Seguridad de la información: Novedades en la norma ISO 27001:2013

Introducción

Desde la publicación inicial de norma internacional ISO/IEC 27001 en el año 2005 el número de implantaciones de los Sistemas para la Gestión de la Seguridad de la Información (SGSI) solo ha hecho que aumentar.

Si bien la publicación de la norma en el 2005 ya advertía en su Anexo B, en línea con las considera- ciones de la OCDE, acerca de la criticidad de la seguridad de la información para el desarrollo del tejido empresarial , los incrementos en los casos detectados y denunciados en los medios públicos de espionaje industrial, paralización de los sistemas informáticos y telemáticos, espionaje masivo a ciudadanos, estafas online, diversos sistemas y plataformas de pago, centros de datos con y sin servicios “cloud” e infraestructuras críticas de todo tipo, únicamente sirven para confirmar que la separación clásica entre la vida real y la denominada “virtual” es ya inexistente, con influencia directa la una en la otra y en un mundo que podemos considerar ya plenamente globalizado.

El siguiente resumen que EQA pone a su disposición sobre la revisión del estándar ISO/IEC 27001:2013 pretende comunicar de modo ágil, directo y sencillo los principales requisitos y modi- ficaciones establecidos en la nueva publicación.

Documentos adicionales más detallados sobre los cambios establecidos en cada cláusula, junto con la relación entre versiones que faciliten las labores de adaptación, están a disposición de todas las organizaciones actualmente certificadas por EQA, además de a todas aquellos interesados en la labor que EQA viene prestando en materia de seguridad de la información desde hace años y las que nos ponemos a su disposición.

ISO /IEC 27001: Gestión de la seguridad

El propósito original en la publicación del año 2005 de lazs normas ISO/IEC 27001 e ISO/IEC 27002 se mantiene y refuerza en la última revisión conjunta aprobada finalmente en 2013, incidiendo en aspectos relacionados con la reducción del riesgo y la atención, en las medidas que se decidan implantar, a una relación lógica de coste/beneficio con una mayor flexibilidad en el modo en que se analizan y gestionan estos aspectos por cada organización.

Aunque para las organizaciones con SGSI implantados no se introduzcan cambios significativos que exijan esfuerzos o especial dedicación en la transición a la versión 2013, los cambios van especialmente orientados a flexibilizar el modo en que cada organización puede cumplir con los requisitos formales del estándar ISO/IEC 27001:2013, lo que debería traducirse en una mayor libertad y facilidad de adaptación de las actividades relacionas con el estándar a las actividades propias de negocio.

Todas las organizaciones pueden verse beneficiadas por estos cambios relacionados en el modo de justificar los requisitos indicados por la norma, especialmente aquellas más pequeñas típicamente con menos recursos y/o con varios sistemas de gestión implementados en la organización.

Actualización ISO/IEC27001 2005 -> 2013

En las siguientes 10 cláusulas que atienden a la nueva versión publicada de 2013 se presenta un resumen rápido de los 32 nuevos requisitos de la nueva versión.

Adicionalmente, hay que destacar diversas modificaciones en el modo de redactar los requisitos en la nueva versión con el objetivo de aclarar su propósito y fundamentos y que merecen una lectura detallada de los contenidos del estándar.

Anexo SL

La publicación ISO/IEC 27001:2013 atiende al nuevo esquema definido por ISO para los sistemas de gestión acorde al formato denominado “Annex SL” de 10 cláusulas, ya aplicado inicialmente en estándares como ISO/IEC 22301 y que será de próxima aplicación a revisiones de estándares relevantes como ISO/IEC 9001:2015, ISO/IEC 14001:2015, entre otros.

Este marco común procede de la Guía 83 de ISO y mejora sustancialmente la capacidad de integración de varios sistemas de gestión independientemente de los estándares de referencia. Las típicas tablas localizadas en los anexos de las normas (p.ej. Anexo C de ISO/IEC 27001:2005) quedan eliminadas al aplicar equivalencias directas en las cláusulas.

0 - INTRODUCCIÓN

Se mantienen los fundamentos en ambas versiones, es decir, la preservación de la Confidencialidad, Integridad y Disponibilidad de la información crítica mediante un proceso adecuado de gestión del riesgo.

