norma española

UNE-ISO/IEC 27001

Noviembre 2007

TÍTULO

Tecnología de la información

Técnicas de seguridad

Sistemas de Gestión de la Seguridad de la Información (SGSI)

Requisitos

(ISO/IEC 27001:2005)

Information technology. Security techniques. Information security management systems. Requirements. (ISO/IEC 27001:2005).

Technologies de l'information. Techniques de sécurité. Systèmes de gestion de sécurité de l'information. Exigences. (ISO/IEC 27001:2005).

CORRESPONDENCIA

Esta norma es idéntica a la Norma Internacional ISO/IEC 27001:2005.

OBSERVACIONES

Esta norma anulará y sustituirá a la Norma UNE 71502:2004 el 2008-12-31.

ANTECEDENTES

Esta norma ha sido elaborada por el comité técnico AEN/CTN 71 *Tecnología de la Información* cuya Secretaría desempeña AETIC.

Editada e impresa por AENOR
Depósito legal: M 52351:2007

LAS OBSERVACIONES A ESTE DOCUMENTO HAN DE DIRIGIRSE A:

AENOR Asociación Española de Normalización y Certificación

C Génova, 6
28004 MADRID-España

Teléfono 91 432 60 00
Fax 91 310 40 32

35 Páginas

Grupo 22

ÍNDICE

PRÓLOGO

ISO (Organización Internacional de Normalización) e IEC (Comisión Electrotécnica Internacional) constituyen el sistema especializado para la normalización a nivel mundial. Los organismos nacionales que son miembros de ISO o IEC participan en el desarrollo de las normas internacionales a través de comités técnicos establecidos por las organizaciones respectivas para realizar acuerdos en campos específicos de la actividad técnica. Los comités técnicos de ISO e IEC colaboran en los campos de interés mutuo. Otras organizaciones internacionales, gubernamentales y no gubernamentales, en colaboración con ISO e IEC, también toman parte en el trabajo. En el campo de la tecnología de la información, ISO e IEC han establecido un comité técnico conjunto, el denominado ISO/IEC JTC 1.

Las normas internacionales se redactan de acuerdo con las reglas establecidas en la Parte 2 de las Directivas ISO/IEC.

La tarea principal de los comités técnicos es elaborar normas internacionales. Los proyectos de normas internacionales adoptados por los comités técnicos se envían a los organismos nacionales miembros para su voto. La publicación como norma internacional requiere la aprobación de al menos el 75% de los organismos nacionales miembros con derecho a voto.

Se llama la atención sobre la posibilidad de que algunos de los elementos de esta norma internacional puedan estar sujetos a derechos de patente. ISO e IEC no asumen la responsabilidad de la identificación de dichos derechos de patente.

La Norma ISO/IEC 27001 ha sido elaborada por el subcomité SC 27 *Técnicas de seguridad* que forma parte del comité técnico conjunto ISO/IEC JTC 1 *Tecnologías de la información.*

0 INTRODUCCIÓN

0.1 Generalidades

Esta norma internacional proporciona un modelo para la creación, implementación, operación, supervisión, revisión, mantenimiento y mejora de un Sistema de Gestión de la Seguridad de la Información (SGSI). La adopción de un SGSI debería ser fruto de una decisión estratégica de una organización. El diseño y la implementación del SGSI dependen de las necesidades y objetivos de cada organización, así como de sus requisitos de seguridad, sus procesos, su tamaño y estructura. Es previsible que estos factores y los sistemas que los soportan cambien con el tiempo. Lo habitual es que la implementación de un SGSI se ajuste a las necesidades de la organización; por ejemplo, una situación sencilla requiere un SGSI simple.

Esta norma internacional sirve para que cualquier parte interesada, ya sea interna o externa a la organización, pueda efectuar una evaluación de la conformidad.

0.2 Enfoque por proceso

Esta norma internacional adopta un enfoque por proceso para la creación, implementación, operación, supervisión, revisión, mantenimiento y mejora del SGSI de una organización.

Una organización tiene que definir y gestionar numerosas actividades para funcionar con eficacia. Cualquier actividad que utiliza recursos y se gestiona de modo que permite la transformación de unos elementos de "entrada" en unos elementos de "salida" puede considerarse un proceso. A menudo, la salida de un proceso se convierte directamente en la entrada del proceso siguiente.

La aplicación de un conjunto de procesos en una organización, junto con la identificación de éstos y sus interacciones y su gestión, puede calificarse de "enfoque por proceso".

El enfoque por proceso para la gestión de la seguridad de la información que se describe en esta norma internacional anima a los usuarios a enfatizar la importancia de:

a) comprender los requisitos de seguridad de la información de una organización y la necesidad de establecer una política de seguridad de la información y sus objetivos;

b) implementar y operar los controles para administrar los riesgos de seguridad de la información de una organización en el marco de sus riesgos empresariales generales;

c) supervisar y revisar el rendimiento y la eficacia del SGSI; y

d) asegurar la mejora continua sobre la base de la medición objetiva.

Esta norma internacional sigue el modelo "Planificar-hacer-verificar-actuar" (*Plan-Do-Check-Act* conocido como modelo PDCA), que se aplica para estructurar todos los procesos del SGSI. La figura 1 muestra cómo un SGSI, partiendo de los requisitos y expectativas de seguridad de la información de las partes interesadas y a través de las acciones y procesos necesarios, produce los elementos de salida de seguridad de la información que responden a dichos requisitos y expectativas. La figura 1 ilustra asimismo los vínculos con los procesos que se describen en los capítulos 4, 5, 6, 7 y 8.

La adopción del modelo PDCA también reflejará los principios definidos en las Directrices de la OCDE (2002)[1)] que rigen la seguridad de los sistemas y las redes de información. Esta norma internacional proporciona un modelo robusto para implementar los principios de dichas directrices que rigen la evaluación de riesgos, el diseño y la implementación de la seguridad, así como la gestión y la reevaluación de la seguridad.

1) Directrices de la OCDE para la Seguridad de los Sistemas y Redes de Información — Hacia una cultura de la seguridad. París: OCDE, julio de 2002. www.oecd.org.

EJEMPLO 1 (requisito de seguridad)

Un requisito podría ser que ninguna violación de la seguridad de la información debe provocar perjuicios económicos graves y/o comprometer a la organización.

EJEMPLO 2 (expectativa de seguridad)

En el caso de que se produjera un incidente grave, como por ejemplo un ataque informático al sitio web de comercio electrónico de una organización, debería haber personas con suficiente formación en los procedimientos adecuados para minimizar las consecuencias.

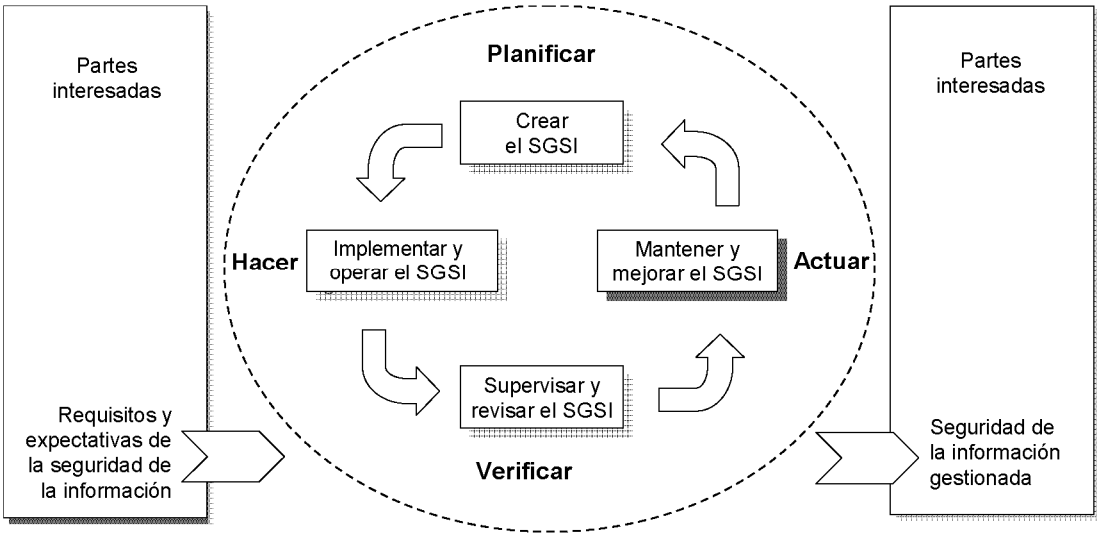

Figura 1 – Modelo PDCA aplicado a los procesos del SGSI

Planificar (creación del SGSI)	Definir la política, objetivos, procesos y procedimientos del SGSI relevantes para gestionar el riesgo y mejorar la seguridad de la información, con el fin de obtener resultados acordes con las políticas y objetivos generales de la organización.
Hacer (implementación y operación del SGSI)	Implementar y operar la política, controles, procesos y procedimientos del SGSI.
Verificar (supervisión y revisión del SGSI)	Evaluar y, en su caso, medir el rendimiento del proceso contra la política, los objetivos y la experiencia práctica del SGSI, e informar de los resultados a la Dirección para su revisión.
Actuar (mantenimiento y mejora del SGSI)	Adoptar medidas correctivas y preventivas, en función de los resultados de la auditoría interna del SGSI y de la revisión por parte de la dirección, o de otras informaciones relevantes, para lograr la mejora continua del SGSI.

