revisadas para verificar que no comprometen la seguridad del sistema o del entorno operativo.
	Incorpore la seguridad de la información al ciclo de vida de desarrollo de sistemas en todas sus fases, desde la concepción hasta la desaparición de un sistema, por medio de la inclusión de "recordatorios" sobre seguridad en los procedimientos y métodos de desarrollo, operaciones y gestión de cambios. Trate el desarrollo e implementación de software como un proceso de cambio. Integre las mejoras de seguridad en las actividades de gestión de cambios (p. ej., documentación y formación procedimental para usuarios y administradores).
	"Estado de la seguridad en sistemas en desarrollo", es decir, un informe sobre el estado actual de la seguridad en los procesos de desarrollo de software, con comentarios sobre incidentes recientes/actuales, vulnerabilidades actuales de seguridad conocidas y pronósticos sobre cualquier riesgo creciente, etc.

0 Comments [Show recent to old](#)
[Post a comment](#)

[Attachments \(2\)](#)

 [RSS of this page](#)

Author: [aglone](#) Version: [1.3](#) Last Edited By: [aglone3](#) Modified: 26 - days ago

Información de contacto

servicios@iso27002.es

Powered by [Zoho Wiki](#) | [Zoho](#) | [Report Abuse](#) | [Wiki Index](#) | [Site Map](#) | [Help](#) | [Feedback](#) | [Jump Start with 2 Free Wikis](#) | [Sign in](#)

http://iso27002.wiki.zoho.com/12-5-Seguridad-en-los-procesos-de-desarrollo-y-soporte.html[28/01/2011 08:37:55 p.m.]

Quick Search

- Navigate pages | Site Map
- 12 5 Seguridad en los procesos de desarrollo y soporte
 - 12.5.1. Procedimientos de control de cambios
 - 12.5.2. Revisión técnica de los cambios en el sistema operativo
 - 12.5.3. Restricciones en los cambios a los paquetes de software
 - 12.5.4. Canales encubiertos y código Troyano
 - 12.5.5. Desarrollo externalizado del software

Site Home » 12. Adquisición, Desarrollo y Mantenimiento de Sistemas de Información » 12 5 Seguridad en los procesos de desarrollo y soporte » 12.5.1. Procedimientos de control de cambios

12.5.1. Procedimientos de control de cambios



Control:

Se debería controlar la implantación de cambios mediante la aplicación de procedimientos formales de control de cambios.

(consultar 10.1.2)

(consultar 10.1.1)

Posibles Soluciones a este control:

Espacio pendiente de posibles aportaciones.

0 Comments Show recent to old
Post a comment

RSS of this page

Author: [aglone](#) Version: [1.1](#) Last Edited By: [aglone3](#) Modified: 27 - days ago

Información de contacto

servicios@iso27002.es

Quick Search

- Navigate pages | Site Map
- 12 5 Seguridad en los procesos de desarrollo y soporte

 - 12.5.1. Procedimientos de control de cambios
 - 12.5.2. Revisión técnica de los cambios en el sistema operativo**
 - 12.5.3. Restricciones en los cambios a los paquetes de software
 - 12.5.4. Canales encubiertos y código Troyano
 - 12.5.5. Desarrollo externalizado del software

Site Home » 12. Adquisición, Desarrollo y Mantenimiento de Sistemas de Información » 12 5 Seguridad en los procesos de desarrollo y soporte » 12.5.2. Revisión técnica de los cambios en el sistema operativo

12.5.2. Revisión técnica de los cambios en el sistema operativo



Control:

Se deberían revisar y probar las aplicaciones críticas de negocio cuando se realicen cambios en el sistema operativo, con objeto de garantizar que no existen impactos adversos para las actividades o seguridad de la Organización

([consultar cláusula 14](#))

([consultar 12.6](#))

Posibles Soluciones a este control:

Espacio pendiente de posibles aportaciones.

0 Comments [Show recent to old](#)

Post a comment

 RSS of this page

Author: [aglone](#) Version: [1.1](#) Last Edited By: [aglone3](#) Modified: 27 - days ago

Información de contacto



Quick Search

- Navigate pages | Site Map
- 12 5 Seguridad en los procesos de desarrollo y soporte

12.5.1. Procedimientos de control de cambios

12.5.2. Revisión técnica de los cambios en el sistema operativo

12.5.3. Restricciones en los cambios a los paquetes de software

12.5.4. Canales encubiertos y código Troyano

12.5.5. Desarrollo externalizado del software

Site Home » 12. Adquisición, Desarrollo y Mantenimiento de Sistemas de Información » 12 5 Seguridad en los procesos de desarrollo y soporte » 12.5.3. Restricciones en los cambios a los paquetes de software

12.5.3. Restricciones en los cambios a los paquetes de software



Control:

Se debería desaconsejar la modificación de los paquetes de software, restringiéndose a lo imprescindible y todos los cambios deberían ser estrictamente controlados.

(consultar 12.6)

Posibles Soluciones a este control:

Espacio pendiente de posibles aportaciones.

0 Comments

Show recent to old

Post a comment

RSS of this page

Author: [aglone](#)

Version: [1.1](#)

Last Edited By: [aglone3](#)

Modified: 27 - days ago

Información de contacto

servicios@iso27002.es

Quick Search

- Navigate pages | Site Map
- 12 5 Seguridad en los procesos de desarrollo y soporte

 - 12.5.1. Procedimientos de control de cambios
 - 12.5.2. Revisión técnica de los cambios en el sistema operativo
 - 12.5.3. Restricciones en los cambios a los paquetes de software
 - 12.5.4. Canales encubiertos y código Troyano**
 - 12.5.5. Desarrollo externalizado del software

Site Home » 12. Adquisición, Desarrollo y Mantenimiento de Sistemas de Información » 12 5 Seguridad en los procesos de desarrollo y soporte » 12.5.4. Canales encubiertos y código Troyano

12.5.4. Canales encubiertos y código Troyano



Control:

Se debería prevenir las posibilidades de fuga de información.

(consultar ISO/IEC 15408)

Posibles Soluciones a este control:

Espacio pendiente de posibles aportaciones.

0 Comments

Show recent to old

Post a comment

RSS of this page

Author: [aglone](#)

Version: [1.1](#)

Last Edited By: [aglone3](#)

Modified: 27 - days ago

Información de contacto

servicios@iso27002.es

Quick Search

- Navigate pages | Site Map
- 12 5 Seguridad en los procesos de desarrollo y soporte
 - 12.5.1. Procedimientos de control de cambios
 - 12.5.2. Revisión técnica de los cambios en el sistema operativo
 - 12.5.3. Restricciones en los cambios a los paquetes de software
 - 12.5.4. Canales encubiertos y código Troyano
 - 12.5.5. Desarrollo externalizado del software**

 [Site Home](#) » [12. Adquisición, Desarrollo y Mantenimiento de Sistemas de Información](#) » [12 5 Seguridad en los procesos de desarrollo y soporte](#) » 12.5.5. Desarrollo externalizado del software

12.5.5. Desarrollo externalizado del software



Control:

Se debería supervisar y monitorizar el desarrollo del software subcontratado por la Organización.

([consultar 15.1.2](#))

Posibles Soluciones a este control:

Espacio pendiente de posibles aportaciones.

0 Comments [Show recent to old](#)
[Post a comment](#)

 [RSS of this page](#)

Author: [aglone](#) Version: [1.1](#) Last Edited By: [aglone3](#) Modified: 27 - days ago

Información de contacto

servicios@iso27002.es

Quick Search

- Navigate pages | Site Map
- ISO 27002

⊞ 05. Política de Seguridad

⊞ 06. Organización de la Seguridad de Información

⊞ 07. Gestión de Activos

⊞ 08. Seguridad ligada a los Recursos Humanos

⊞ 09. Seguridad Física y del Entorno

⊞ 10. Gestión de Comunicaciones y Operaciones

⊞ 11. Control de Accesos

⊞ 12. Adquisición, Desarrollo y Mantenimiento de Sistemas de Información

⊞ 12 1 Requisitos de seguridad de los sistemas

⊞ 12 2 Seguridad de las aplicaciones del sistema

⊞ 12 3 Controles criptográficos

⊞ 12 4 Seguridad de los ficheros del sistema

⊞ 12 5 Seguridad en los procesos de desarrollo y soporte

⊞ 12 6 Gestión de las vulnerabilidades técnicas

● 12.6.1. Control de las vulnerabilidades técnicas





⊞ 13. Gestión de Incidentes de Seguridad de la Información

⊞ 14. Gestión de Continuidad del Negocio


⊞ 15. Conformidad

● Objetivos

● Contacto

● Aviso Legal
- Site Home » 12. Adquisición, Desarrollo y Mantenimiento de Sistemas de Información » 12 6 Gestión de las vulnerabilidades técnicas
- ## 12 6 Gestión de las vulnerabilidades técnicas
-
- | | |
|---|---|
|  Objetivo | Reducir los riesgos originados por la explotación de vulnerabilidades técnicas publicadas. |
|  Principios | <p>Se debería implantar una gestión de la vulnerabilidad técnica siguiendo un método efectivo, sistemático y cíclico, con la toma de medidas que confirmen su efectividad.</p> <p>Se deberían considerar sistemas operativos, así como todas las aplicaciones que se encuentren en uso.</p> |
|  | <p>Haga un seguimiento constante de parches de seguridad mediante herramientas de gestión de vulnerabilidades y/o actualización automática siempre que sea posible (p. ej., Microsoft Update o Secunia Software Inspector).</p> <p>Evalúe la relevancia y criticidad o urgencia de los parches en su entorno tecnológico.</p> <p>Pruebe y aplique los parches críticos, o tome otras medidas de protección, tan rápida y extensamente como sea posible, para vulnerabilidades de seguridad que afecten a sus sistemas y que estén siendo explotadas fuera activamente.</p> <p>Evite quedarse tan atrás en la rutina de actualización de versiones que sus sistemas queden fuera de soporte por el fabricante.</p> |
|  | Latencia de parcheo o semiperiodo de despliegue (tiempo que ha llevado parchear la mitad de los sistemas vulnerables -evita variaciones circunstanciales debidas a retrasos en unos pocos sistemas, tales como portátiles fuera de la empresa o almacenados-). |
- 0 Comments

Show recent to old

Post a comment
- Attachments (2)
-  RSS of this page
- Author: [aglone](#) Version: [1.3](#) Last Edited By: [aglone3](#) Modified: 26 - days ago
- ### Información de contacto
- servicios@iso27002.es
- Powered by [Zoho Wiki](#) | [Zoho](#) | [Report Abuse](#) | [Wiki Index](#) | [Site Map](#) | [Help](#) | [Feedback](#) | [Jump Start with 2 Free Wikis](#) | [Sign in](#)
- http://iso27002.wiki.zoho.com/12-6-Gestión-de-las-vulnerabilidades-técnicas.html[28/01/2011 08:38:53 p.m.]