Otra de las novedades más destacadas, es la posibilidad de alcanzar la mejora continua mediante implantaciones de un SGSI no necesariamente basadas en el "enfoque a procesos" representado por el diagrama con el modelo "PDCA", también denominado “ciclo Deming”.

1 - OBJETO Y CAMPO DE APLICACIÓN

La publicación ISO/IEC 27001:2013 atiende al nuevo esquema definido por ISO para los sistemas de gestión acorde al formato denominado “Annex SL” de 10 cláusulas, ya aplicado inicialmente en estándares como ISO/IEC 22301 y que será de próxima aplicación a revisiones de estándares relevantes como ISO/IEC 9001:2015, ISO/IEC 14001:2015, entre otros.

2 - REFERENCIAS NORMATIVAS

Se elimina en la nueva versión de 2013 la referencia a ISO/IEC 27002 de modo que, aunque las buenas prácticas recopiladas en el estándar ISO/IEC 27002 siguen siendo una ayuda práctica y directa para localizar y determinar controles de seguridad válidos en la gestión de los riesgos, este estándar puede ser complementado o incluso sustituido por otras referencias (regionales, sectoriales, regulatorios o reglamentarios) más útiles según la necesidad particular.

3 - TÉRMINOS Y DEFINICIONES

Se han eliminado de esta sección todas las definiciones de la versión 2005 y se han reubicado en el estándar ISO/IEC 27000 con el objetivo de consolidar la validez e interpretación de los mismos términos y definiciones en todas las publicaciones de la serie 27000.

4 - CONTEXTO DE LA ORGANIZACIÓN

4.1 - Conocimiento de la organización y su contexto

La organización debe determinar cuestiones externas e internas que son relevantes para sus propósitos y que afectan a su capacidad para lograr el/los resultado/s deseado/s de su sistema de gestión de seguridad de la información

Se debe revisar la definición del alcance actual, especialmente en su relación con entidades externas al mismo como novedad. Se trata de mejorar y desarrollar una capacidad de análisis de mayor grado con carácter preventivo.

Relaciones: Cláusula ISO/IEC 27001:2005: 8.3;

4.2 - Conocimiento de las necesidades y expectativas de las partes interesadas

a) La organización debe determinar las partes interesadas que son relevantes para el sistema de gestión de seguridad de la información

Se debe revisar la definición del alcance actual, especialmente en su relación con entidades externas al mismo como novedad. Se trata de mejorar y desarrollar una capacidad de análisis de mayor grado con carácter preventivo.

Relaciones: Cláusula ISO/IEC 27001:2005: 5.2.1 c), 7.2 b), 4.2.3 b), 4.2.4 d);

4.3 - Determinar el alcance del SGSI

Cuando se determina el alcance la organización debe considerar: a) cuestiones externas e internas referenciadas en 4.1; c) interrelaciones y dependencias entre las actividades desarrolladas por la organización y aquellas que son desarrolladas por otras organizaciones.

Se debe revisar la definición del alcance actual, espe cialmente en su relación con entidades externas al mismo como novedad. Se trata de mejorar y desarrollar una capacidad de análisis de mayor grado con carácter preventivo. A diferencia del alcance de certificación, la redefinición de los requisitos para el alcance en la nueva versión es una excelente oportunidad para indicar de forma más clara y específica todos los aspectos relevantes en el ámbito de la gestión de la seguridad.

Relaciones: Cláusula ISO/IEC 27001:2005: 4.2.1 a), 4.2.3 f);

4.4 - Sistema de Gestión de Seguridad de la Información

Sin novedades fundamentales, las consideraciones al ciclo PDCA de la versión de 2005 localizadas Plan: 4.2.1 - Do: 4.2.2 - Check: 4.2.3 - Act: 4.2.4 se trasladan en la nueva versión a Plan: 5, 6, 7 - Do: 8 - Check: 9 - Act: 10.

Relaciones: Cláusula ISO/IEC 27001:2005: 4.1;

5 - LIDERAZGO

Sin novedadesfundamentales, las consideraciones al ciclo PDCA de la versión de 2005 localizadas Plan: 4.2.1 - Do: 4.2.2 - Check: 4.2.3 - Act: 4.2.4 se trasladan en la nueva versión a Plan: 5, 6, 7 - Do: 8 - Check: 9 - Act: 10.