0.3 Compatibilidad con otros sistemas de gestión

Esta norma internacional sigue las pautas marcadas en las Normas ISO 9001:2000 e ISO 14001:2004 para asegurar una implementación integrada y consistente con las mencionadas normas de gestión. De este modo, un sistema de gestión bien concebido puede cumplir los requisitos de todas esas normas. La tabla C.1 muestra la relación entre los capítulos de esta norma internacional y las Normas ISO 9001:2000 e ISO 14001:2004.

Esta norma internacional está diseñada para posibilitar a una organización el adaptar su SGSI a los requisitos de los sistemas de gestión mencionados.

IMPORTANTE: Esta publicación no pretende incluir todas las provisiones necesarias en un contrato. Los usuarios de la norma son responsables de su correcta aplicación. La conformidad con esta norma internacional no otorga inmunidad frente al cumplimiento de las obligaciones legales.

1 OBJETO Y CAMPO DE APLICACIÓN

1.1 Generalidades

Esta norma internacional abarca todo tipo de organizaciones (por ejemplo, empresas, organismos y entes públicos, entidades sin ánimo de lucro) y especifica los requisitos para la creación, implementación, operación, supervisión, revisión, mantenimiento y mejora de un SGSI documentado, en el marco de los riesgos empresariales generales de la organización. Especifica los requisitos para el establecimiento de controles de seguridad, adaptados a las necesidades de una organización o de partes de la misma.

El SGSI está diseñado con el fin de asegurar la selección de controles de seguridad, adecuados y proporcionados, que protejan los activos de información y den garantías a las partes interesadas.

NOTA 1 Las referencia al término "empresarial" o de "negocio" en esta norma internacional deberían interpretarse en un sentido amplio, abarcando aquellas actividades que son esenciales para alcanzar los fines que persigue la organización.

NOTA 2 La Norma ISO/IEC 17799 proporciona una guía de implantación que puede utilizarse al diseñar los controles.

1.2 Aplicación

Los requisitos establecidos en esta norma internacional son genéricos y aplicables a todas las organizaciones, cualquiera que sea su tipo, tamaño y naturaleza. Cuando una organización declara que cumple esta norma internacional, no se admitirá la exclusión de ninguno de los requisitos definidos en los capítulos 4, 5, 6, 7 y 8.

Toda exclusión de controles que se considere necesaria para cumplir los criterios de aceptación del riesgo necesita ser justificada mediante evidencia de que los riesgos asociados han sido aceptados por las personas responsables. Cuando se excluya algún control, no se aceptará ninguna declaración de conformidad con esta norma internacional a menos que tales exclusiones no afecten a la capacidad y/o responsabilidad de la organización para garantizar la seguridad de la información de acuerdo con los requisitos de seguridad derivados de la evaluación de riesgos y de los requisitos legales o reglamentarios aplicables.

NOTA En la mayoría de los casos, si una organización tiene implantado un sistema de gestión del proceso de negocio (por ejemplo, ISO 9001 o ISO 14001), es preferible cumplir los requisitos de esta norma internacional dentro del sistema de gestión ya existente.

2 NORMAS PARA CONSULTA

Las normas que a continuación se indican son indispensables para la aplicación de esta norma. Para las referencias con fecha, sólo se aplica la edición citada. Para las referencias sin fecha se aplica la última edición de la norma (incluyendo cualquier modificación de ésta).

ISO/IEC 17799:2005 *Tecnología de la información. Técnicas de seguridad. Código de buenas prácticas para la gestión de la seguridad de la información.*

3 TÉRMINOS Y DEFINICIONES

Para los fines del presente documento, se aplican las siguientes definiciones.

3.1 activo:
Cualquier bien que tiene valor para la organización.

[ISO/IEC 13335-1:2004]

3.2 disponibilidad:
La propiedad de ser accesible y utilizable por una entidad autorizada.

[ISO/IEC 13335-1:2004]

3.3 confidencialidad:
La propiedad por la que la información no se pone a disposición o se revela a individuos, entidades o procesos no autorizados.

[ISO/IEC 13335-1:2004]

3.4 seguridad de la información:
La preservación de la confidencialidad, la integridad y la disponibilidad de la información, pudiendo, además, abarcar otras propiedades, como la autenticidad, la responsabilidad, la fiabilidad y el no repudio.

[ISO/IEC 17799:2005]

3.5 evento de seguridad de la información:
La ocurrencia detectada en un estado de un sistema, servicio o red que indica una posible violación de la política de seguridad de la información, un fallo de las salvaguardas o una situación desconocida hasta el momento y que puede ser relevante para la seguridad.

[ISO/IEC TR 18044:2004]

3.6 incidente de seguridad de la información:
un único evento o una serie de eventos de seguridad de la información, inesperados o no deseados, que tienen una probabilidad significativa de comprometer las operaciones empresariales y de amenazar la seguridad de la información.

[ISO/IEC TR 18044:2004]

3.7 Sistema de Gestión de la Seguridad de la Información (SGSI) *[Information Security Management System (ISMS)]*:
La parte del sistema de gestión general, basada en un enfoque de riesgo empresarial, que se establece para crear, implementar, operar, supervisar, revisar, mantener y mejorar la seguridad de la información.

NOTA El sistema de gestión incluye la estructura organizativa, las políticas, las actividades de planificación, las responsabilidades, las prácticas, los procedimientos, los procesos y los recursos.

3.8 integridad:
La propiedad de salvaguardar la exactitud y completitud de los activos.

[ISO/IEC 13335-1:2004]

3.9 riesgo residual:
Riesgo remanente que existe después de que se hayan tomado las medidas de seguridad.

[ISO/IEC Guide 73:2002]

3.10 aceptación del riesgo:
La decisión de aceptar un riesgo.

[ISO/IEC Guide 73:2002]

3.11 análisis de riesgos:
Utilización sistemática de la información disponible para identificar peligros y estimar los riesgos.

[ISO/IEC Guide 73:2002]

3.12 evaluación de riesgos:
El proceso general de análisis y estimación de los riesgos.

[ISO/IEC Guide 73:2002]

3.13 estimación de riesgos:
El proceso de comparación del riesgo estimado con los criterios de riesgo, para así determinar la importancia del riesgo.

[ISO/IEC Guide 73:2002]

3.14 gestión de riesgos
Actividades coordinadas para dirigir y controlar una organización con respecto a los riesgos.

[ISO/IEC Guide 73:2002]

3.15 tratamiento de riesgos
El proceso de selección e implementación de las medidas encaminadas a modificar los riesgos.

[ISO/IEC Guide 73:2002].

NOTA En esta norma internacional, el término "control" se utiliza como sinónimo de "medida de seguridad."

3.16 declaración de aplicabilidad:
Declaración documentada que describe los objetivos de control y los controles que son relevantes para el SGSI de la organización y aplicables al mismo.

NOTA Los objetivos de control y los controles se basan en los resultados y conclusiones de la evaluación de riesgos y en los procesos de tratamiento del riesgo, en los requisitos legales o reglamentarios, en las obligaciones contractuales y en las necesidades empresariales de la organización en materia de seguridad de la información.