Quick Search

Navigate pages | Site Map

12 6 Gestión de las vulnerabilidades técnicas

12.6.1. Control de las vulnerabilidades técnicas

12.6.1. Control de las vulnerabilidades técnicas



Control:

Se debería obtener información oportuna sobre la vulnerabilidad técnica de los sistemas de información que se están utilizando, evaluar la exposición de la organización ante tal vulnerabilidad y tomar las medidas adecuadas para hacer frente a los riesgos asociados.

(consultar 7.1)

(consultar 7.1.1)

(consultar 12.5.1)

(consultar 13.2)

(consultar 11.4.5)

Posibles Soluciones a este control:

	This is a VA / PT report for a fictitious bank called eClipse Bank PLC carried out by another fictitious company Cynergi Solutions Inc. All names, URLs, IPs, etc are fictitious	Vulnerability Assessment & Penetration Test Report template
	SQLmap is an open source automatic SQL injection tool. It is able to detect and exploit SQL injections and allows the user to enumerate data from the database, execute commands on the operating system, establish an out-of-band connection and much more.	SQL Map
	OpenVAS stands for Open Vulnerability Assessment System and is a network security scanner with associated tools like a graphical user front-end. The core component is a server with a set of network vulnerability tests (NVTs) to detect security problems in remote systems and applications. OpenVAS products are Free Software under GNU GPL.	OpenVAS
	The Open Web Application Security Project (OWASP) is a not-for-profit worldwide charitable organization focused on improving the security of application software.	OWASP
	NeXpose Community Edition enables security professionals to start implementing a formalized vulnerability management program, prove the value of their security testing efforts and protect business data in critical infrastructure assets.	Nexpose
	Fully featured security distribution consisting of a bunch of powerful, open source and free tools that can be used for various purposes including, but not limited to, penetration testing, ethical hacking, system and network administration, cyber forensics investigations, security testing, vulnerability analysis, and much more.	Matriux
	A fully automated, active web application security reconnaissance tool.	Google Code Skipfish
	This document is a sample of a vulnerability testing process for a fictitious company, Company X. It outlines Company X's technical security testing process. The key deliverable is to take a risk base approach to identifying and validating system vulnerabilities.	Testing Process
	Cuando se completa un análisis de red, las capacidades de Gestión de Actualizaciones de GFI LANguard le proporcionan lo que necesita para instalar y administrar eficazmente las actualizaciones en todos los equipos a través de diferentes plataformas de sistemas operativos y productos Microsoft en 38 idiomas. No sólo puede descargar automáticamente las actualizaciones de seguridad de Microsoft que falten, también puede implantar automáticamente las actualizaciones o service packs de Microsoft que falten en toda la red al final de los análisis programados.	GFI LANguard

0 Comments [Show recent to old](#)
[Post a comment](#)

Información de contacto

servicios@iso27002.es

Quick Search

- Navigate pages | Site Map
- ISO 27002

⊞ 05. Política de Seguridad

⊞ 06. Organización de la Seguridad de Información

⊞ 07. Gestión de Activos

⊞ 08. Seguridad ligada a los Recursos Humanos

⊞ 09. Seguridad Física y del Entorno

⊞ 10. Gestión de Comunicaciones y Operaciones

⊞ 11. Control de Accesos

⊞ 12. Adquisición, Desarrollo y Mantenimiento de Sistemas de Información

⊞ 13. Gestión de Incidentes de Seguridad de la Información

⊞ 13 1 Comunicación de eventos y debilidades en la seguridad de la información

● 13 1 1 Comunicación de eventos en seguridad

● 13.1.2. Comunicación de debilidades en seguridad

⊞ 13 2 Gestión de incidentes y mejoras en la seguridad de la información

⊞ 14. Gestión de Continuidad del Negocio

⊞ 15. Conformidad

● Objetivos






● Contacto

● Aviso Legal
- Site Home

>>

13. Gestión de Incidentes de Seguridad de la Información

>>

13 1 Comunicación de eventos y debilidades en la seguridad de la información
- ## 13 1 Comunicación de eventos y debilidades en la seguridad de la información
-
- | | |
|--|--|
| 
Objetivo | Garantizar que los eventos y debilidades en la seguridad asociados con los sistemas de información se comuniquen de modo que se puedan realizar acciones correctivas oportunas. |
| 
Principios | <p>Debería establecerse el informe formal de los eventos y de los procedimientos de escalada.</p> <p>Todos los empleados, contratistas y terceros deberían estar al tanto de los procedimientos para informar de los diferentes tipos de eventos y debilidades que puedan tener impacto en la seguridad de los activos organizacionales.</p> <p>Se les debería exigir que informen de cualquier evento o debilidad en la seguridad de información lo más rápido posible y al punto de contacto designado.</p> |
|  | Establezca y dé a conocer una hotline (generalmente, el helpdesk habitual de TI) para que la gente pueda informar de incidentes, eventos y problemas de seguridad. |
|  | <p>Estadísticas del helpdesk de TI, con análisis sobre el número y tipos de llamadas relativas a seguridad de la información (p. ej., cambios de contraseña; porcentaje de preguntas acerca de riesgos y controles de seguridad de la información respecto al total de preguntas).</p> <p>A partir de las estadísticas, cree y publique una tabla de clasificación por departamentos (ajustada según el número de empleados por departamento), mostrando aquellos que están claramente concienciados con la seguridad, frente a los que no lo están.</p> |
- 0 Comments [Show recent to old](#)
[Post a comment](#)
- [Attachments](#) (2)
-  [RSS of this page](#)
- Author: [aglone](#) Version: [1.3](#) Last Edited By: [aglone3](#) Modified: 26 - days ago
- ### Información de contacto
- servicios@iso27002.es
- Powered by [Zoho Wiki](#) | [Zoho](#) | [Report Abuse](#) | [Wiki Index](#) | [Site Map](#) | [Help](#) | [Feedback](#) | [Jump Start with 2 Free Wikis](#) | [Sign in](#)
- http://iso27002.wiki.zoho.com/13-1-Comunicación-de-eventos-y-debilidades-en-la-seguridad-de-la-información.html[28/01/2011 08:39:13 p.m.]

Quick Search

Navigate pages | Site Map

13 1 Comunicación de eventos y debilidades en la seguridad de la información

- 13 1 1 Comunicación de eventos en seguridad
- 13.1.2. Comunicación de debilidades en seguridad

Site Home » 13. Gestión de Incidentes de Seguridad de la Información » 13 1 Comunicación de eventos y debilidades en la seguridad de la información » 13 1 1 Comunicación de eventos en seguridad

13 1 1 Comunicación de eventos en seguridad



Control:





Se deberían comunicar los eventos en la seguridad de información lo más rápido posible mediante canales de gestión apropiados.

(consultar 8.2.2)

(consultar 13.2.3)

Para mayor información sobre el reporte de eventos y la gestión de incidentes en la seguridad de información se puede consultar la norma ISO/IEC TR 18044.

Posibles Soluciones a este control:

	Modelos para la comunicación y gestión de incidentes (inglés)	Sans.org
	Spiceworks is the complete network management & monitoring, helpdesk, PC inventory & software reporting solution to manage Everything IT in small and medium businesses.	Spiceworks
	Paglo is on-demand tool. Businesses can discover all their IT information and get instant answers to their computer, network, and security questions.	Paglo
	GMF is a free software project distributed under the GPL (GNU Public License). It provides a general framework to manage contents going a step further of traditional CMS which are built thinking about content publishing.	GMF - GenosOrg

0 Comments [Show recent to old](#)
[Post a comment](#)

[Attachments \(1\)](#)

 [RSS of this page](#)

Author: [aglone](#) Version: [1.5](#) Last Edited By: [aglone3](#) Modified: 27 - days ago

Información de contacto

servicios@iso27002.es

Quick Search

Navigate pages | Site Map

13 1 Comunicación de eventos y debilidades en la seguridad de la información

13 1 1 Comunicación de eventos en seguridad

13.1.2. Comunicación de debilidades en seguridad

Site Home » 13. Gestión de Incidentes de Seguridad de la Información » 13 1 Comunicación de eventos y debilidades en la seguridad de la información » 13.1.2. Comunicación de debilidades en seguridad

13.1.2. Comunicación de debilidades en seguridad



Control:

Todos los empleados, contratistas y terceros que son usuarios de los sistemas y servicios de información deberían anotar y comunicar cualquier debilidad observada o sospechada en la seguridad de los mismos.

Posibles Soluciones a este control:

Espacio pendiente de posibles aportaciones.

0 Comments [Show recent to old](#)
[Post a comment](#)

 [RSS of this page](#)

Author: [aglone](#) Version: [1.1](#) Last Edited By: [aglone3](#) Modified: 27 - days ago

Información de contacto

servicios@iso27002.es

Quick Search

- Navigate pages | Site Map
- ISO 27002

05. Política de Seguridad

06. Organización de la Seguridad de Información

07. Gestión de Activos

08. Seguridad ligada a los Recursos Humanos

09. Seguridad Física y del Entorno

10. Gestión de Comunicaciones y Operaciones

11. Control de Accesos

12. Adquisición, Desarrollo y Mantenimiento de Sistemas de Información

13. Gestión de Incidentes de Seguridad de la Información
 - 13 1 Comunicación de eventos y debilidades en la seguridad de la información
 - 13 2 Gestión de incidentes y mejoras en la seguridad de la información**
 - 13.2.1. Identificación de responsabilidades y procedimientos
 - 13.2.2. Evaluación de incidentes en seguridad
 - 13.2.3. Recogida de pruebas

14. Gestión de Continuidad del Negocio






15. Conformidad

Objetivos

Contacto

Aviso Legal

13 2 Gestión de incidentes y mejoras en la seguridad de la información

	<h1>Espacio de Patrocinio disponible</h1>
	Garantizar que se aplica un enfoque consistente y eficaz para la gestión de los incidentes en la seguridad de información.
	<p>Deberían establecerse las responsabilidades y procedimientos para manejar los eventos y debilidades en la seguridad de información de una manera efectiva y una vez que hayan sido comunicados.</p> <p>Se debería aplicar un proceso de mejora continua en respuesta para monitorear, evaluar y gestionar en su totalidad los incidentes en la seguridad de información.</p> <p>Cuando se requieran evidencias, éstas deben ser recogidas para asegurar el cumplimiento de los requisitos legales.</p>
	Las revisiones post-incidente y los casos de estudio para incidentes serios, tales como fraudes, ilustran los puntos débiles de control, identifican oportunidades de mejora y conforman por sí mismos un mecanismo eficaz de concienciación en seguridad.
	<p>Número y gravedad de incidentes; evaluaciones de los costes de analizar, detener y reparar los incidentes y cualquier pérdida tangible o intangible producida.</p> <p>Porcentaje de incidentes de seguridad que han causado costes por encima de umbrales aceptables definidos por la dirección.</p>

0 Comments

Show recent to old

Post a comment

Attachments (2)



RSS of this page

Author: [aglone](#)

Version: [1.3](#)

Last Edited By: [aglone3](#)

Modified: 26 - days ago

Información de contacto

servicios@iso27002.es

Quick Search

- Navigate pages | Site Map
- 13 2 Gestión de incidentes y mejoras en la seguridad de la información

 - 13.2.1. Identificación de responsabilidades y procedimientos
 - 13.2.2. Evaluación de incidentes en seguridad
 - 13.2.3. Recogida de pruebas

13.2.1. Identificación de responsabilidades y procedimientos



Control:

Se deberían establecer las responsabilidades y procedimientos de gestión para asegurar una respuesta rápida, efectiva y ordenada a los incidentes en la seguridad de información.