Relaciones: Cláusula ISO/IEC 27001:2005: 4.1;

5.1 - Liderazgo y compromiso

La alta dirección debe demostrar su liderazgo y compromiso con respecto al sistema de gestión de seguridad de la información a través de: b) garantizar la integración de los requisitos del sistema de gestión de seguridad de la información en los procesos de la organización; d) comunicar la importancia de una gestión eficaz de seguridad de la información y de adaptarse a los requisitos del sistema de gestión de seguridad de la información;

Se requiere que la alta dirección, además de gestionar (versión 2005), lidere la integración real de los requisitos del SGSI en los procesos de la organización como novedad. El cambio del rol de “gestor” a “líder” indica un mayor compromiso en las actividades relevantes y el papel de la alta dirección en propagar el ámbito de la seguridad a todo el personal del alcance para el logro de las metas y objetivos.

Relaciones: Cláusula ISO/IEC 27001:2005: 5.1;

5.2 - Política

Sin novedades fundamentales, la nueva versión del estándar no diferencia más entre "Política del SGSI" y la "Política de Seguridad de la Información". Sólo se considera una "política de seguridad de la información" (que puede ser documentada bajo la denominación “Política” o en otro modo particular admitido por cada organización).

Relaciones: Cláusula ISO/IEC 27001:2005: 4.2.1 b);

5.3 - Roles, responsabilidades y atribuciones en la organización informar a la alta dirección del estado de la seguridad.

Sin cambios fundamentales, se incide en la necesidad ya recogida por la versión anterior de una definición de roles y responsabilidades y la forma de interrelación entre el personal, especialmente en los mecanismos de informar a la alta dirección del estado de la seguridad.

Relaciones: Cláusula ISO/IEC 27001:2005: 5.1. c);

6 - Planificación

6.1 - Acciones para detectar los riesgos y oportunidades

6.1.1 - General

Sin cambios fundamentales, las acciones preventivas en el nuevo estándar desaparecen bajo esta denominación específica y forman parte ahora dentro de las acciones de identificación del riesgo y oportunidades para la mejora.

Relaciones: Cláusula ISO/IEC 27001:2005: 8.3;

6.1.2 - Análisis de riesgos en seguridad de la información

La metodología utilizada atendiendo a la versión ISO/IEC 27001:2005 está alineada con la nueva versión de ISO/IEC 27001:2013, aunque actualmente ya no se requiere dentro del proceso de identificación del riesgo identificar todos aquellos activos de información y sus propietarios, ni las amenazas, ni las vulnerabilidades de manera específica. Se incluye la nueva figura de “propietario del riesgos”.Sin novedades fundamentales, la nueva versión del estándar no diferencia más entre "Política del SGSI" y la "Política de Seguridad de la Información". Sólo se considera una "política de seguridad de la información" (que puede ser documentada bajo la denominación “Política” o en otro modo particular admitido por cada organización).

La alineación de ISO/IEC 27001:2013 con el estándar ISO 31000:2009 (“Gestión de Riesgos — Guías y principios”) abre por tanto posibilidades de cambios en el proceso de análisis del riesgo a otras posibilidades y metodologías más intuitivas, próximas al modo de gestión del negocio o adaptadas a las capacidades y recursos posibles para este proceso según sea el caso en cada organización.Relaciones: Cláusula ISO/IEC 27001:2005: 4.2.1 b);

Relaciones: Cláusula ISO/IEC 27001:2005: 4.2.1 c), 4.2.1 d), 4.2.1 e);

6.1.3 - Tratamiento de los riesgos de seguridad

El modo de uso del Anexo A puede ser ahora ligeramente diferente y más clara que en la versión del 2005. La determinación de controles para la reducción de los niveles en los riesgos identificados puede determinarse ahora en relación directa a ISO/IEC 27002 y/o a cualquier otra referencia documental (p.ej. NIST, Esquemas Nacionales de Seguridad, Buenas Prácticas de otros instituciones,…) o propia lógica de análisis de la organización.

El Anexo A pierde por tanto cierto carácter de requisito en los 114 controles que incluye aunque se deben mantener justificaciones claras sobre las consideraciones para la aplicación o no de acciones relacionadas. Al desarrollar esta actividad de justificación se debe prestar atención a la correcta interpretación de los controles indicados, especialmente en los nuevos incluidos.