4 SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

4.1 Requisitos generales

La organización debe crear, implementar, operar, supervisar, revisar, mantener y mejorar un SGSI documentado dentro del contexto de las actividades empresariales generales de la organización y de los riesgos que ésta afronta. A efectos de esta norma internacional, el proceso utilizado se basa en el modelo PDCA descrito en la figura 1.

4.2 Creación y gestión del SGSI

4.2.1 Creación del SGSI

La organización debe hacer lo siguiente:

a) Definir el alcance y los límites del SGSI en términos de las características de la actividad empresarial, de la organización, su ubicación, sus activos y tecnología, incluyendo los detalles y la justificación de cualquier exclusión del alcance (véase 1.2).

b) Definir una política del SGSI acorde con las características de la actividad empresarial, la organización, su ubicación, sus activos y tecnología, que:

   1) incluya un marco para la fijación de objetivos y establezca una orientación general sobre las directrices y principios de actuación en relación con la seguridad de la información;

   2) tenga en cuenta los requisitos de la actividad empresarial, los requisitos legales o reglamentarios y las obligaciones de seguridad contractuales;

   3) esté alineada con el contexto de la estrategia de gestión de riesgos de la organización contexto en el que tendrá lugar la creación y el mantenimiento del SGSI;

4) establezca criterios de estimación del riesgo [véase 4.2.1c)] y

5) sea aprobada por la Dirección.

NOTA A efectos de esta norma internacional, la política de seguridad de la información se considera un subconjunto de la política del SGSI. Estas políticas pueden estar descritas en un único documento.

c) Definir el enfoque de la evaluación de riesgos de la organización.

1) Especificar una metodología de evaluación de riesgos adecuada para el SGSI, las necesidades de negocio identificadas en materia de seguridad de la información de la empresa y los requisitos legales y reglamentarios.

2) Desarrollar criterios de aceptación de riesgo y fijar los niveles de riesgo aceptables [véase 5.1f)].

La metodología seleccionada para la evaluación de riesgos debe asegurar que las evaluaciones de riesgos generen resultados comparables y reproducibles.

NOTA Hay diferentes metodologías para la evaluación de riesgos. En la Norma ISO/IEC TR 13335-3, Tecnología de la información. Directrices para la gestión de la seguridad de TI. Técnicas de gestión de la seguridad de TI , se comentan algunos ejemplos de metodologías para la evaluación de riesgos.

d) Identificar los riesgos.

1) Identificar los activos que están dentro del ámbito de aplicación del SGSI y a los propietarios[2)] de estos activos.

2) Identificar las amenazas a que están expuestos esos activos.

3) Identificar las vulnerabilidades bajo las que podrían actuar dichas amenazas.

4) Identificar los impactos que sobre los activos puede tener una pérdida de confidencialidad, integridad y disponibilidad en los mismos.

e) Analizar y valorar los riesgos.

1) Evaluar los efectos en la actividad empresarial de la organización que pudieran derivarse de eventuales fallos de seguridad, teniendo en cuenta las consecuencias de una pérdida de confidencialidad, integridad o disponibilidad de los activos.

2) Evaluar la probabilidad, de una forma realista, de que se produzcan fallos de seguridad a la luz de las amenazas y vulnerabilidades existentes, los impactos asociados a los activos y los controles implementados.

3) Estimar los niveles de riesgo.

4) Determinar si los riesgos son aceptables o si requieren un tratamiento conforme a los criterios de aceptación de riesgos establecidos en 4.2.1c)2).

f) Identificar y evaluar las opciones para el tratamiento de riesgos.

Las posibles acciones a realizar, entre otras, son las siguientes:

1) aplicar controles adecuados;

2) asumir los riesgos de manera consciente y objetiva, conforme a las políticas de la organización y a los criterios de aceptación de riesgos [véase 4.2.1c)2)];

3) evitar los riesgos; y

4) transferir los riesgos asociados a la actividad empresarial a otras partes, como por ejemplo compañías de seguros o proveedores.

2) El término “propietario” se refiere a un individuo o una entidad al que se le ha asignado la responsabilidad administrativa para el control de la producción, el desarrollo, el mantenimiento, el uso y la seguridad de los activos. El término “propietario” no significa que la persona tenga realmente algún derecho de propiedad sobre el activo.

g) Seleccionar los objetivos de control y los controles para el tratamiento de los riesgos.

Los objetivos de control y los controles deben seleccionarse e implementarse para cumplir los requisitos identificados en la evaluación de riesgos y en el proceso de tratamiento de riesgos. Esta selección debe tener en cuenta los criterios de aceptación de riesgos [véase 4.2.1c)2)], además de los requisitos legales, reglamentarios y contractuales.

Los objetivos de control y los controles del anexo A deben seleccionarse como parte de este proceso en la medida en que sirvan para satisfacer los requisitos identificados.

Los objetivos de control y los controles enumerados en el anexo A no son exhaustivos, por lo que pueden seleccionarse otros objetivos de control y otros controles adicionales.

NOTA El anexo A contiene una lista completa de objetivos de control y controles que se han considerado comúnmente relevantes en las organizaciones. El anexo A proporciona a los usuarios de esta norma internacional un punto de partida para seleccionar los controles, garantizando que no se pasan por alto importantes opciones de control.

h) Obtener la aprobación, por parte de la Dirección, de los riesgos residuales propuestos.

i) Obtener la autorización de la Dirección para implementar y operar el SGSI.

j) Elaborar una declaración de aplicabilidad.

Una declaración de aplicabilidad debe incluir lo siguiente:

1) los objetivos de control y los controles seleccionados en 4.2.1g) y las justificaciones de su selección;

2) los objetivos de control y los controles actualmente implementados [véase 4.2.1e)2)]; y

3) la exclusión de cualquier objetivo de control y control del anexo A y la justificación de esta exclusión.

NOTA La declaración de aplicabilidad proporciona un resumen de las decisiones relativas al tratamiento de los riesgos. La justificación de las exclusiones facilita una comprobación cruzada de que no se ha omitido inadvertidamente ningún control.

4.2.2 Implementación y operación del SGSI

La organización debe hacer lo que se indica a continuación.

a) Formular un plan de tratamiento de riesgos que identifique las acciones de la Dirección, los recursos, las responsabilidades y las prioridades adecuados para gestionar los riesgos de la seguridad de la información (véase 5).

b) Implementar el plan de tratamiento de riesgos para lograr los objetivos de control identificados, que tenga en cuenta la financiación y la asignación de funciones y responsabilidades.

c) Implementar los controles seleccionados en 4.2.1g) para cumplir los objetivos de control.

d) Definir el modo de medir la eficacia de los controles o de los grupos de controles seleccionados y especificar cómo tienen que usarse estas mediciones para evaluar la eficacia de los controles de cara a producir unos resultados comparables y reproducibles [véase 4.2.3c)].

NOTA La medición de la eficacia de los controles permite a los directivos y al personal determinar hasta qué punto los controles cumplen los objetivos de control planificados.

e) Implementar programas de formación y de concienciación (véase 5.2.2).

f) Gestionar la operación del SGSI.

g) Gestionar los recursos del SGSI (véase 5.2).

h) Implementar procedimientos y otros controles que permitan una detección temprana de eventos de seguridad y una respuesta ante cualquier incidente de seguridad [véase 4.2.3a)].

4.2.3 Supervisión y revisión del SGSI

La organización debe hacer lo que se indica a continuación.

a) Ejecutar procedimientos de supervisión y revisión, así como otros mecanismos de control para:

   1) detectar lo antes posible los errores en los resultados del procesado;

   2) identificar lo antes posible las debilidades del sistema de seguridad así como el aprovechamiento de éstas tanto con o sin éxito, y los incidentes;

   3) permitir a la Dirección determinar si las actividades de seguridad delegadas en otras personas o llevadas a cabo por medios informáticos o a través de tecnologías de la información, dan los resultados esperados;

   4) ayudar a detectar eventos de seguridad y por tanto a prevenir incidentes de seguridad mediante el uso de indicadores; y

   5) determinar si las acciones tomadas para resolver una violación de la seguridad han sido eficaces.

b) Realizar revisiones periódicas de la eficacia del SGSI teniendo en cuenta los resultados de las auditorías de seguridad, los incidentes, los resultados de las mediciones de la eficacia, las sugerencias así como los comentarios de todas las partes interesadas Estas revisiones incluyen el cumplimiento de la política, y de los objetivos del SGSI, y la revisión de los controles de seguridad

c) Medir la eficacia de los controles para verificar si se han cumplido los requisitos de seguridad.

d) Revisar las evaluaciones de riesgos en intervalos planificados y revisar los riesgos residuales y los niveles de riesgo aceptables que han sido identificados, teniendo en cuenta los cambios en:

   1) la organización;

   2) la tecnología;

   3) los objetivos y requisitos empresariales;

   4) las amenazas identificadas;

   5) la eficacia de los controles implementados; y

   6) los factores externos, como por ejemplo los cambios del entorno legal o reglamentario, de las obligaciones contractuales y del clima social.

e) Realizar las auditorías internas del SGSI en intervalos planificados (véase 6).