- (consultar 13.1)
- (consultar 10.10.2)
- (consultar 10.4.1)
- (consultar 14.1.3)
- (consultar 13.2.2)
- (consultar 13.2.3)
- (consultar también 6.2 para acceso externo)

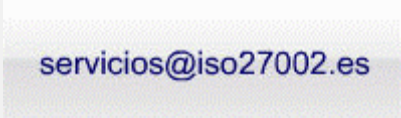
Posibles Soluciones a este control:

Espacio pendiente de posibles aportaciones.

0 Comments [Show recent to old](#)

Post a comment

Información de contacto



Quick Search

- Navigate pages | Site Map
- 13 2 Gestión de incidentes y mejoras en la seguridad de la información
 - 13.2.1. Identificación de responsabilidades y procedimientos
 - 13.2.2. Evaluación de incidentes en seguridad**
 - 13.2.3. Recogida de pruebas

 [Site Home](#) » [13. Gestión de Incidentes de Seguridad de la Información](#) » [13 2 Gestión de incidentes y mejoras en la seguridad de la información](#) » 13.2.2. Evaluación de incidentes en seguridad

13.2.2. Evaluación de incidentes en seguridad




Control:

Debería existir un mecanismo que permitan cuantificar y monitorear los tipos, volúmenes y costes de los incidentes en la seguridad de información.

([consultar 5.1.2](#))

Posibles Soluciones a este control:

	Guía de respuesta a incidentes del GovCertUK, organismo responsable del soporte a los departamentos gubernamentales del Reino Unido en los incidentes de seguridad.	Incident Response Guidelines
---	---	--

0 Comments [Show recent to old](#)
[Post a comment](#)

 [RSS of this page](#)

Author: [aglone](#) **Version:** [1.1](#) **Last Edited By:** [aglone3](#) **Modified:** 27 - days ago

Información de contacto

servicios@iso27002.es

Quick Search

Navigate pages | Site Map

13 2 Gestión de incidentes y mejoras en la seguridad de la información

- 13.2.1. Identificación de responsabilidades y procedimientos
- 13.2.2. Evaluación de incidentes en seguridad
- 13.2.3. Recogida de pruebas**

13.2.3. Recogida de pruebas



Control:

Cuando una acción de seguimiento contra una persona u organización, después de un incidente en la seguridad de información, implique acción legal (civil o criminal), la evidencia debe ser recolectada, retenida y presentada conforme a las reglas para la evidencia establecidas en la jurisdicción relevante.

Posibles Soluciones a este control:

	Closed circuit television (CCTV). Management and operation. Code of practice	http://shop.bsigroup.com
	CAINE (Computer Aided INvestigative Environment) is an Italian GNU/Linux live distribution created as a project of Digital Forensics. CAINE offers a complete forensic environment that is organized to integrate existing software tools as software modules and to provide a friendly graphical interface.	Caine
	Fully featured security distribution consisting of a bunch of powerful, open source and free tools that can be used for various purposes including, but not limited to, penetration testing, ethical hacking, system and network administration, cyber forensics investigations, security testing, vulnerability analysis, and much more.	Matriux
	AVG Rescue CD es un poderoso juego de herramientas indispensable para rescatar y reparar equipos infectados.	AVG CD rescate
	The SANS SIFT Workstation is a VMware Appliance that is pre-configured with all the necessary tools to perform a detailed digital forensic examination. It is compatible with Expert Witness Format (E01), Advanced Forensic Format (AFF), and raw (dd) evidence formats. The brand new version has been completely rebuilt on an Ubuntu base with many additional tools and capabilities that can match any modern forensic tool suite.	SANS

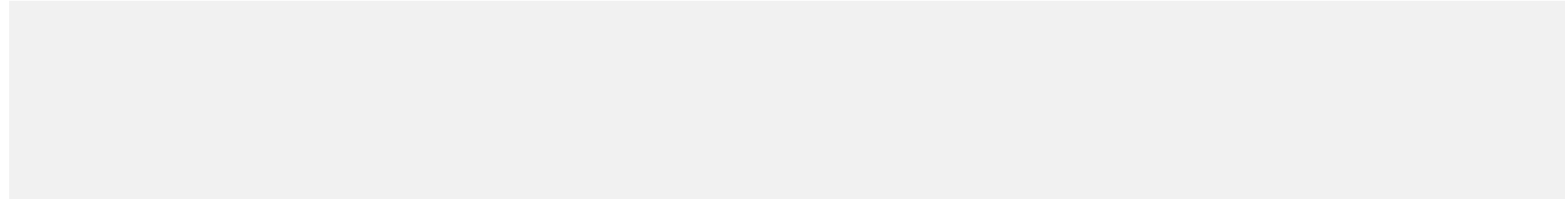
0 Comments [Show recent to old](#)
[Post a comment](#)

[RSS of this page](#)

Author: [aglone](#) Version: [1.1](#) Last Edited By: [aglone3](#) Modified: 27 - days ago

Información de contacto

servicios@iso27002.es



Quick Search

Navigate pages | Site Map

ISO 27002

05. Política de Seguridad

06. Organización de la Seguridad de Información

07. Gestión de Activos

08. Seguridad ligada a los Recursos Humanos

09. Seguridad Física y del Entorno

10. Gestión de Comunicaciones y Operaciones

11. Control de Accesos

12. Adquisición, Desarrollo y Mantenimiento de Sistemas de Información

13. Gestión de Incidentes de Seguridad de la Información

14. Gestión de Continuidad del Negocio

14 1 Aspectos de la gestión de continuidad del negocio

14.1.1. Proceso de la gestión de continuidad del negocio

14.1.2. Continuidad del negocio y análisis de impactos

14.1.3. Redacción e implantación de planes de continuidad

14.1.4. Marco de planificación para la continuidad del negocio

14.1.5. Prueba, mantenimiento y reevaluación de planes de continuidad

15. Conformidad





Objetivos

Contacto

Aviso Legal

14 1 Aspectos de la gestión de continuidad del negocio



	Reaccionar a la interrupción de actividades del negocio y proteger sus procesos críticos frente a desastres o grandes fallos de los sistemas de información.
	<p>Se debería implantar un proceso de gestión de continuidad del negocio para reducir, a niveles aceptables, la interrupción causada por los desastres y fallos de seguridad (que, por ejemplo, puedan resultar de desastres naturales, accidentes, fallas de equipos o acciones deliberadas) mediante una combinación de controles preventivos y de recuperación.</p> <p>Este proceso debería identificar los procesos críticos de negocio e integrar los requisitos de gestión de la seguridad de información para la continuidad del negocio con otros requisitos de continuidad relacionados con dichos aspectos como operaciones, proveedores de personal, materiales, transporte e instalaciones.</p> <p>Se deberían analizar las consecuencias de los desastres, fallas de seguridad, pérdidas de servicio y la disponibilidad del servicio y desarrollar e implantar planes de contingencia para asegurar que los procesos del negocio se pueden restaurar en los plazos requeridos las operaciones esenciales.</p> <p>La seguridad de información debería ser una parte integral del plan general de continuidad del negocio y de los demás procesos de gestión dentro de la organización.</p> <p>La gestión de la continuidad del negocio debería incluir adicionalmente al proceso de evaluación, controles para la identificación y reducción de riesgos, limitar las consecuencias de incidencias dañinas y asegurar la reanudación a tiempo de las operaciones esenciales.</p>
	<p>Considere la gestión de continuidad de negocio como un proceso con entradas procedentes de diversas funciones (alta dirección, TI, operaciones, RRHH, etc.) y actividades (evaluación de riesgos, etc.).</p> <p>Asegure la coherencia y concienciación mediante personas y unidades organizativas relevantes en los planes de continuidad de negocio.</p> <p>Deberían llevarse a cabo las pruebas pertinentes (tales como pruebas sobre el papel, simulacros, pruebas de failover, etc.) para (a) mantener los planes actualizados, (b) aumentar la confianza de la dirección en los planes y (c) familiarizar a los empleados relevantes con sus funciones y responsabilidades bajo condiciones de desastre.</p> <p>Obtenga consejos de implantación en BS 25999 - Gestión de la Continuidad de Negocio.</p>
	<p>Porcentaje de planes de continuidad de negocio en cada una de las fases del ciclo de vida (requerido / especificado / documentado / probado).</p> <p>Porcentaje de unidades organizativas con planes de continuidad de negocio que han sido adecuadamente (a) documentados y (b) probados mediante tests apropiados en los últimos 12 meses.</p>

0 Comments [Show recent to old](#)
[Post a comment](#)

[Attachments \(2\)](#)

 [RSS of this page](#)

Author: [aglone](#) Version: [1.3](#) Last Edited By: [aglone3](#) Modified: 26 - days ago

Información de contacto

servicios@iso27002.es

Quick Search

Navigate pages | Site Map

14 1 Aspectos de la gestión de continuidad del negocio

14.1.1. Proceso de la gestión de continuidad del negocio

14.1.2. Continuidad del negocio y análisis de impactos

14.1.3. Redacción e implantación de planes de continuidad

14.1.4. Marco de planificación para la continuidad del negocio

14.1.5. Prueba, mantenimiento y reevaluación de planes de continuidad

Proceso de la gestión de continuidad del negocio

14.1.1. Proceso de la gestión de continuidad del negocio



Control:

Se debería desarrollar y mantener un proceso de gestión de la continuidad del negocio en la organización que trate los requerimientos de seguridad de la información necesarios para la continuidad del negocio.