El Anexo A pierde por tanto cierto carácter de requisito en los 114 controles que incluye aunque se deben mantener justificaciones claras sobre las consideraciones para la aplicación o no de acciones relacionadas. Al desarrollar esta actividad de justificación se debe prestar atención a la correcta interpretación de los controles indicados, especialmente en los nuevos incluidos.

Relaciones: Cláusula ISO/IEC 27001:2005: 4.2.1 f), 4.2.1 g), 4.2.1 h), 4.2.1 j), 4.2.2 a); 4.2.2 b)

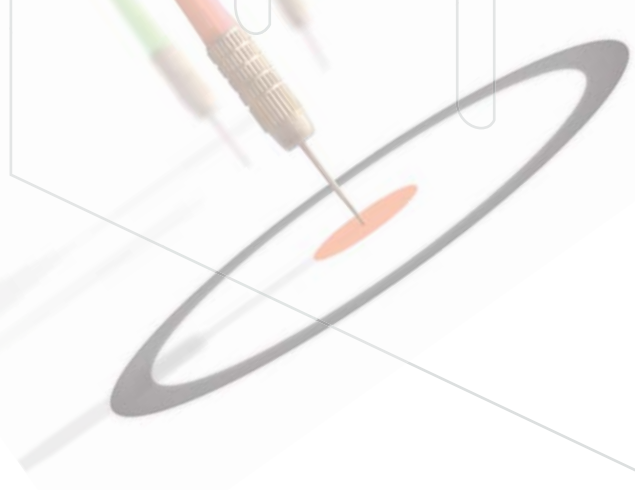
6.2 - Objetivos en seguridad de la información y planificación para lograrlos

Se deberán reconsiderar los objetivos en seguridad de la información, especialmente aquellos con enfoques genéricos que forman habitualmente parte de la política del SGSI para aplicar un enfoque orientado a acciones y medición de resultados realmente concretos.

Al planificar cómo alcanzar sus objetivos de seguridad de la información, la organización debe determinar de forma clara qué se hará, qué recursos serán necesarios, quién será responsable, cuándo se completará, y cómo se evaluarán los resultados.

Tener en cuenta los requisitos de seguridad de la información aplicable, así como los resultados de la evaluación y tratamiento de riesgos y su orientación respecto a los objetivos es un enfoque claramente orientado a que la organización pueda confirmar la efectividad del SGSI y su correspondencia con las intenciones del negocio.

Relaciones: Cláusula ISO/IEC 27001:2005: 5.1 b);



7 - MANTENIMIENTO

7.1 - Recursos

Sin cambios fundamentales. Relaciones: Cláusula ISO/IEC 27001:2005: 4.2.2 g), 5.2.1;

7.2 - Competencias

Sin cambios fundamentales. Relaciones: Cláusula ISO/IEC 27001:2005: 5.2.2;

7.3 - Concienciación

Se amplía el ámbito de modo que ahora todas las personas que desarrollan su trabajo bajo el control de la organización deben ser conscientes de la política de seguridad de la información.

Relaciones: Cláusula ISO/IEC 27001:2005: 4.2.2 e), 5.2.2;

7.4 - Comunicación

La organización debe determinar la necesidad de las comunicaciones internas y externas pertinentes para el sistema de gestión de seguridad de la información entre las que se incluye: a) lo que debe comunicarse; b) cuando debe comunicarse; c) a quién se comunica; d) quién debe comunicarlo; e) los procesos por los que la comunicación se debe efectuar.

La organización debe determinar la necesidad de las comunicaciones internas y externas pertinentes para el sistema de gestión de seguridad de la información entre las que se incluye: a) lo que debe comunicarse; b) cuando debe comunicarse; c) a quién se comunica; d) quién debe comunicarlo; e) los procesos por los que la comunicación se debe efectuar.

Relaciones: Cláusula ISO/IEC 27001:2005: 4.2.4 c), 5.1 d);

7.5 - Comunicación

Se introduce el término de 'Información documentada' que engloba en uno sólo la diferenciación tradicional entre "documentos" y "registros" de la versión 2005.