   NOTA Las auditorías internas, a veces denominadas auditorías por primera parte, las lleva a cabo la propia organización, o bien se realizan por encargo de ésta, con fines internos.

f) Realizar, por parte de la Dirección una revisión del SGSI, con carácter regular para asegurar que el ámbito de aplicación sigue siendo adecuado y que se identifican mejoras del proceso del SGSI (véase 7.1).

g) Actualizar los planes de seguridad teniendo en cuenta las conclusiones de las actividades de supervisión y revisión.

h) Registrar las acciones e incidencias que pudieran afectar a la eficacia o al funcionamiento del SGSI (véase 4.3.3).

4.2.4 Mantenimiento y mejora del SGSI

Regularmente, la organización debe hacer lo que se indica a continuación:

a) Implementar en el SGSI las mejoras identificadas.

b) Aplicar las medidas correctivas y preventivas adecuadas de acuerdo con los apartados 8.2 y 8.3, sobre la base de la experiencia en materia de seguridad de la propia organización y de otras organizaciones.

c) Comunicar las acciones y mejoras a todas las partes interesadas con un nivel de detalle acorde con las circunstancias.

d) Asegurar que las mejoras alcancen los objetivos previstos.

4.3 Requisitos de la documentación

4.3.1 Generalidades

La documentación debe incluir las decisiones de la Dirección junto con los registros (records) de las mismas, debiendo quedar constancia de que las acciones dan respuesta a las decisiones y a las políticas adoptadas, y garantizando que dichos documentos y los correspondientes registros están disponibles.

NOTA NACIONAL 1 Según recoge la Norma UNE-ISO 15489-1, el inglés posee tres términos distintos (documents, records y archives), para designar lo que en castellano, como en el resto de lenguas latinas, cuenta con una única voz (documentos). Así, document es el equivalente de documento en su significado genérico, como mera información registrada. Por el contrario, los términos records y archives designan de manera específica a aquellos documentos producidos como prueba y reflejo de las actividades de la organización que los ha creado, reservándose el empleo de este último a los documentos de carácter histórico.

NOTA NACIONAL 2 Un registro disponible es aquél que puede ser localizado, recuperado, presentado e interpretado.

Es importante poder demostrar la relación de los controles seleccionados con los resultados de los procesos de evaluación y de tratamiento de riesgos y por tanto, con la política y objetivos del SGSI.

La documentación del SGSI debe incluir:

a) declaraciones documentadas de la política [véase 4.2.1b)] y de los objetivos del SGSI;

b) el alcance del SGSI [véase 4.2.1a)];

c) los procedimientos y mecanismos de control que soportan al SGSI;

d) una descripción de la metodología de evaluación de riesgos [véase 4.2.1c)];

e) el informe de evaluación de riesgos [véase 4.2.1c) a 4.2.1 g)];

f) el plan de tratamiento de riesgos [véase 4.2.2b)];

g) los procedimientos documentados que necesita la organización para asegurar una correcta planificación, operación y control de sus procesos de seguridad de la información, y para describir cómo medir la eficacia de los controles [véase 4.2.3 c)];

h) los registros requeridos por esta norma internacional (véase 4.3.3); y

i) la declaración de aplicabilidad.

NOTA 1 Cuando en esta norma internacional aparece el término “procedimiento documentado”, significa que el procedimiento se crea, se documenta, se implementa y se mantiene.

NOTA 2 La extensión de la documentación del SGSI puede diferir de una organización a otra debido a:

- el tamaño y tipo de actividades de la organización; y
- el alcance y la complejidad de los requisitos de seguridad y del sistema que se está gestionando.

NOTA 3 Los documentos y registros pueden estar en cualquier formato o tipo de medio.

4.3.2 Control de documentos

Los documentos exigidos por el SGSI (véase 4.3.1) deben estar protegidos y controlados. Se debe establecer un procedimiento documentado para definir las acciones de gestión necesarias para:

a) aprobar en forma los documentos previamente a su distribución;

b) revisar, actualizar y volver a aprobar los documentos, según vaya siendo necesario;

c) asegurar que están identificados los cambios, así como el estado del documento que contiene la última revisión;

d) asegurar que las versiones correspondientes de los documentos están disponibles;

e) asegurar que los documentos permanecen legibles y fácilmente identificables;

f) asegurar que los documentos están disponibles para todo aquel que los necesita, y se transfieren, almacenan y se destruyen de acuerdo con los procedimientos aplicables a su clasificación;

g) asegurar que los documentos procedentes del exterior están identificados;

h) asegurar que la distribución de los documentos está controlada;

i) prevenir el uso no intencionado de documentos obsoletos; y

j) aplicar una identificación adecuada a los documentos obsoletos que son retenidos con algún propósito.

4.3.3 Control de registros

Se deben crear y mantener registros para proporcionar evidencias de la conformidad con los requisitos y del funcionamiento eficaz del SGSI. Dichos registros deben esta protegidos y controlados. El SGSI debe tener en cuenta cualquier requisito legal o regulatorio aplicable, así como las obligaciones contractuales. Los registros deben permanecer legibles, fácilmente identificables y recuperables. Los controles necesarios para la identificación, almacenamiento, protección, recuperación, retención y disposición de los registros deben estar documentados e implementados.

Deben conservarse los registros del desarrollo del proceso, según se indica en 4.2, y de todos los sucesos derivados de incidentes de seguridad significativos relativos al SGSI.

EJEMPLO

Ejemplos de registros son: el libro de visitas, los informes de auditoría y los formularios de autorización de acceso cumplimentados.

5 RESPONSABILIDAD DE LA DIRECCIÓN

5.1 Compromiso de la Dirección

La Dirección debe suministrar evidencias de su compromiso para crear, implementar, operar, supervisar, revisar, mantener y mejorar el SGSI, a través de las siguientes acciones:

a) formulando la política del SGSI;

b) velando por el establecimiento de los objetivos y planes del SGSI;

c) estableciendo los roles y responsabilidades en materia de seguridad de la información;

d) comunicando a la organización la importancia de cumplir los objetivos y la política de seguridad de la información, sus responsabilidades legales y la necesidad de la mejora continua;

e) proporcionando recursos suficientes para crear, implementar, operar, supervisar, revisar, mantener y mejorar el SGSI (véase 5.2.1);

f) decidiendo los criterios de aceptación de riesgos y los niveles aceptables de riesgo;

g) velando por que se realicen las auditorías internas del SGSI (véase 6); y

h) dirigiendo las revisiones del SGSI (véase 7).

5.2 Gestión de los recursos

5.2.1 Provisión de los recursos

La organización debe determinar y proporcionar los recursos necesarios para:

a) establecer, implementar, operar, supervisar, revisar, mantener y mejorar el SGSI;

b) asegurar que los procedimientos de seguridad de la información responden a los requisitos empresariales;

c) identificar y cumplir los requisitos legales y reglamentarios, así como las obligaciones de seguridad contractuales;

d) mantener la seguridad adecuada mediante la aplicación correcta de todos los controles implantados;

e) llevar a cabo revisiones, cuando sean necesarias, y reaccionar en base a los resultados de estas revisiones; y

f) cuando se requiera, mejorar la eficacia del SGSI.