(consultar 14.1.2)

(consultar 7.1.1)

(consultar 14.1.3)

(consultar 14.1.5)

(consultar 6.1.1)

Posibles Soluciones a este control:

	Guía práctica para pymes en español de cómo implantar un plan de continuidad de negocio, editada por Inteco y Deloitte.	Guía pymes continuidad de negocio
	Guía en inglés de buenas prácticas de continuidad de negocio del Business Continuity Institute.	BCI Good Practices
	Estándar NIST SP 800-34 sobre planificación de contingencias para sistemas de información (en inglés).	NIST SP 800-34
	Buenas prácticas de gestión de continuidad de negocio del Disaster Recovery Institute International - DRII (en inglés).	DRII Professional Practices
	Guía de continuidad de negocio de ASIS International (en inglés).	ASIS Business Continuity Guideline
	BS 25999-1: Norma de BSI en inglés que recoge un código de buenas prácticas para la gestión de la continuidad de negocio.	BS 25999-1:2006 en inglés
	Traducción al español de la norma BS 25999-1:2006.	BS 25999-1:2006 en español
	UNE 71599-1: Norma española de buenas prácticas en gestión de contiuidad de negocio, basada en BS 25999-1:2006.	UNE 71599-1:2010
	BS 25999-2: Norma de BSI en inglés que establece los requisitos para un sistema de gestión de continuidad de negocio.	BS 25999-2:2007 en inglés
	Traducción al español de la norma BS 25999-2:2007.	BS 25999-2:2007 en español
	UNE 71599-2: Norma española que establece los requisitos para un sistema de gestión de continuidad de negocio, basada en BS 25999-2:2007.	UNE 71599-2:2010
	GTAG 10, Guía de gestión de continuidad de negocio del Institute of Internal Auditors (en inglés).	GTAG 10 - Business Continuity Management
	Guía de planificación de continuidad de negocio, en inglés, del Federal Financial Institutions Examination Council. La acompaña una lista de verificación -checklist-, útil para auditar el proceso.	FFIEC BCP FFIEC Audit of BC workprogram
FIST Conference	Presentación en español de Manuel Ballester, de introducción a la continuidad de negocio, realizada en las Conferencias FIST.	FISTconference.org
	BS 25777:2008: Norma, en inglés, de BSI de buenas prácticas de gestión de continuidad de las TIC.	BS 25777:2008
	ISO/IEC 24762: Directrices para servicios de recuperación de desastres TIC (en inglés).	ISO/IEC 24762
	Guía de gestión de continuidad de negocio publicada por el gobierno de la provincia canadiense de Saskatchewan (en inglés).	BCM Planning Guidelines

1 Comments Show recent to old

Guest, 7 - days ago

Otra presentación de Manuel Ballester sobre continuidad de negocio:

http://www.slideshare.net/slides_eoi/continuidad-de-negocio-usando-software-libre

Post a comment



RSS of this page

Author: [aglone](#) Version: [1.6](#) Last Edited By: [javier_ruiz](#) Modified: 7 - days ago

Información de contacto

servicios@iso27002.es

Quick Search

- Navigate pages | Site Map
- 14 1 Aspectos de la gestión de continuidad del negocio
 - 14.1.1. Proceso de la gestión de continuidad del negocio
 - 14.1.2. Continuidad del negocio y análisis de impactos**
 - 14.1.3. Redacción e implantación de planes de continuidad
 - 14.1.4. Marco de planificación para la continuidad del negocio
 - 14.1.5. Prueba, mantenimiento y reevaluación de planes de continuidad

🏠 Site Home » 14. Gestión de Continuidad del Negocio » 14 1 Aspectos de la gestión de continuidad del negocio » 14.1.2.

Continuidad del negocio y análisis de impactos






14.1.2. Continuidad del negocio y análisis de impactos



Control:

Se deberían identificar los eventos que puedan causar interrupciones a los procesos de negocio junto con la probabilidad e impacto de dichas interrupciones y sus consecuencias para la seguridad de información.

Posibles Soluciones a este control:

	Solutions from Q1 Labs are quickly becoming the standard for centralized management of enterprise network and security information.	Oradar
	Basic tools to help you get your BCM programme underway. They are all free and can be adapted for most types of organisation (except maybe the very large).	Talking Business Continuity
	Here you will find information for businesses and voluntary organisations about business continuity management (BCM). Business continuity management can ensure your organisation can handle an emergency, continue to function, and can recover effectively afterwards.	direct.gov.uk
	"Business Continuity Planning Workbook" del gobierno de la provincia canadiense de Saskatchewan, con especial incidencia en el análisis de impactos. En inglés.	BC Planning Workbook
	Consejos para la realización de un Business Impact Analysis (BIA), en inglés.	SANS Institute Reading Room

0 Comments [Show recent to old](#)
[Post a comment](#)

 RSS of this page

Author: [aglone](#) Version: [1.3](#) Last Edited By: [javier ruiz](#) Modified: 8 - days ago

Información de contacto

servicios@iso27002.es

Quick Search

Navigate pages | Site Map

14 1 Aspectos de la gestión de continuidad del negocio

14.1.1. Proceso de la gestión de continuidad del negocio

14.1.2. Continuidad del negocio y análisis de impactos

14.1.3. Redacción e implantación de planes de continuidad

14.1.4. Marco de planificación para la continuidad del negocio

14.1.5. Prueba, mantenimiento y reevaluación de planes de continuidad

Redacción e implantación de planes de continuidad

14.1.3. Redacción e implantación de planes de continuidad



Control:

Se deberían desarrollar e implantar planes de mantenimiento o recuperación de las operaciones del negocio para asegurar la disponibilidad de la información en el grado y en las escalas de tiempo requeridos, tras la interrupción o fallo de los procesos críticos de negocio.

(consultar 14.1.3 f)

Posibles Soluciones a este control:

	PD 25111: documento en inglés de BSI que da directrices sobre aspectos de continuidad de negocio relativos a las personas.	PD 25111:2010
	Documento del Business Continuity Institute, en inglés, describiendo las competencias y tareas de los responsables de continuidad de negocio.	BCI-Professional Competence
	Guía Práctica para el Desarrollo de Planes de Contingencia de Sistemas de Información del Gobierno de Perú.	Guía contingencia INEI
	IBM System Storage Business Continuity: Part 1 Planning Guide.	IBM System Storage Business Continuity: Part 1 Planning Guide
	IBM System Storage Business Continuity: Part 2 Solutions Guide.	IBM System Storage Business Continuity: Part 2 Solutions Guide
	Checklist de continuidad de negocio para pequeñas empresas, en inglés.	Business continuity and disaster recovery checklist for small business owners
	Repositorio de artículos sobre gestión de crisis, en inglés, de Continuity Central.	Crisis Management: Advanced resources
	Repositorio de artículos sobre continuidad TI, en inglés, de Continuity Central.	IT Continuity: Advanced resources
Canadian Centre for Emergency Preparedness	Documento en inglés que propone una estructura y tareas para un equipo de gestión de emergencias.	Emergency Management Team Set Up
Canadian Centre for Emergency Preparedness	Plantilla en inglés de estrategia de continuidad para un determinado escenario de impacto.	Strategy Worksheet
Canadian Centre for Emergency Preparedness	Documento en inglés con directrices y ejemplos para la preparación de un plan de comunicación de crisis.	Crisis communication plan
Canadian Centre for Emergency Preparedness	Plantilla en inglés de plan de continuidad de negocio y ejemplo correspondiente.	BCP Template Sample

0 Comments [Show recent to old](#)
[Post a comment](#)

RSS of this page

Author: [aglone](#) Version: [1.5](#) Last Edited By: [javier ruiz](#) Modified: 8 - days ago

Información de contacto

servicios@iso27002.es

Quick Search

- ## Navigate pages | Site Map
- 14 1 Aspectos de la gestión de continuidad del negocio
 - 14.1.1. Proceso de la gestión de continuidad del negocio
 - 14.1.2. Continuidad del negocio y análisis de impactos
 - 14.1.3. Redacción e implantación de planes de continuidad
 - 14.1.4. Marco de planificación para la continuidad del negocio**
 - 14.1.5. Prueba, mantenimiento y reevaluación de planes de continuidad

14.1.4. Marco de planificación para la continuidad del negocio



Control:

Se debería mantener un esquema único de planes de continuidad del negocio para garantizar que dichos planes son consistentes, para tratar los requisitos de seguridad y para identificar las prioridades de prueba y mantenimiento.

Posibles Soluciones a este control:

Espacio pendiente de posibles aportaciones.

0 Comments [Show recent to old](#)
[Post a comment](#)



RSS of this page

Author: [aglone](#) **Version:** [1.1](#) **Last Edited By:** [aglone3](#) **Modified:** 27 - days ago

Información de contacto

servicios@iso27002.es

Quick Search

Navigate pages | Site Map

14 1 Aspectos de la gestión de continuidad del negocio

14.1.1. Proceso de la gestión de continuidad del negocio

14.1.2. Continuidad del negocio y análisis de impactos

14.1.3. Redacción e implantación de planes de continuidad

14.1.4. Marco de planificación para la continuidad del negocio

14.1.5. Prueba, mantenimiento y reevaluación de planes de continuidad


14.1.5. Prueba, mantenimiento y reevaluación de planes de continuidad



Control:

Se deberían probar regularmente los planes de continuidad del negocio para garantizar su actualización y eficacia.