7.5.1 - General

Existe una diferencia importante de concepto y la eliminación de un listado determinado (anterior cláusula 4.3) donde se indican los mínimos de documentación. Se eliminan los procedimientos documentados (de auditoría interna, de control de la documentación y registros, de acciones preventivas y correctivas) como requisitos en sí mismos y se debe buscar por parte de las organizaciones aquella “información documentada” requerida por la nueva versión del estándar.

Relaciones: Cláusula ISO/IEC 27001:2005: 4.3;

7.5.2 - General

Sin Novedades Fundamentales

7.5.3 - Control de la información documentada

Sin Novedades Fundamentales

8 - OPERACIÓN

Sin Novedades Fundamentales

8.1 - Planificación operacional y control

La organización debe planificar, implementar y controlar los procesos necesarios para cumplir los requisitos de seguridad de la información, y para poner en práctica las acciones determinadas en el punto 6.1. La organización debe controlar los cambios planificados y revisar las consecuencias de cambios no deseados, adoptando medidas para mitigar los posibles efectos adversos, según sea necesario.

Se esperan posibles mejoras en los mecanismos de control que actualmente se aplican, según sea conveniente, especialmente en el aspecto de mitigación de posibles aspectos adversos asociados típicamente a una evaluación previa del riesgo y medidas de “paso atrás” a un estado inicial o previo seguro y controlado.

Relaciones: Cláusula ISO/IEC 27001:2005: 4.2.2 f);

8.2 - Análisis de riesgos en seguridad de la información

Sin cambios fundamentales en la periodicidad de revisión (intervalos planificados o cuando se propongan o producen cambios significativos) y teniendo en consideración los criterios establecidos en el punto 6.1.2 a)

Relaciones: Cláusula ISO/IEC 27001:2005: 4.2.3 d);

8.3 - Tratamiento de los riesgos de seguridad

Sin Novedades Fundamentales. Relaciones: Cláusula ISO/IEC 27001:2005: 4.2.2 b), 4.2.2 c);

9 - EVALUACIÓN DEL RENDIMIENTO

9.1 - Monitorización, medición, análisis y evaluación

La organización debe evaluar el desempeño de la seguridad de la información y la eficacia del sistema de gestión de seguridad de la información de un modo más claro y definido determinando: b) los métodos de monitorización, medición, análisis y evaluación, según se apliquen, para garantizar la validez de los resultados; c) cuándo se llevarán a cabo las monitorizaciones y mediciones; d) quién monitoriza y mide; f) quién analiza y evalúa los resultados.

Relaciones: Cláusula ISO/IEC 27001:2005: 4.2.2 d), 4.2.3 b), 4.2.3 c);

9.2 - Auditorías internas

Sin novedades fundamentales se remarca el aspecto de seleccionar auditores y realizar auditorías que garanticen la objetividad y la imparcialidad del proceso de auditoría.

Relaciones: Cláusula ISO/IEC 27001:2005: 4.2.3 e), 6;

9.3 - Revisión por la dirección

Se permite determinar ahora un periodo más flexible y personalizado en los intervalos de revisión por la dirección (no debe ser anual como requisito) y se añade principalmente la necesidad de revisar el cumplimiento de los objetivos de seguridad de la información en línea con otras cláusulas de la nueva versión relacionadas.

Relaciones: Cláusula ISO/IEC 27001:2005: 4.2.3 f), 7;

10 - MEJORA

10.1 - No conformidades y acciones correctivas

Las novedades fundamentales están en el modo de reaccionar a las no conformidades y evitar la recurrencia en el mismo o en otros lugares. Se trata de evitar la falta de profundidad localizada en el modo de acometer los análisis de causa para las no conformidades y la consecuente deficiencia en las acciones acometidas son una de las causas principales de las novedades en esta nueva versión y para los sistemas de gestión en general.

Relaciones: Cláusula ISO/IEC 27001:2005: 4.2.4, 8.2;

10.12 - Mejora contínua

Sin novedades fundamentales. Los requisitos para la mejora continua y acciones correctivas (cláusulas 8.1 y 8.2 de la versión 2005) pasan a formar parte de la cláusula 10.2 y 10.1 del nuevo estándar respectivamente. Los requisitos de las acciones preventivas (cláusula 8.3) se replantean en la nueva sección 6.1.1 como parte de los requisitos generales de la evaluación del riesgo. En este sentido, los requisitos de la versión 2005 no desaparecen, sólo se mencionan de un modo distinto.