5.2.2 Concienciación, formación y capacitación

La organización debe asegurarse de que todo el personal al que se le hayan asignado responsabilidades definidas en el SGSI sea competente para llevar a cabo las tareas requeridas, a través de:

a) determinar las competencias necesarias para el personal que lleva a cabo trabajos que afecten al SGSI;

b) impartir formación o realizar otras acciones (por ejemplo, la contratación de personal competente) para satisfacer estas necesidades;

c) evaluar la eficacia de las acciones realizadas; y

d) mantener registros de educación, formación, aptitudes, experiencia y cualificaciones (véase 4.3.3).

La organización, debe asegurarse también de que todo el personal afectado sea consciente de la trascendencia y de la importancia de las actividades de seguridad de la información y de su contribución a los objetivos del SGSI.

6 AUDITORÍAS INTERNAS DEL SGSI

La organización debe realizar auditorías internas del SGSI a intervalos planificados, para determinar si los objetivos de control, los controles, los procesos y los procedimientos de este SGSI:

a) cumplen los requisitos de esta norma internacional, así como la legislación y normativa aplicables;

b) cumplen los requisitos de seguridad de la información identificados;

c) se implantan y se mantienen de forma efectiva; y

d) dan el resultado esperado.

Se debe planificar un programa de auditorías, teniendo en cuenta el estado e importancia de los procesos y las áreas a auditar, así como los resultados de las auditorías previas. Se deben definir los criterios, el alcance, la frecuencia y los métodos de auditoría. La selección de auditores y la dirección de las auditorías debe garantizar la objetividad e imparcialidad del proceso de auditoría. Los auditores no deben auditar su propio trabajo.

Las responsabilidades y los requisitos para la planificación, realización de las auditorías, la información de los resultados y el mantenimiento de los registros (véase 4.3.3), deben estar definidos en un procedimiento documentado.

El responsable del área auditada debe velar por que se realicen acciones para eliminar, sin demoras indebidas, las disconformidades detectadas y sus causas. Las actividades de seguimiento, deben incluir la verificación de las acciones realizadas y los informes de los resultados de la verificación (véase 8).

NOTA La Norma ISO 19011:2002, *Directrices para la auditoría de los sistemas de gestión de la calidad y/o ambiental,* proporciona orientaciones útiles para realizar las auditorías internas del SGSI.

7 REVISIÓN DEL SGSI POR LA DIRECCIÓN

7.1 Generalidades

La Dirección debe revisar el SGSI de la organización a intervalos planificados (al menos una vez al año) para asegurar que se mantiene su conveniencia, adecuación y eficacia. Esta revisión debe contemplar las oportunidades de mejora y la necesidad de cambios en el SGSI, incluyendo la política y los objetivos de seguridad de la información. Los resultados de las revisiones deben estar claramente documentados y se deben mantener los registros (véase 4.3.3).

7.2 Datos iniciales de la revisión

Los datos utilizados por la Dirección para la revisión deben incluir:

a) los resultados de las auditorías y revisiones del SGSI;

b) los comentarios de las partes interesadas;

c) las técnicas, productos o procedimientos que podrían utilizarse dentro de la organización para mejorar el comportamiento y la eficacia del SGSI;

d) el estado de las acciones preventivas o correctivas;

e) las vulnerabilidades o amenazas no abordadas adecuadamente en la evaluación de riesgos previa;

f) los resultados de las mediciones de la eficacia;

g) las acciones de seguimiento de las revisiones anteriores;

h) cualquier cambio que pudiera afectar al SGSI; y

i) las recomendaciones de mejora.

7.3 Resultados de la revisión

Los resultados de la revisión realizada por la Dirección deben incluir cualquier decisión y acción relativas a :

a) la mejora de la eficacia del SGSI;

b) la actualización de la evaluación de riesgos y del plan de tratamiento de riesgos;

c) la modificación de los procedimientos y controles que afectan a la seguridad de la información, cuando sea necesario para responder a los eventos internos o externos que pueden afectar al SGSI, incluyendo los cambios en:

   1) los requisitos del negocio;

   2) los requisitos de seguridad;

   3) los procesos de negocio que afectan a los requisitos de negocio existentes;

   4) los requisitos legales o reglamentarios;

   5) las obligaciones contractuales; y

   6) los niveles de riesgo y/o los criterios de aceptación de los riesgos.

d) las necesidades de recursos;

e) la mejora en el modo de medir la eficacia de los controles.

8 MEJORA DEL SGSI

8.1 Mejora continua

La organización debe mejorar de manera continua la eficacia del SGSI, mediante el uso de la política y de los objetivos de seguridad de la información, de los resultados de las auditorías, del análisis de la monitorización de eventos, de las acciones correctivas y preventivas y de las revisiones de la Dirección (véase 7).

8.2 Acción correctiva

La organización debe realizar acciones para eliminar la causa de las no conformidades con los requisitos del SGSI, a fin de evitar que vuelvan a producirse. El procedimiento documentado para las acciones correctivas debe definir los requisitos para:

a) identificar las no conformidades;

b) determinar las causas de las no conformidades;

c) evaluar la necesidad de adoptar acciones para asegurarse de que las no conformidades no vuelvan a producirse;

d) determinar e implantar las acciones correctivas necesarias;

e) registrar los resultados de las acciones realizadas (véase 4.3.3); y

f) revisar las acciones correctivas realizadas.

8.3 Acción preventiva

La organización debe determinar las acciones necesarias para eliminar la causa de las posibles no conformidades con los requisitos del SGSI, para evitar que éstas vuelvan a producirse. Las acciones preventivas adoptadas deben ser apropiadas en relación a los efectos de los problemas potenciales. El procedimiento documentado para las acciones preventivas debe definir los requisitos para:

a) identificar las posibles no conformidades y sus causas;

b) evaluar la necesidad de adoptar acciones para prevenir la ocurrencia de no conformidades;

c) determinar e implementar las acciones preventivas necesarias;

d) registrar los resultados de las acciones adoptadas (véase 4.3.3); y

e) revisar las acciones preventivas adoptadas.

La organización debe identificar los cambios en los riesgos, así como los requisitos de las acciones preventivas, centrando la atención en los riesgos que hayan sufrido cambios significativos.

La prioridad de las acciones preventivas debe determinarse basándose en los resultados de la evaluación de riesgos.

NOTA Actuar para prevenir las no conformidades suele ser más rentable que realizar acciones correctivas.

ANEXO A (Normativo)

OBJETIVOS DE CONTROL Y CONTROLES

Los objetivos de control y los controles indicados en la tabla A.1 tienen correspondencia directa con los establecidos en la Norma ISO/IEC 17799:2005, capítulos 5 a 15. Las listas de la tabla A.1 no son exhaustivas y una organización puede considerar que son necesarios objetivos de control y controles adicionales. Los objetivos de control y los controles que figuran en estas tablas deben ser seleccionados como parte del proceso del SGSI especificado en el apartado 4.2.1.

Los capítulos 5 a 15 de la Norma ISO/IEC 17799:2005 ofrecen asesoramiento para la implantación junto con una guía de buenas prácticas de apoyo a los controles especificados en los puntos A.5 hasta A.15.

Tabla A.1 – Objetivos de control y controles

A.5 Política de seguridad		
A.5.1 Política de seguridad de la información		
Objetivo: Proporcionar indicaciones para la gestión y soporte de la seguridad de la información de acuerdo con los requisitos empresariales y con la legislación y las normativas aplicables.		
A.5.1.1	Documento de política de seguridad de la información	*Control* La Dirección debe aprobar un documento de política de seguridad de la información, publicarlo y distribuirlo a todos los empleados y terceros afectados.
A.5.1.2	Revisión de la política de seguridad e la información	*Control* La política de seguridad de la información debe revisarse a intervalos planificados o siempre que se produzcan cambios significativos, a fin de asegurar que se mantenga su idoneidad, adecuación y eficacia.
A.6 Aspectos organizativos de la seguridad de la información		
A.6.1 Organización interna		
Objetivo: Gestionar la seguridad de la información dentro de la organización.		
A.6.1.1	Comité de gestión de seguridad de la información.	*Control* La Dirección debe prestar un apoyo activo a la seguridad dentro de la organización a través de directrices claras, un compromiso demostrado, asignaciones explícitas y el reconocimiento de las responsabilidades de seguridad de la información.
A.6.1.2	Coordinación de la seguridad de la información	*Control* Las actividades relativas a la seguridad de la información deben ser coordinadas entre los representantes de las diferentes partes de la organización con sus correspondientes roles y funciones de trabajo.
A.6.1.3	Asignación de responsabilidades relativas a la seguridad de la información	*Control* Deben definirse claramente todas las responsabilidades relativas a la seguridad de la información.
A.6.1.4	Proceso de autorización de recursos para el procesado de la información	*Control* Para cada nuevo recurso de procesado de la información, debe definirse e implantarse un proceso de autorización por parte de la Dirección.
A.6.1.5	Acuerdos de confidencialidad	*Control* Debe determinarse y revisarse periódicamente la necesidad de establecer acuerdos de confidencialidad o no revelación, que reflejen las necesidades de la organización para la protección de la información.