Posibles Soluciones a este control:

Disaster Recovery Journal	Documento en inglés que establece pautas para la realización de "pruebas de escritorio" (o sobre el papel, sin simulacro real) para verificación de planes de continuidad de negocio.	Disaster Recovery Journal
BSI Shop	PD 25666:2010 es una guía en inglés publicada por BSI, que establece buenas prácticas para la realización de pruebas de planes de continuidad de negocio.	PD 25666:2010
	Diversos artículos en inglés de Continuity Central acerca de la prueba de planes de continuidad de negocio.	Continuity Central
SISTESEG	Presentación de la empresa colombiana SISTESEG sobre auditoría de planes de continuidad de negocio y recuperación de desastres (en entorno TI).	Presentación de SISTESEG
Canadian Centre for Emergency Preparedness	Documento en inglés con checklists y consejos para el diseño, gestión y evaluación de pruebas de planes de continuidad de negocio.	EPCB Exercise/Test Methodology
Canadian Centre for Emergency Preparedness	Ejemplo en inglés de plantilla de evaluación del desarrollo de pruebas de planes de continuidad de negocio.	Exercise Evaluation Form

0 Comments [Show recent to old](#)
[Post a comment](#)

 [RSS of this page](#)

Author: [aglone](#) Version: [2.1](#) Last Edited By: [javier_ruiz](#) Modified: 7 - days ago

Información de contacto

servicios@iso27002.es

Quick Search

- Navigate pages | Site Map
- ISO 27002

05. Política de Seguridad

06. Organización de la Seguridad de Información

07. Gestión de Activos

08. Seguridad ligada a los Recursos Humanos

09. Seguridad Física y del Entorno

10. Gestión de Comunicaciones y Operaciones

11. Control de Accesos

12. Adquisición, Desarrollo y Mantenimiento de Sistemas de Información

13. Gestión de Incidentes de Seguridad de la Información

14. Gestión de Continuidad del Negocio

15. Conformidad

15 1 Conformidad con los requisitos legales

15.1.1. Identificación de la legislación aplicable

15.1.2. Derechos de propiedad intelectual (IPR)

15.1.3. Salvaguarda de los registros de la Organización

15.1.4. Protección de datos de carácter personal y de la intimidad de las personas

15.1.5. Evitar mal uso de los dispositivos de tratamiento de la información

15.1.6. Reglamentación de los controles de cifrados

15 2 Revisiones de la política de seguridad y de la conformidad técnica


15 3 Consideraciones sobre la auditoría de sistemas

Objetivos





Contacto

Aviso Legal

15 1 Conformidad con los requisitos legales



Espacio de Patrocinio disponible

 <div>Objetivo</div>	Evitar incumplimientos de cualquier ley, estatuto, regulación u obligación contractual y de cualquier requisito de seguridad.
 <div>Principios</div>	<p>El diseño, operación, uso y gestión de los sistemas de información pueden ser objeto de requisitos estatutarios, reguladores y de seguridad contractuales.</p> <p>Los requisitos legales específicos deberían ser advertidos por los asesores legales de la organización o por profesionales adec uadamente cualificados.</p> <p>Los requisitos que marca la legislación cambian de un país a otro y pueden variar para la información que se genera en un país y se transmite a otro país distinto (por ej., flujos de datos entre fronteras).</p>
	Obtenga asesoramiento legal competente, especialmente si la organización opera o tiene clientes en múltiples jurisdicciones.
	<p>Número de cuestiones o recomendaciones de cumplimiento legal, agrupadas y analizadas por su estado (cerradas, abiertas, nuevas, retrasadas) e importancia o nivel de riesgo (alto, medio o bajo).</p> <p>Porcentaje de requisitos externos clave que, mediante auditorías objetivas o de otra forma admisible, han sido considerados conformes.</p>

0 Comments [Show recent to old](#)
[Post a comment](#)

[Attachments \(2\)](#)

 [RSS of this page](#)

Author: [aglone](#) Version: [1.3](#) Last Edited By: [aglone3](#) Modified: 26 - days ago

Información de contacto

servicios@iso27002.es

Quick Search

- Navigate pages | Site Map
- 15 1 Conformidad con los requisitos legales

15.1.1. Identificación de la legislación aplicable

15.1.2. Derechos de propiedad intelectual (IPR)

15.1.3. Salvaguarda de los registros de la Organización

15.1.4. Protección de datos de carácter personal y de la intimidad de las personas

15.1.5. Evitar mal uso de los dispositivos de tratamiento de la información

15.1.6. Reglamentación de los controles de cifrados

15.1.1. Identificación de la legislación aplicable



Control:

Todos los requisitos estatutarios, de regulación u obligaciones contractuales relevantes, así como las acciones de la Organización para cumplir con estos requisitos, deberían ser explícitamente definidos, documentados y actualizados para cada uno de los sistemas de información y la Organización.

Posibles Soluciones a este control:

<div>integración.JPG</div> <div></div>	Enlace a una lista de leyes internacionales de privacidad por país y región. (inglés)	informationshield
<div></div>	Free Vulnerability Assessment Tools and Checklists. This simple checklist could be used to help every company perform their own assessment for the IT environment and infrastructure. This checklist based on ISO17799/ISO27001 and can be used for PCI DSS, SOX or HIPAA compliances.	controlscada
<div></div>	En este capítulo se hace un breve repaso por el estado de los sistemas legales del mundo, en el marco legal de Europa y en el de España. Se comentan los aspectos legales relacionados con delitos informáticos, y más concretamente, los relacionados con los Sistemas de Detección de Intrusiones.	dgonzalez.net

0 Comments [Show recent to old](#)
[Post a comment](#)

RSS of this page

Author: [aglone](#) Version: [1.1](#) Last Edited By: [aglone3](#) Modified: 27 - days ago

Información de contacto

servicios@iso27002.es

Quick Search

- Navigate pages | Site Map
- 15 1 Conformidad con los requisitos legales

15.1.1. Identificación de la legislación aplicable

15.1.2. Derechos de propiedad intelectual (IPR)

15.1.3. Salvaguarda de los registros de la Organización

15.1.4. Protección de datos de carácter personal y de la intimidad de las personas

15.1.5. Evitar mal uso de los dispositivos de tratamiento de la información

15.1.6. Reglamentación de los controles de cifrados

🌐 Site Home » 15. Conformidad » 15 1 Conformidad con los requisitos legales » 15.1.2. Derechos de propiedad intelectual (IPR)

15.1.2. Derechos de propiedad intelectual (IPR)



Control:

Se deberían implantar procedimientos adecuados que garanticen el cumplimiento de la legislación, regulaciones y requisitos contractuales para el uso de material con posibles derechos de propiedad intelectual asociados y para el uso de productos software propietario.

Posibles Soluciones a este control:

	Modelos para la comunicación y gestión de incidentes contra la propiedad intelectual (inglés)	http://www.sans.org
	Especificaciones para el etiquetado de software con el objeto de optimizar su identificación y gestión. (inglés)	Estándar ISO/IEC 19770-2:2009
	Modificación de la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal.	Ley Orgánica 5/2010, de 22 de junio

0 Comments [Show recent to old](#)
[Post a comment](#)

RSS of this page

Author: [aglone](#) Version: [1.1](#) Last Edited By: [aglone3](#) Modified: 27 - days ago

Información de contacto

servicios@iso27002.es

Quick Search

- Navigate pages | Site Map
- 15 1 Conformidad con los requisitos legales

15.1.1. Identificación de la legislación aplicable

15.1.2. Derechos de propiedad intelectual (IPR)

15.1.3. Salvaguarda de los registros de la Organización

15.1.4. Protección de datos de carácter personal y de la intimidad de las personas

15.1.5. Evitar mal uso de los dispositivos de tratamiento de la información

15.1.6. Reglamentación de los controles de cifrados

Site Home » 15. Conformidad » 15 1 Conformidad con los requisitos legales » 15.1.3. Salvaguarda de los registros de la Organización

15.1.3. Salvaguarda de los registros de la Organización



Control:

Los registros importantes se deberían proteger de la pérdida, destrucción y falsificación, de acuerdo a los requisitos estatutarios, regulaciones, contractuales y de negocio.

(consultar 12.3)

Posibles Soluciones a este control:

Espacio pendiente de posibles aportaciones.

0 Comments Show recent to old
Post a comment

RSS of this page

Author: aglone Version: 1.1 Last Edited By: aglone3 Modified: 27 - days ago

Información de contacto

servicios@iso27002.es

Quick Search

Navigate pages | Site Map

15 1 Conformidad con los requisitos legales

15.1.1. Identificación de la legislación aplicable

15.1.2. Derechos de propiedad intelectual (IPR)

15.1.3. Salvaguarda de los registros de la Organización

15.1.4. Protección de datos de carácter personal y de la intimidad de las personas

15.1.5. Evitar mal uso de los dispositivos de tratamiento de la información

15.1.6. Reglamentación de los controles de cifrados

Site Home » 15. Conformidad » 15 1 Conformidad con los requisitos legales » 15.1.4. Protección de datos de carácter personal y de la intimidad de las personas

15.1.4. Protección de datos de carácter personal y de la intimidad de las personas



Control:

Se debería garantizar la protección y privacidad de los datos y según requiera la legislación, regulaciones y, si fueran aplicables, las cláusulas relevantes contractuales.

Posibles Soluciones a este control:

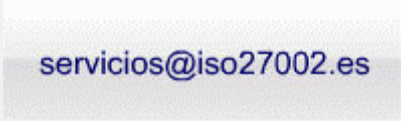
	Herramienta de diagnóstico basado en un autotest basado en preguntas con respuesta múltiple. Al final, la Agencia Española de Protección de Datos, le facilita un informe con indicaciones y recursos que le orienten, en su caso, para cumplir con lo dispuesto en la LOPD.	Agencia Española de Protección de Datos
--	--	---

0 Comments [Show recent to old](#)
[Post a comment](#)

RSS of this page

Author: [aglone](#) Version: [1.1](#) Last Edited By: [aglone3](#) Modified: 27 - days ago

Información de contacto



Quick Search

- Navigate pages | Site Map
- 15 1 Conformidad con los requisitos legales

15.1.1. Identificación de la legislación aplicable

15.1.2. Derechos de propiedad intelectual (IPR)

15.1.3. Salvaguarda de los registros de la Organización

15.1.5. Evitar mal uso de los dispositivos de tratamiento de la información

15.1.6. Reglamentación de los controles de cifrados

 [Site Home](#) » [15. Conformidad](#) » [15 1 Conformidad con los requisitos legales](#) » 15.1.5. Evitar mal uso de los dispositivos de tratamiento de la información

15.1.5. Evitar mal uso de los dispositivos de tratamiento de la información



Control:

Se debería disuadir a los usuarios del uso de los recursos dedicados al tratamiento de la información para propósitos no autorizados.

([consultar 6.1.4](#))

([consultar 11.5.1](#))

Posibles Soluciones a este control:

Espacio pendiente de posibles aportaciones.

0 Comments [Show recent to old](#)
[Post a comment](#)

 [RSS of this page](#)

Author: [aglone](#) Version: [1.1](#) Last Edited By: [aglone3](#) Modified: 27 - days ago

Información de contacto

servicios@iso27002.es

Quick Search

- Navigate pages | Site Map
- 15 1 Conformidad con los requisitos legales

15.1.1. Identificación de la legislación aplicable

15.1.2. Derechos de propiedad intelectual (IPR)

15.1.3. Salvaguarda de los registros de la Organización

15.1.4. Protección de datos de carácter personal y de la intimidad de las personas

15.1.5. Evitar mal uso de los dispositivos de tratamiento de la información

15.1.6. Reglamentación de los controles de cifrados

15.1.6. Reglamentación de los controles de cifrados



Control:

Se deberían utilizar controles cifrados en conformidad con todos acuerdos, leyes y regulaciones pertinentes.