Relaciones: Cláusula ISO/IEC 27001:2005: 4.2.4, 8.1;

Anexo A: Controles ISO/IEC 27001:2005 - Eliminados/Consolidados

Se indican a continuación de modo resumido los controles de la versión anterior no contemplados en la nueva versión.

Dominio 2005	Control 2005	Descripción Control ISO/IEC 27001:2005
A6	A6.1.1	Compromiso de la Dirección con la seguridad de la información
	A6.1.2	Coordinación de la seguridad de la información
	A6.1.4	Proceso de autoriazación de recursos para el tratamiento de la información
	A6.2.1	Identificación de riesgos por el acceso de terceros
	A6.2.2	Tratamiento de la seguridad en la relación con los clientes
A10	A6.1.1	Compromiso de la Dirección con la seguridad de la información
	A6.1.2	Coordinación de la seguridad de la información
	A6.1.4	Proceso de autoriazación de recursos para el tratamiento de la información
	A6.2.1	Identificación de riesgos por el acceso de terceros
	A6.2.2	Tratamiento de la seguridad en la relación con los clientes
A11	A11.4.2	Autentificación de usuario para conexiones externas
	A11.4.3	Identificación de equipos en redes
	A11.4.4	Diagnóstico remoto y protección de los puertos de configuración
	A11.4.6	Control de la conexión a red
	A11.4.7	Control de encanamiento de red
	A11.6.2	Aislamiento de sistemas sensibles
A12	A12.2.1	Validación de los datos iniciales
	A12.2.2	Control del procesamiento interno
	A12.2.3	Autentificación e integridad de los mensajes
	A12.2.4	Validación de los datos de salida
	A12.5.4	Fugas de información
A14	A14.1.1	Inclusión de la seguridad de la información en el proceso de gestión de la continuidad del negocio
	A14.1.3	Desarrollo e implantación de planes de continuidadque incluyan la seguridad de la información
	A14.1.4	Marco de referencia para la planificación de la continuidad del negocio
A15	A15.1.5	Prevención del uso indebido de las instalaciones de procesamiento de la información
	A15.3.2	Protección de las herramientas de auditoría de los sistemas de información

Anexo A

El Anexo A ser reorganiza ahora en 14 dominios (11 en la versión 2005), 35 objetivos de control (39 en versión 2005) y 114 controles (133 en versión 2005).

Cláusula 2013	Descripción Control ISO/IEC 27001:2003
5	**POLÍTICAS DE SEGURIDAD**
6	**ASPECTOS ORGANIZATIV OS DE LA SEGURIDAD DE LA INFORMACIÓN**
6.1	Organización interna
6.1.5	Seguridad de la información en la gestión de proyectos
7	**SEGURIDAD LIGADA A LOS RECURSOS HUMANOS**
8	**GESTIÓN DE ACTIVOS**
9	**CONTROL DE ACCESOS**
10	**CIFRADO**
11	**SEGURIDAD FÍSICA Y AMBIENTAL**
12	
12.6	Gestión de la vulnerabilidad técnica
12.6.2	Restricciones en la instalación de software
13	**SEGURIDAD EN LAS TELECOMUNICACIONES**
14	**ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN**
14.2	Seguridad en los procesos de desarrollo y soporte
14.2.1	Política de desarrollo seguro de software
14.2.5	Uso de principios de ingeniería en protección de sistemas
14.2.6	Seguridad en entornos de desarrollo
14.2.8	Pruebas de funcionalidad durante el desarrollo de los sistemas
15	**RELACIONES CON SUMINISTRADORES**
15.1	Seguridad de la información en las relaciones con suministradores
15.1.1	Política de seguridad de la información para suministradores
15.1.3	Cadena de suministro en tecnologías de la información y comunicaciones
16	**GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN**
16.1	Gestión de incidentes de seguridad de la información y mejoras
16.1.4	Valoración de eventos de seguridad de la información y toma de decisiones
16.1.5	Respuesta a los incidentes de seguridad
17	**ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN EN LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO**
17.2	Redundancias
17.2.1	Disponibilidad de instalaciones para el procesamiento de la información
18	**CUMPLIMIENTO**