A.6.1.6	Contacto con las autoridades	*Control* Deben mantenerse los contactos adecuados con las autoridades competentes.
A.6.1.7	Contacto con grupos de especial interés	*Control* Deben mantenerse los contactos apropiados con grupos de interés especial, u otros foros, y asociaciones profesionales especializados en seguridad.
A.6.1.8	Revisión independiente de la seguridad de la información	*Control* El enfoque de la organización para la gestión de la seguridad de la información y su implantación (es decir, los objetivos de control, los controles, las políticas, los procesos y los procedimientos para la seguridad de la información), debe someterse a una revisión independiente a intervalos planificados o siempre que se produzcan cambios significativos en la implantación de la seguridad.
A.6.2 Terceros *Objetivo:* Mantener la seguridad de la información de la organización y de los dispositivos de procesado de la información que son objeto de acceso, tratamiento, comunicación o gestión por terceros.		
A.6.2.1	Identificación de los riesgos derivados del acceso de terceros	*Control* Deben identificarse los riesgos para la información y para los dispositivos de procesado de la información de la organización derivados de los procesos de negocio que requieran de terceros, e implantar los controles apropiados antes de otorgar el acceso.
A.6.2.2	Tratamiento de la seguridad en la relación con los clientes	*Control* Antes de otorgar acceso a los clientes a los activos o a la información de la organización, deben tratarse todos los requisitos de seguridad identificados.
A.6.2.3	Tratamiento de la seguridad en contratos con terceros	*Control* Los acuerdos con terceros que conlleven acceso, tratamiento, comunicación o gestión, bien de la información de la organización, o de los recursos de tratamiento de la información, o bien la incorporación de productos o servicios a los recursos de tratamiento de la información, deben cubrir todos los requisitos de seguridad pertinentes.
A.7 Gestión de activos		
A.7.1 Responsabilidad sobre los activos *Objetivo:* Conseguir y mantener una protección adecuada de los activos de la organización.		
A.7.1.1	Inventario de activos	*Control* Todos los activos deben estar claramente identificados y debe elaborarse y mantenerse un inventario de todos los activos importantes.
A.7.1.2	Propiedad de los activos	*Control* Toda la información y activos asociados con los recursos para el tratamiento de la información deben tener un propietario[3)] que forme parte de la organización y haya sido designado como propietario
A.7.1.3	Uso aceptable de los activos	*Control* Se deben identificar, documentar e implantar las reglas para el uso aceptable de la información y los activos asociados con los recursos para el procesado de la información.

3) Explicación: El término "propietario" se refiere a la persona o entidad a la que se le ha asignado la responsabilidad administrativa del control de la producción, desarrollo, mantenimiento, uso y seguridad de los activos. El término "propietario" no significa que la persona tenga realmente algún derecho de propiedad sobre el activo.

A.7.2 Clasificación de la información		
Objetivo: Asegurar que la información recibe un nivel adecuado de protección.		
A.7.2.1	Directrices de clasificación	*Control* La información debe ser clasificada según su valor, los requisitos legales, la sensibilidad y la criticidad para la organización.
A.7.2.2	Etiquetado y manipulado de la información	*Control* Se debe desarrollar e implantar un conjunto adecuado de procedimientos para etiquetar y manejar la información, de acuerdo con el esquema de clasificación adoptado por la organización.
A.8 Seguridad ligada a los recursos humanos		
A.8.1 Antes del empleo[4)]		
Objetivo: Asegurar que los empleados, los contratistas y los terceros entienden sus responsabilidades, y son adecuados para llevar a cabo las funciones que les corresponden, así como para reducir el riesgo de robo, fraude o de uso indebido de los recursos.		
A.8.1.1	Funciones y responsabilidades	*Control* Las funciones y responsabilidades de seguridad de los empleados, contratistas y terceros se deben definir y documentar de acuerdo con la política de seguridad de la información de la organización.
A.8.1.2	Investigación de antecedentes	*Control* La comprobación de los antecedentes de todos los candidatos al puesto de trabajo, de los contratistas o de los terceros, se debe llevar a cabo de acuerdo con las legislaciones, normativas y códigos éticos que sean de aplicación y de una manera proporcionada a los requisitos del negocio, la clasificación de la información a la que se accede y los riesgos considerados.
A.8.1.3	Términos y condiciones de contratación	*Control* Como parte de sus obligaciones contractuales, los empleados, los contratistas y los terceros deben aceptar y firmar los términos y condiciones de su contrato de trabajo, que debe establecer sus responsabilidades y las de la organización en lo relativo a seguridad de la información.
A.8.2 Durante el empleo		
Objetivo: Asegurar que todos los empleados, contratistas y terceros son conscientes de las amenazas y problemas que afectan a la seguridad de la información y de sus responsabilidades y obligaciones, y de que están preparados para cumplir la política de seguridad de la organización, en el desarrollo habitual de su trabajo, y para reducir el riesgo de error humano.		
A.8.2.1	Responsabilidades de la Dirección	*Control* La Dirección debe exigir a los empleados, contratistas y terceros, que apliquen la seguridad de acuerdo con las políticas y procedimientos establecidos en la organización.
A.8.2.2	Concienciación, formación y capacitación en seguridad de la información	*Control* Todos los empleados de la organización y, cuando corresponda, los contratistas y terceros, deben recibir una adecuada concienciación y formación, con actualizaciones periódicas, sobre las políticas y procedimientos de la organización, según corresponda con su puesto de trabajo.

4) Explicación: La palabra "empleo" utilizada en este documento hace referencia a distintas situaciones: contratación de personal (temporal o de larga duración), nombramiento de cargos, cambio de cargos, asignación de contratistas, y terminación de cualquiera de estos acuerdos o compromisos.

A.8.2.3	Proceso disciplinario	*Control* Debe existir un proceso disciplinario formal para los empleados que hayan provocado alguna violación de la seguridad.
A.8.3 Cese del empleo o cambio de puesto de trabajo *Objetivo:* Asegurar que los empleados, contratistas y terceros abandonan la organización o cambian de puesto de trabajo de una manera ordenada.		
A.8.3.1	Responsabilidad del cese o cambio	*Control* Las responsabilidades para proceder al cese en el empleo o al cambio de puesto de trabajo deben estar claramente definidas y asignadas.
A.8.3.2	Devolución de activos	*Control* Todos los empleados, contratistas y terceros deben devolver todos activos de la organización que estén en su poder al finalizar su empleo, contrato o acuerdo.
A.8.3.3	Retirada de los derechos de acceso	*Control* Los derechos de acceso a la información y a los recursos de tratamiento de la información de todos los empleados, contratistas y terceros deben ser retirados a la finalización del empleo, del contrato o del acuerdo, o bien deben ser adaptados a los cambios producidos
A.9 Seguridad física y ambiental		
A.9.1 Áreas seguras *Objetivo:* Prevenir los accesos físicos no autorizados, los daños y las intromisiones en las instalaciones y en la información de la organización.		
A.9.1.1	Perímetro de seguridad física	*Control* Se deben utilizar perímetros de seguridad (barreras, muros, puertas de entrada con control a través de tarjeta, o puestos de control) para proteger las áreas que contienen la información y los recursos de tratamiento de la información.
A.9.1.2	Controles físicos de entrada	*Control* Las áreas seguras deben estar protegidas por controles de entrada adecuados, para asegurar que únicamente se permite el acceso al personal autorizado.
A.9.1.3	Seguridad de oficinas, despachos e instalaciones	*Control* Se deben diseñar y aplicar las medidas de seguridad física para las oficinas, despachos e instalaciones.
A.9.1.4	Protección contra las amenazas externas y de origen ambiental	*Control* Se debe diseñar y aplicar una protección física contra el daño causado por fuego, inundación, terremoto, explosión, revueltas sociales y otras formas de desastres naturales o provocados por el hombre.
A.9.1.5	Trabajo en áreas seguras	*Control* Se deben diseñar e implantar una protección física y una serie de directrices para trabajar en las áreas seguras.
A.9.1.6	Áreas de acceso público y de carga y descarga	*Control* Deben controlarse los puntos de acceso tales como las áreas de carga y descarga y otros puntos, a través de los que personal no autorizado puede acceder a las instalaciones, y si es posible, dichos puntos se deben aislar de los recursos de tratamiento de la información para evitar los accesos no autorizados.
A.9.2 Seguridad de los equipos *Objetivo:* Evitar pérdidas, daños, robos o circunstancias que pongan en peligro los activos, o que puedan provocar la interrupción de las actividades de la organización.		