Posibles Soluciones a este control:

	La situación legal de los programas criptológicos varía según los países, y las leyes que rigen el uso y comercio de estos programas evolucionan con rapidez. Wikitel es un proyecto promovido por la Comisión del Mercado de las Telecomunicaciones (CMT).	Wikitel
--	---	-------------------------

0 Comments [Show recent to old](#)
[Post a comment](#)

RSS of this page

Author: [aglone](#) Version: [1.1](#) Last Edited By: [aglone3](#) Modified: 27 - days ago

Información de contacto

servicios@iso27002.es

Quick Search

- Navigate pages | Site Map
- ISO 27002

05. Política de Seguridad

06. Organización de la Seguridad de Información

07. Gestión de Activos

08. Seguridad ligada a los Recursos Humanos

09. Seguridad Física y del Entorno

10. Gestión de Comunicaciones y Operaciones

11. Control de Accesos

12. Adquisición, Desarrollo y Mantenimiento de Sistemas de Información

13. Gestión de Incidentes de Seguridad de la Información

14. Gestión de Continuidad del Negocio

15. Conformidad

15 1 Conformidad con los requisitos legales

15 2 Revisiones de la política de seguridad y de la conformidad técnica

15 3 Consideraciones sobre la auditoría de sistemas





Objetivos

Contacto

Aviso Legal

15 2 Revisiones de la política de seguridad y de la conformidad técnica



	Garantizar la conformidad de los sistemas con las políticas y estándares de seguridad de la Organización.
	Se deberían realizar revisiones regulares de la seguridad de los sistemas de información. Las revisiones se deberían realizar según las políticas de seguridad apropiadas y las plataformas técnicas y sistemas de información deberían ser auditados para el cumplimiento de los estándares adecuados de implantación de la seguridad y controles de seguridad documentados.
	Alinee los procesos de auto-evaluación de controles de seguridad con las auto-evaluaciones de gobierno corporativo, cumplimiento legal y regulador, etc., complementados por revisiones de la dirección y verificaciones externas de buen funcionamiento.
	Número de cuestiones o recomendaciones de política interna y otros aspectos de cumplimiento, agrupadas y analizadas por su estado (cerradas, abiertas, nuevas, retrasadas) e importancia o nivel de riesgo (alto, medio o bajo). Porcentaje de revisiones de cumplimiento de seguridad de la información sin incumplimientos sustanciales.

0 Comments [Show recent to old](#)
[Post a comment](#)

[Attachments \(2\)](#)

 [RSS of this page](#)

Author: [aglone](#) Version: [1.3](#) Last Edited By: [aglone3](#) Modified: 26 - days ago

Información de contacto

servicios@iso27002.es

Quick Search

Navigate pages | Site Map

15 2 Revisiones de la política de seguridad y de la conformidad técnica

- 15.2.1. Conformidad con la política de seguridad
- 15.2.2. Comprobación de la conformidad técnica

Site Home » 15. Conformidad » 15 2 Revisiones de la política de seguridad y de la conformidad técnica » 15.2.1. Conformidad con la política de seguridad

15.2.1. Conformidad con la política de seguridad



Control:

Los directivos se deberían asegurar que todos los procedimientos de seguridad dentro de su área de responsabilidad se realizan correctamente y cumplen con los estándares y políticas de seguridad.

(consultar 6.1.8)

Posibles Soluciones a este control:

Espacio pendiente de posibles aportaciones.

0 Comments Show recent to old
Post a comment

RSS of this page

Author: aglone Version: 1.1 Last Edited By: aglone3 Modified: 27 - days ago

Información de contacto

servicios@iso27002.es

Quick Search

Navigate pages | [Site Map](#)

15 2 Revisiones de la política de seguridad y de la conformidad técnica

15.2.1. Conformidad con la política de seguridad

15.2.2. Comprobación de la conformidad técnica

 [Site Home](#) » [15. Conformidad](#) » [15 2 Revisiones de la política de seguridad y de la conformidad técnica](#) » 15.2.2. Comprobación de la conformidad técnica


15.2.2. Comprobación de la conformidad técnica



Control:

Se debería comprobar regularmente la conformidad de los sistemas de información con los estándares de implantación de la seguridad.

Posibles Soluciones a este control:

 the CENTER for INTERNET SECURITY	CIS offers a variety of audit tools for assessing compliance with CIS Benchmarks.	CIS Benchmarks
--	---	--------------------------------

0 Comments [Show recent to old](#)
[Post a comment](#)

 [RSS of this page](#)

Author: [aglone](#) Version: [1.1](#) Last Edited By: [aglone3](#) Modified: 27 - days ago

Información de contacto

servicios@iso27002.es

Quick Search

- Navigate pages | Site Map
- ISO 27002

05. Política de Seguridad

06. Organización de la Seguridad de Información

07. Gestión de Activos

08. Seguridad ligada a los Recursos Humanos

09. Seguridad Física y del Entorno

10. Gestión de Comunicaciones y Operaciones

11. Control de Accesos

12. Adquisición, Desarrollo y Mantenimiento de Sistemas de Información

13. Gestión de Incidentes de Seguridad de la Información

14. Gestión de Continuidad del Negocio

15. Conformidad

15 1 Conformidad con los requisitos legales

15 2 Revisiones de la política de seguridad y de la conformidad técnica






15 3 Consideraciones sobre la auditoría de sistemas

15.3.1. Controles de auditoria de sistemas


15.3.2. Protección de las herramientas de auditoria de sistemas

Objetivos

Contacto

Aviso Legal
- Site Home » 15. Conformidad » 15 3 Consideraciones sobre la auditoría de sistemas
- ## 15 3 Consideraciones sobre la auditoría de sistemas
- | | |
|---|---|
|  | Espacio de Patrocinio disponible |
|  | Maximizar la efectividad del proceso de auditoría de los sistemas de información y minimizar las intromisiones a/desde éste proceso. |
|  | <p>Deberían existir controles para proteger los sistemas en activo y las herramientas de auditoría durante el desarrollo de las auditorías de los sistemas de información.</p> <p>También se requiere la protección para salvaguardar la integridad y prevenir el mal uso de las herramientas de auditoría.</p> |
|  | <p>Invierta en auditoría TI cualificada que utilice ISO 27001, COBIT, ITIL, CMM y estándares y métodos de buenas prácticas similares como referencias de comparación.</p> <p>Examine ISO 19011 "Directrices para la auditoría de los sistemas de gestión de la calidad y/o ambiental" como fuente valiosa para la realización de auditorías internas del SGSI.</p> <p>ISO 19011 proporciona un marco excelente para crear un programa de auditorías internas y contiene asimismo las cualificaciones del equipo de auditoría interna.</p> |
|  | <p>Número de cuestiones o recomendaciones de auditoría, agrupadas y analizadas por su estado (cerradas, abiertas, nuevas, retrasadas) e importancia o nivel de riesgo (alto, medio o bajo).</p> <p>Porcentaje de hallazgos de auditoría relativos a seguridad de la información que han sido resueltos y cerrados, respecto al total de abiertos en el mismo periodo. Tiempo medio real de resolución/cierre de recomendaciones, respecto a los plazos acordados por la dirección al final de las auditorías.</p> |
- 0 Comments

Show recent to old

Post a comment
- Attachments (2)
- 

RSS of this page
- Author: [aglone](#)

Version: [1.4](#)

Last Edited By: [aglone3](#)

Modified: 26 - days ago
- ### Información de contacto
- servicios@iso27002.es
- Powered by [Zoho Wiki](#) | [Zoho](#) | [Report Abuse](#) | [Wiki Index](#) | [Site Map](#) | [Help](#) | [Feedback](#) | [Jump Start with 2 Free Wikis](#) | [Sign in](#)
- http://iso27002.wiki.zoho.com/15-3-Consideraciones-sobre-la-auditoría-de-sistemas.html[28/01/2011 08:42:54 p.m.]

Quick Search

Navigate pages | Site Map

15 3 Consideraciones sobre la auditoría de sistemas

15.3.1. Controles de auditoria de sistemas

15.3.2. Protección de las herramientas de auditoria de sistemas

Site Home » 15. Conformidad » 15 3 Consideraciones sobre la auditoría de sistemas » 15.3.1. Controles de auditoria de sistemas

15.3.1. Controles de auditoria de sistemas



Espacio de Patrocinio disponible

Control:

Se deberían planificar y acordar cuidadosamente los requisitos y actividades de auditoría que impliquen comprobaciones en los sistemas en activo con objeto de minimizar el riesgo de interrupciones de los procesos de negocio.

Posibles Soluciones a este control:

Espacio pendiente de posibles aportaciones.

0 Comments Show recent to old

Post a comment



RSS of this page

Author: [aglone](#) Version: [1.1](#) Last Edited By: [aglone3](#) Modified: 27 - days ago

Información de contacto

servicios@iso27002.es

Powered by [Zoho Wiki](#) | [Zoho](#) | [Report Abuse](#) | [Wiki Index](#) | [Site Map](#) | [Help](#) | [Feedback](#) | [Jump Start with 2 Free Wikis](#) | [Sign in](#)

http://iso27002.wiki.zoho.com/15-3-1-Controles-de-auditoria-de-sistemas.html[28/01/2011 08:43:05 p.m.]

Quick Search

Navigate pages | Site Map

15 3 Consideraciones sobre la auditoría de sistemas

15.3.1. Controles de auditoria de sistemas

15.3.2. Protección de las herramientas de auditoria de sistemas

Site Home » 15. Conformidad » 15 3 Consideraciones sobre la auditoría de sistemas » 15.3.2. Protección de las herramientas de auditoria de sistemas

15.3.2. Protección de las herramientas de auditoria de sistemas



Control:

Se deberían proteger los accesos a las herramientas de auditoría de los sistemas de información con objeto de prevenir cualquier posible mal uso o compromiso.

Posibles Soluciones a este control:

	This is a VA / PT report for a fictitious bank called eClipse Bank PLC carried out by another fictitious company Cynergi Solutions Inc. All names, URLs, IPs, etc are fictitious	Vulnerability Assessment & Penetration Test Report template
	Open Source Security Information Management: Colección de herramientas bajo la licencia BSD, diseñadas para ayudar a los administradores de red en la seguridad de las computadoras, detección de intrusos y prevención.	OSSIM
	Collection of tools for network auditing and penetration testing. dsniff, filesnarf, mailsnarf, msgsnarf, urlsnarf, and webspY passively monitor a network for interesting data (passwords, e-mail, files, etc.). arpspoof, dnsspoof, and macof facilitate the interception of network traffic normally unavailable to an attacker (e.g, due to layer-2 switching). sshmitm and webmitm implement active monkey-in-the-middle attacks against redirected SSH and HTTPS sessions by exploiting weak bindings in ad-hoc PKI.	Dsniff
	Password auditing and recovery. 15 days trial.	lOphTcrack
	BackTrack is intended for all audiences from the most savvy security professionals to early newcomers to the information security field. BackTrack promotes a quick and easy way to find and update the largest database of security tool collection to-date.	BackTrack
	Fully featured security distribution consisting of a bunch of powerful, open source and free tools that can be used for various purposes including, but not limited to, penetration testing, ethical hacking, system and network administration, cyber forensics investigations, security testing, vulnerability analysis, and much more.	Matriux
	The SANS SIFT Workstation is a VMware Appliance that is pre-configured with all the necessary tools to perform a detailed digital forensic examination. It is compatible with Expert Witness Format (E01), Advanced Forensic Format (AFF), and raw (dd) evidence formats. The brand new version has been completely rebuilt on an Ubuntu base with many additional tools and capabilities that can match any modern forensic tool suite.	SANS
	IDA Pro is a Windows or Linux hosted multi-processor disassembler and debugger that offers so many features it is hard to describe them all.	IDA Pro

0 Comments [Show recent to old](#)
[Post a comment](#)

RSS of this page

Author: [aglone](#) Version: [1.1](#) Last Edited By: [aglone3](#) Modified: 27 - days ago

Información de contacto

servicios@iso27002.es

Quick Search

- Navigate pages | [Site Map](#)
- **ISO 27002**

⊞ 05. PolÃ­tica de Seguridad

⊞ 06. Organizaci3n de la Seguridad de Informaci3n

⊞ 07. gesti3n de Activos

⊞ 08. Seguridad ligada a los Recursos Humanos

⊞ 09. Seguridad FÃ­sica y del Entorno

⊞ 10. gesti3n de Comunicaciones y Operaciones

⊞ 11. Control de Accesos

⊞ 12. Adquisici3n, Desarrollo y Mantenimiento de Sistemas de Informaci3n

⊞ 13. gesti3n de Incidentes de Seguridad de la Informaci3n

⊞ 14. gesti3n de Continuidad del Negocio

⊞ 15. Conformidad

• [Objetivos](#)

• [Contacto](#)

• [Aviso Legal](#)

 [Site Home](#) >> 10 9 3 Seguridad en informaci3n pÃ³blica

You do not have permission to create page in this wiki.

Informaci3n de contacto

servicios@iso27002.es

Quick Search

- Navigate pages | [Site Map](#)
- **ISO 27002**

⊞ 05. Poltica de Seguridad

⊞ 06. Organizaci3n de la Seguridad de Informaci3n

⊞ 07. Gest3n de Activos

⊞ 08. Seguridad ligada a los Recursos Humanos

⊞ 09. Seguridad F3sica y del Entorno

⊞ 10. Gest3n de Comunicaciones y Operaciones

⊞ 11. Control de Accesos

⊞ 12. Adquisici3n, Desarrollo y Mantenimiento de Sistemas de Informaci3n


⊞ 13. Gest3n de Incidentes de Seguridad de la Informaci3n

⊞ 14. Gest3n de Continuidad del Negocio

⊞ 15. Conformidad

• [Objetivos](#)

• [Contacto](#)

• [Aviso Legal](#)
-  [Site Home](#)

>> 10 10 6 Sincronizaci3n del reloj
- You do not have permission to create page in this wiki.
- Informaci3n de contacto
- servicios@iso27002.es
- Powered by [Zoho Wiki](#) | [Zoho](#) | [Report Abuse](#) | [Wiki Index](#) | [Site Map](#) | [Help](#) | [Feedback](#) | [Jump Start with 2 Free Wikis](#) | [Sign in](#)
- http://iso27002.wiki.zoho.com/10-10-6-Sincronizaci3n-del-reloj.html[28/01/2011 08:43:38 p.m.]

Quick Search

- Navigate pages | Site Map
- ISO 27002

05. Política de Seguridad

06. Organización de la Seguridad de Información

07. Gestión de Activos

08. Seguridad ligada a los Recursos Humanos

09. Seguridad Física y del Entorno

10. Gestión de Comunicaciones y Operaciones

11. Control de Accesos

12. Adquisición, Desarrollo y Mantenimiento de Sistemas de Información

13. Gestión de Incidentes de Seguridad de la Información

14. Gestión de Continuidad del Negocio

15. Conformidad

Objetivos

Contacto

Aviso Legal

Wiki Index

Show: [All](#) | [A](#) | [B](#) | [C](#) | [D](#) | [E](#) | [F](#) | [G](#) | [H](#) | [I](#) | [J](#) | [K](#) | [L](#) | [M](#) | [N](#) | [O](#) | [P](#) | [Q](#) | [R](#) | [S](#) | [T](#) | [U](#) | [V](#) | [W](#) | [X](#) | [Y](#) | [Z](#)

► [Aviso Legal](#)

Información de contacto

servicios@iso27002.es

Quick Search

- Navigate pages | Site Map
- ISO 27002

05. Política de Seguridad

06. Organización de la Seguridad de Información

07. Gestión de Activos

08. Seguridad ligada a los Recursos Humanos

09. Seguridad Física y del Entorno

10. Gestión de Comunicaciones y Operaciones

11. Control de Accesos

12. Adquisición, Desarrollo y Mantenimiento de Sistemas de Información

13. Gestión de Incidentes de Seguridad de la Información

14. Gestión de Continuidad del Negocio

15. Conformidad

Objetivos

Contacto

Aviso Legal

Wiki Index

Show: [All](#) | [A](#) | [B](#) | [C](#) | [D](#) | [E](#) | [F](#) | [G](#) | [H](#) | [I](#) | [J](#) | [K](#) | [L](#) | [M](#) | [N](#) | [O](#) | [P](#) | [Q](#) | [R](#) | [S](#) | [T](#) | [U](#) | [V](#) | [W](#) | [X](#) | [Y](#) | [Z](#)

► [Contacto](#)

Información de contacto

servicios@iso27002.es

Quick Search

- Navigate pages | Site Map
- ISO 27002

05. Política de Seguridad

06. Organización de la Seguridad de Información

07. Gestión de Activos

08. Seguridad ligada a los Recursos Humanos

09. Seguridad Física y del Entorno

10. Gestión de Comunicaciones y Operaciones

11. Control de Accesos

12. Adquisición, Desarrollo y Mantenimiento de Sistemas de Información

13. Gestión de Incidentes de Seguridad de la Información

14. Gestión de Continuidad del Negocio

15. Conformidad

Objetivos

Contacto

Aviso Legal

Wiki Index

Show: [All](#) | [A](#) | B | [C](#) | D | E | F | G | H | I | J | K | L | M | N | [O](#) | P | Q | R | S | T | U | V | W | X | Y | Z

► [ISO 27002](#)

Información de contacto

servicios@iso27002.es

Quick Search

- Navigate pages | Site Map
- ISO 27002

05. Política de Seguridad

06. Organización de la Seguridad de Información

07. Gestión de Activos

08. Seguridad ligada a los Recursos Humanos

09. Seguridad Física y del Entorno

10. Gestión de Comunicaciones y Operaciones

11. Control de Accesos

12. Adquisición, Desarrollo y Mantenimiento de Sistemas de Información

13. Gestión de Incidentes de Seguridad de la Información

14. Gestión de Continuidad del Negocio

15. Conformidad

Objetivos

Contacto

Aviso Legal

Wiki Index

Show: [All](#) | [A](#) | [B](#) | [C](#) | [D](#) | [E](#) | [F](#) | [G](#) | [H](#) | [I](#) | [J](#) | [K](#) | [L](#) | [M](#) | [N](#) | **O** | [P](#) | [Q](#) | [R](#) | [S](#) | [T](#) | [U](#) | [V](#) | [W](#) | [X](#) | [Y](#) | [Z](#)

► [Objetivos](#)

Información de contacto

servicios@iso27002.es

Quick Search

- Navigate pages | [Site Map](#)
- ISO 27002

⊞ 05. Pol3tica de Seguridad

⊞ 06. Organizaci3n de la Seguridad de Informaci3n

⊞ 07. gesti3n de Activos

⊞ 08. Seguridad ligada a los Recursos Humanos

⊞ 09. Seguridad F3sica y del Entorno

⊞ 10. gesti3n de Comunicaciones y Operaciones

⊞ 11. Control de Accesos

⊞ 12. Adquisici3n, Desarrollo y Mantenimiento de Sistemas de Informaci3n

⊞ 13. gesti3n de Incidentes de Seguridad de la Informaci3n

⊞ 14. gesti3n de Continuidad del Negocio

⊞ 15. Conformidad

• [Objetivos](#)

• [Contacto](#)

• [Aviso Legal](#)

 [Site Home](#) >> 15 1 1 Identificaci3n de la legislaci3n aplicable

You do not have permission to create page in this wiki.

Informaci3n de contacto

servicios@iso27002.es

Quick Search

Navigate pages | Site Map

ISO 27002

05. Política de Seguridad

06. Organización de la Seguridad de Información

07. Gestión de Activos

08. Seguridad ligada a los Recursos Humanos

09. Seguridad Física y del Entorno

10. Gestión de Comunicaciones y Operaciones

11. Control de Accesos

12. Adquisición, Desarrollo y Mantenimiento de Sistemas de Información

13. Gestión de Incidentes de Seguridad de la Información

14. Gestión de Continuidad del Negocio

15. Conformidad

Objetivos

Contacto

Aviso Legal

Wiki Index

Show: **All** | [A](#) | [B](#) | [C](#) | [D](#) | [E](#) | [F](#) | [G](#) | [H](#) | [I](#) | [J](#) | [K](#) | [L](#) | [M](#) | [N](#) | [O](#) | [P](#) | [Q](#) | [R](#) | [S](#) | [T](#) | [U](#) | [V](#) | [W](#) | [X](#) | [Y](#) | [Z](#)

- [05. Política de Seguridad](#)

► [08. Seguridad ligada a los Recursos Humanos](#)

► [10.1.2. Control de cambios operacionales](#)

► [10 1 Procedimientos y responsabilidades de operación](#)

► [10. 10. 3. Protección de los registros de incidencias](#)

► [10. 10. 6. Sincronización del reloj](#)

► [10.2.2. Monitorización y revisión de los servicios contratados](#)

► [10. 3. 1. Planificación de capacidades](#)

► [10. 4. 1. Medidas y controles contra software malicioso](#)

► [10. 5. 1. Recuperación de la información](#)

► [10. 6. 2. Seguridad en los servicios de red](#)

► [10. 7. 2. Eliminación de soportes](#)

► [10 7 Utilización y seguridad de los soportes de información](#)