A.9.2.1	Emplazamiento y protección de equipos	*Control* Los equipos deben situarse o protegerse de forma que se reduzcan los riesgos derivados de las amenazas y peligros de origen ambiental así como las ocasiones de que se produzcan accesos no autorizados.
A.9.2.2	Instalaciones de suministro	*Control* Los equipos deben estar protegidos contra fallos de alimentación y otras anomalías causadas por fallos en las instalaciones de suministro.
A.9.2.3	Seguridad del cableado	*Control* El cableado eléctrico y de telecomunicaciones que transmite datos o que da soporte a los servicios de información debe estar protegido frente a interceptaciones o daños.
A.9.2.4	Mantenimiento de los equipos	*Control* Los equipos deben recibir un mantenimiento correcto que asegure su disponibilidad y su integridad.
A.9.2.5	Seguridad de los equipos fuera de las instalaciones	*Control* Teniendo en cuenta los diferentes riesgos que conlleva trabajar fuera de las instalaciones de la organización, deben aplicarse medidas de seguridad a los equipos situados fuera dichas instalaciones.
A.9.2.6	Reutilización o retirada segura de equipos	*Control* Todos los soportes de almacenamiento deben ser comprobados para confirmar que todo dato sensible y todas las licencias de software se han eliminado o bien se han recargado de manera segura, antes de su retirada.
A.9.2.7	Retirada de materiales propiedad de la empresa	*Control* Los equipos, la información o el software no deben sacarse de las instalaciones, sin una autorización previa.
A.10 Gestión de comunicaciones y operaciones		
A.10.1 Responsabilidades y procedimientos de operación		
Objetivo: Asegurar el funcionamiento correcto y seguro de los recursos de procesamiento de la información.		
A.10.1.1	Documentación de los procedimientos de operación	*Control* Deben documentarse y mantenerse los procedimientos de operación y ponerse a disposición de todos los usuarios que los necesiten.
A.10.1.2	Gestión de cambios	*Control* Deben controlarse los cambios en los recursos y los sistemas de tratamiento de la información.
A.10.1.3	Segregación de tareas	*Control* Las tareas y áreas de responsabilidad deben segregarse para reducir la posibilidad de que se produzcan modificaciones no autorizadas o no intencionadas o usos indebidos de los activos de la organización.
A.10.1.4	Separación de los recursos de desarrollo, prueba y operación	*Control* Deben separarse los recursos de desarrollo, de pruebas y de operación, para reducir los riesgos de acceso no autorizado o los cambios en el sistema operativo.
A.10.2 Gestión de la provisión de servicios por terceros		
Objetivo: Implantar y mantener el nivel apropiado de seguridad de la información en la provisión del servicio, en consonancia con los acuerdos de provisión de servicios por terceros.		
A.10.2.1	Provisión de servicios	*Control* Se debe comprobar que los controles de seguridad, las definiciones de los servicios y los niveles de provisión, incluidos en el acuerdo de provisión de servicios por terceros, han sido implantados, puestos en operación y son mantenidos por parte de un tercero.

A.10.2.2	Supervisión y revisión de los servicios prestados por terceros	*Control* Los servicios, informes y registros proporcionados por un tercero deben ser objeto de supervisión y revisión periódicas, y también deben llevarse a cabo auditorias periódicas.
A.10.2.3	Gestión de cambios en los servicios prestados por terceros	*Control* Se deben gestionar los cambios en la provisión de los servicios, incluyendo el mantenimiento y la mejora de las políticas, los procedimientos y los controles de seguridad de la información existentes, teniendo en cuenta la criticidad de los procesos y sistemas del negocio afectados así como la reevaluación de los riesgos.
A.10.3 Planificación y aceptación del sistema *Objetivo:* Minimizar el riesgo de fallos de los sistemas.		
A.10.3.1	Gestión de capacidades	*Control* La utilización de los recursos se debe supervisar y ajustar así como realizar proyecciones de los requisitos futuros de capacidad, para garantizar el comportamiento requerido del sistema.
A.10.3.2	Aceptación del sistema	*Control* Se deben establecer los criterios para la aceptación de nuevos sistemas de información, de las actualizaciones y de nuevas versiones de los mismos, y se deben llevar a cabo pruebas adecuadas de los sistemas durante el desarrollo y previamente a la aceptación.
A.10.4 Protección contra código malicioso y descargable *Objetivo:* Proteger la integridad del software y de la información.		
A.10.4.1	Controles contra el código malicioso	*Control* Se deben implantar los controles de detección, prevención y recuperación que sirvan como protección contra código malicioso y se deben implantar procedimientos adecuados de concienciación del usuario.
A.10.4.2	Controles contra el código descargado en el cliente	*Control* Cuando se autorice el uso de código descargado en el cliente, (JavaScript, VBScript, applets de Java applets, controles ActiveX, etc..), la configuración debe garantizar que dicho código autorizado funciona de acuerdo con una política de seguridad claramente definida, y se debe evitar que se ejecute el código no autorizado.
A.10.5 Copias de seguridad *Objetivo:* Mantener la integridad y disponibilidad de la información y de los recursos de tratamiento de la información.		
A.10.5.1	Copias de seguridad de la información	*Control* Se deben realizar copias de seguridad de la información y del software, y se deben probar periódicamente con conforme a la política de copias de seguridad acordada.
A.10.6 Gestión de la seguridad de las redes *Objetivo:* Asegurar la protección de la información en las redes y la protección de la infraestructura de soporte.		
A.10.6.1	Controles de red	*Control* Las redes deben estar adecuadamente gestionadas y controladas, para que estén protegidas frente a posibles amenazas y para mantener la seguridad de los sistemas y de las aplicaciones que utilizan estas redes, incluyendo la información en tránsito.

A.10.6.2	Seguridad de los servicios de red	*Control* Se deben identificar las características de seguridad, los niveles de servicio, y los requisitos de gestión de todos los servicios de red y se deben incluir en todo acuerdo de servicios de red, tanto si estos servicios se prestan dentro de la organización como si se subcontratan.
A.10.7 Manipulación de los soportes *Objetivo:* Evitar la revelación, modificación, retirada o destrucción no autorizada de los activos, y la interrupción de las actividades de la organización.		
A.10.7.1	Gestión de soportes extraíbles	*Control* Se deben establecer procedimientos para la gestión de los soportes extraíbles.
A.10.7.2	Retirada de soportes	*Control* Los soportes deben ser retirados de forma segura cuando ya no vayan a ser necesarios, mediante los procedimientos formales establecidos.
A.10.7.3	Procedimientos de manipulación de la información	*Control* Deben establecerse procedimientos para la manipulación y el almacenamiento de la información, de modo que se proteja dicha información contra la revelación no autorizada o el uso indebido.
A.10.7.4	Seguridad de la documentación del sistema	*Control* La documentación del sistema debe estar protegida contra accesos no autorizados.
A.10.8 Intercambio de información *Objetivo:* Mantener la seguridad de la información y del software intercambiados dentro de una organización y con un tercero		
A.10.8.1	Políticas y procedimientos de intercambio de información	*Control* Deben establecerse políticas, procedimientos y controles formales que protejan el intercambio de información mediante el uso de todo tipo de recursos de comunicación.
A.10.8.2	Acuerdos de intercambio	*Control* Deben establecerse acuerdos para el intercambio de información y del software entre la organización y los terceros.
A.10.8.3	Soportes físicos en tránsito	*Control* Durante el transporte fuera de los límites físicos de la organización, los soportes que contengan información deben estar protegidos contra accesos no autorizados, usos indebidos o deterioro.
A.10.8.4	Mensajería electrónica	*Control* La información que sea objeto de mensajería electrónica debe estar adecuadamente protegida.
A.10.8.5	Sistemas de información empresariales	*Control* Deben formularse e implantarse políticas y procedimientos para proteger la información asociada a la interconexión de los sistemas de información empresariales
A.10.9 Servicios de comercio electrónico *Objetivo:* Garantizar la seguridad de los servicios de comercio electrónico, y el uso seguro de los mismos		
A.10.9.1	Comercio electrónico	*Control* La información incluida en el comercio electrónico que se transmita a través de redes públicas debe protegerse contra las actividades fraudulentas, las disputas contractuales, y la revelación o modificación no autorizada de dicha información.