► [10. 8. 3. Soportes físicos en tránsito](#)

► [10 8 Intercambio de información y software](#)

► [10 9 3 Seguridad en información pública](#)

► [11.1.1. Política de control de accesos](#)

► [11.2.2. Gestión de privilegios](#)

► [11 2 Gestión de acceso de usuario](#)

► [11.3.3. Políticas para escritorios y monitores sin información](#)

► [11.4.2. Autenticación de usuario para conexiones externas](#)

► [11.4.5. Segregación en las redes](#)

► [11 4 Control de acceso en red](#)

► [11.5.3. Sistema de gestión de contraseñas](#)

► [11.5.6. Limitación del tiempo de conexión](#)

► [11 6 2 Aislamiento de sistemas sensibles](#)

► [11.7.2. Tele trabajo](#)

► [12.1.1. Análisis y especificación de los requisitos de seguridad](#)

► [12.2.2. Control del proceso interno](#)

► [12 2 Seguridad de las aplicaciones del sistema](#)

► [12 3 Controles criptográficos](#)

► [12.4.3. Control de acceso a la librería de programas fuente](#)

► [12.5.2. Revisión técnica de los cambios en el sistema operativo](#)

► [12.5.5. Desarrollo externalizado del software](#)

► [12 6 Gestión de las vulnerabilidades técnicas](#)

► [13.1.2. Comunicación de debilidades en seguridad](#)

► [13.2.2. Evaluación de incidentes en seguridad](#)

► [13. Gestión de Incidentes de Seguridad de la Información](#)

► [14.1.3. Redacción e implantación de planes de continuidad](#)

► [14 1 Aspectos de la gestión de continuidad del negocio](#)

► [15.1.2. Derechos de propiedad intelectual \(IPR\)](#)

► [15.1.5. Evitar mal uso de los dispositivos de tratamiento de la información](#)

► [15.2.1. Conformidad con la política de seguridad](#)

► [06. Organización de la Seguridad de Información](#)

► [09. Seguridad Física y del Entorno](#)

► [10.1.3. Segregación de tareas](#)

► [10. 10. 1. Registro de incidencias](#)

► [10. 10. 4. Diarios de operación del administrador y operador](#)

► [10 10 Monitorización](#)

► [10.2.3. Gestión de los cambios en los servicios contratados](#)

► [10. 3. 2. Aceptación del sistema](#)

► [10. 4. 2. Medidas y controles contra código móvil](#)

► [10 5 Gestión interna de soportes y recuperación](#)

► [10 6 Gestión de redes](#)

► [10. 7. 3. Procedimientos de utilización de la información](#)

► [10. 8. 1. Políticas y procedimientos de intercambio de información](#)

► [10. 8. 4. Mensajería electrónica](#)

► [10. 9. 1. Seguridad en comercio electrónico](#)

► [10 9 Servicios de comercio electrónico](#)

► [11 1 Requerimientos de negocio para el control de accesos](#)

► [11.2.3. Gestión de contraseñas de usuario](#)

► [11.3.1. Uso de contraseña](#)

► [11 3 Responsabilidades del usuario](#)

► [11.4.3. Autenticación de nodos de la red](#)

► [11.4.6. Control de conexión a las redes](#)

► [11.5.1. Procedimientos de conexión de terminales](#)

► [11.5.4. Uso de los servicios del sistema](#)

► [11 5 Control de acceso al sistema operativo](#)

► [11 6 Control de acceso a las aplicaciones](#)

► [11 7 Informática móvil y tele trabajo](#)

► [12 1 Requisitos de seguridad de los sistemas](#)

► [12.2.3. Autenticación de mensajes](#)

► [12.3.1. Política de uso de los controles criptográficos](#)

► [12.4.1. Control del software en explotación](#)

► [12 4 Seguridad de los ficheros del sistema](#)

► [12.5.3. Restricciones en los cambios a los paquetes de software](#)

► [12 5 Seguridad en los procesos de desarrollo y soporte](#)

► [12. Adquisición, Desarrollo y Mantenimiento de Sistemas de Información](#)

► [13 1 Comunicación de eventos y debilidades en la seguridad de la información](#)

► [13.2.3. Recogida de pruebas](#)

► [14.1.1. Proceso de la gestión de continuidad del negocio](#)

► [14.1.4. Marco de planificación para la continuidad del negocio](#)

► [14. Gestión de Continuidad del Negocio](#)

► [15.1.3. Salvaguarda de los registros de la Organización](#)

► [15.1.6. Reglamentación de los controles de cifrados](#)

► [15.2.2. Comprobación de la conformidad técnica](#)

► [07. Gestión de Activos](#)

► [10.1.1. Documentación de procedimientos operativos](#)

► [10.1.4. Separación de los recursos para desarrollo y producción](#)

► [10. 10. 2. Supervisión del uso de los sistemas](#)

► [10. 10. 5. Registro de fallos](#)

► [10.2.1. Prestación de servicios](#)

► [10 2 Supervisión de los servicios contratados a terceros](#)

► [10 3 Planificación y aceptación del sistema](#)

► [10 4 Protección contra software malicioso y código móvil](#)

► [10. 6. 1. Controles de red](#)

► [10. 7. 1. Gestión de soportes extraíbles](#)

► [10. 7. 4. Seguridad de la documentación de sistemas](#)

► [10. 8. 2. Acuerdos de intercambio](#)

► [10. 8. 5. Sistemas de información empresariales](#)

► [10. 9. 2. Seguridad en transacciones en línea](#)

► [10. Gestión de Comunicaciones y Operaciones](#)

► [11.2.1. Registro de usuario](#)

► [11.2.4. Revisión de los derechos de acceso de los usuarios](#)

► [11.3.2. Equipo informático de usuario desatendido](#)

► [11.4.1. Política de uso de los servicios de red](#)

► [11.4.4. Protección a puertos de diagnóstico remoto](#)

► [11.4.7. Control de encaminamiento en la red](#)

► [11.5.2. Identificación y autenticación de usuario](#)

► [11.5.5. Desconexión automática de terminales](#)

► [11.6.1. Restricción de acceso a la información](#)

► [11 7 1 Informática móvil](#)

► [11. Control de Accesos](#)

► [12.2.1. Validación de los datos de entrada](#)

► [12.2.4. Validación de los datos de salida](#)

► [12.3.2. Cifrado](#)

► [12.4.2. Protección de los datos de prueba del sistema](#)

► [12.5.1. Procedimientos de control de cambios](#)

► [12.5.4. Canales encubiertos y código Troyano](#)

► [12.6.1. Control de las vulnerabilidades técnicas](#)

► [13 1 1 Comunicación de eventos en seguridad](#)

► [13.2.1. Identificación de responsabilidades y procedimientos](#)

► [13 2 Gestión de incidentes y mejoras en la seguridad de la información](#)

► [14.1.2. Continuidad del negocio y análisis de impactos](#)

► [14.1.5. Prueba, mantenimiento y reevaluación de planes de continuidad](#)

► [15.1.1. Identificación de la legislación aplicable](#)

► [15.1.4. Protección de datos de carácter personal y de la intimidad de las personas](#)

► [15 1 Conformidad con los requisitos legales](#)

► [15 2 Revisiones de la política de seguridad y de la conformidad técnica](#)

- ▶ [15.3.1. Controles de auditoria de sistemas](#)
- ▶ [15.3.2. Protección de las herramientas de auditoria de sistemas](#)
- ▶ [15 3 Consideraciones sobre la auditoría de sistemas](#)
- ▶ [15. Conformidad](#)
- ▶ [5.1.1 Documento de política de seguridad de la información](#)
- ▶ [5.1.2 Revisión de la política de seguridad de la información](#)
- ▶ [5 1 Política de seguridad de la información](#)
- ▶ [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](#)
- ▶ [6.1.4. Proceso de Autorización de Recursos para el Tratamiento de la Información](#)
- ▶ [6.1.5. Acuerdos de Confidencialidad](#)
- ▶ [6.1.6. Contacto con las Autoridades](#)
- ▶ [6.1.7. Contacto con Grupos de Interés Especial](#)
- ▶ [6.1.8. Revisión Independiente de la Seguridad de la Información](#)
- ▶ [6 1 Organización Interna](#)
- ▶ [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](#)
- ▶ [6 2 Terceros](#)
- ▶ [7.1.2. Responsable de los activos](#)
- ▶ [7 1 3 Acuerdos sobre el uso adecuado de los activos](#)
- ▶ [7.1.1. Inventario de Activos](#)
- ▶ [7.2.1 Directrices de Clasificación](#)
- ▶ [7 2 Clasificación de la Información](#)
- ▶ [8.1.1. Inclusión de la seguridad en las responsabilidades laborales](#)
- ▶ [8.1.2. Selección y política de personal](#)
- ▶ [8.1.3. Términos y condiciones de la relación laboral](#)
- ▶ [8 1 Seguridad en la definición del trabajo y los recursos](#)
- ▶ [8.2.1. Supervisión de las obligaciones](#)
- ▶ [8.2.2. Formación y capacitación en seguridad de la información](#)
- ▶ [8.2.3. Procedimiento disciplinario](#)
- ▶ [8 2 Seguridad en el desempeño de las funciones del empleo](#)
- ▶ [8.3.1. Cese de responsabilidades](#)
- ▶ [8.3.2. Restitución de activos](#)
- ▶ [8.3.3. Cancelación de permisos de acceso](#)
- ▶ [8 3 Finalización o cambio del puesto de trabajo](#)
- ▶ [9.1.1. Perímetro de seguridad física](#)
- ▶ [9.1.2. Controles físicos de entrada](#)
- ▶ [9.1.3. Seguridad de oficinas, despachos y recursos](#)
- ▶ [9.1.4. Protección contra amenazas externas y del entorno](#)
- ▶ [9.1.5. El trabajo en áreas seguras](#)
- ▶ [9.1.6. Áreas aisladas de carga y descarga](#)
- ▶ [9 1 Áreas seguras](#)
- ▶ [9.2.1. Instalación y protección de equipos](#)
- ▶ [9.2.2. Suministro eléctrico](#)
- ▶ [9 2 5 Seguridad de equipos fuera de los locales de la Organización](#)
- ▶ [9.2.3. Seguridad del cableado](#)
- ▶ [9.2.4. Mantenimiento de equipos](#)
- ▶ [9 2 Seguridad de los equipos](#)
- ▶ [9.2.6. Seguridad en la reutilización o eliminación de equipos](#)
- ▶ [9.2.7. Traslado de activos](#)
- ▶ [Aviso Legal](#)
- ▶ [Contacto](#)
- ▶ [ISO 27002](#)
- ▶ [Objetivos](#)

Información de contacto

servicios@iso27002.es