A.10.9.2	Transacciones en línea	*Control* La información contenida en las transacciones en línea debe estar protegida para evitar transmisiones incompletas, errores de direccionamiento, alteraciones no autorizadas de los mensajes, la revelación, la duplicación o la reproducción no autorizadas del mensaje.
A.10.9.3	Información puesta a disposición pública	*Control* La integridad de la información puesta a disposición pública se debe proteger para evitar modificaciones no autorizadas.
A.10.10 Supervisión		
Objetivo: Detectar las actividades de procesamiento de la información no autorizadas.		
A.10.10.1	Registro de auditorias	*Control* Se deben realizar registros de auditoria de las actividades de los usuarios, las excepciones y eventos de seguridad de la información, y se deben mantener estos registros durante un periodo acordado para servir como prueba en investigaciones futuras y en la supervisión del control de acceso.
A.10.10.2	Supervisión del uso del sistema	*Control* Se deben establecer procedimientos para supervisar el uso de los recursos de procesamiento de la información y se deben revisar periódicamente los resultados de las actividades de supervisión.
A.10.10.3	Protección de la información de los registros	*Control* Los dispositivos de registro y la información de los registros deben estar protegidos contra manipulaciones indebidas y accesos no autorizados.
A.10.10.4	Registros de administración y operación	*Control* Se deben registrar las actividades del administrador del sistema y de la operación del sistema.
A.10.10.5	Registro de fallos	*Control* Los fallos deben ser registrados y analizados y se deben tomar las correspondientes acciones
A.10.10.6	Sincronización del reloj	*Control* Los relojes de todos los sistemas de procesamiento de la información dentro de una organización o de un dominio de seguridad, deben estar sincronizados con una precisión de tiempo acordada.
A.11 Control de acceso		
A.11.1 Requisitos de negocio para el control de acceso		
Objetivo: Controlar el acceso a la información		
A.11.1.1	Política de control de acceso	*Control* Se debe establecer, documentar y revisar una política de control de acceso basada en los requisitos empresariales y de seguridad para el acceso.
A.11.2 Gestión de acceso de usuario		
Objetivo: Asegurar el acceso de un usuario autorizado y prevenir el acceso no autorizado a los sistemas de información		
A.11.2.1	Registro de usuario	*Control* Debe establecerse un procedimiento formal de registro y de anulación de usuarios para conceder y revocar el acceso a todos los sistemas y servicios de información.
A.11.2.2	Gestión de privilegios	*Control* La asignación y el uso de privilegios deben estar restringidos y controlados.
A.11.2.3	Gestión de contraseñas de usuario	*Control* La asignación de contraseñas debe ser controlada a través de un proceso de gestión formal

A.11.2.4	Revisión de los derechos de acceso de usuario	*Control* La Dirección debe revisar los derechos de acceso de usuario a intervalos regulares y utilizando un proceso formal.
A.11.3 Responsabilidades de usuario *Objetivo:* Prevenir el acceso de usuarios no autorizados, así como evitar el que se comprometa o se produzca el robo de la información o de los recursos de procesamiento de la información		
A.11.3.1	Uso de contraseña	*Control* Se debe requerir a los usuarios el seguir las buenas prácticas de seguridad en la selección y el uso de las contraseñas.
A.11.3.2	Equipo de usuario desatendido	*Control* Los usuarios deben asegurarse de que el equipo desatendido tiene la protección adecuada.
A.11.3.3	Política de puesto de trabajo despejado y pantalla limpia	*Control* Debe adoptarse una política de puesto de trabajo despejado de papeles y de soportes de almacenamiento extraíbles junto con una política de pantalla limpia para los recursos de procesamiento de la información.
A.11.4 Control de acceso a la red *Objetivo:* Prevenir el acceso no autorizado a los servicios en red.		
A.11.4.1	Política de uso de los servicios en red	*Control* Se debe proporcionar a los usuarios únicamente el acceso a los servicios para que los que hayan sido específicamente autorizados.
A.11.4.2	Autenticación de usuario para conexiones externas	*Control* Se deben utilizar los métodos apropiados de autenticación para controlar el acceso de los usuarios remotos.
A.11.4.3	Identificación de los equipos en las redes	*Control* La identificación automática de los equipos se debe considerar como un medio de autenticación de las conexiones provenientes de localizaciones y equipos específicos.
A.11.4.4	Diagnóstico remoto y protección de los puertos de configuración	*Control* Se debe controlar el acceso físico y lógico a los puertos de diagnóstico y de configuración.
A.11.4.5	Segregación de las redes	*Control* Los grupos de servicios de información, usuarios y sistemas de información deben estar segregados en redes.
A.11.4.6	Control de la conexión a la red	*Control* En redes compartidas, especialmente en aquellas que traspasen las fronteras de la organización, debe restringirse la capacidad de los usuarios para conectarse a la red, esto debe hacerse de acuerdo a la política de control de acceso y a los requisitos de las aplicaciones del negocio (véase 11.1).
A.11.4.7	Control de encaminamiento (*routing)* de red	*Control* Se deben implantar controles de encaminamiento (*routing*) de redes para asegurar que las conexiones de los ordenadores y los flujos de información no violan la política de control de acceso de las aplicaciones empresariales.
A.11.5 Control de acceso al sistema operativo *Objetivo:* Prevenir el acceso no autorizado a los sistemas operativos.		
A.11.5.1	Procedimientos seguros de inicio de sesión	Control El acceso a los sistemas operativos se debe controlar por medio de un procedimiento seguro de inicio de sesión.

A.11.5.2	Identificación y autenticación de usuario	*Control* Todos los usuarios deben tener un identificador único (ID de usuario) para su uso personal y exclusivo, y se debe elegir una técnica adecuada de autenticación para confirmar la identidad solicitada del usuario.
A.11.5.3	Sistema de gestión de contraseñas	*Control* Los sistemas para la gestión de contraseñas deben ser interactivos y establecer contraseñas seguras y robustas.
A.11.5.4	Uso de los recursos del sistema	*Control* Se debe restringir y controlar rigurosamente el uso de programas y utilidades que puedan ser capaces de invalidar los controles del sistema y de la aplicación.
A.11.5.5	Desconexión automática de sesión.	*Control* Las sesiones inactivas deben cerrarse después de un periodo de inactividad definido.
A.11.5.6	Limitación del tiempo de conexión	*Control* Para proporcionar seguridad adicional a las aplicaciones de alto riesgo, se deben utilizar restricciones en los tiempos de conexión.
A.11.6 Control de acceso a las aplicaciones y a la información *Objetivo:* Prevenir el acceso no autorizado a la información que contienen las aplicaciones		
A.11.6.1	Restricción del acceso a la información	*Control* Se debe restringir el acceso a la información y a las aplicaciones a los usuarios y al personal de soporte, de acuerdo con la política de control de acceso definida.
A.11.6.2	Aislamiento de sistemas sensibles	*Control* Los sistemas sensibles deben tener un entorno de ordenadores dedicados (aislados).
A.11.7 Ordenadores portátiles y teletrabajo *Objetivo:* Garantizar la seguridad de la información cuando se utilizan ordenadores portátiles y servicios de teletrabajo.		
A.11.7.1	Ordenadores portátiles y comunicaciones móviles	*Control* Se debe implantar una política formal y se deben adoptar las medidas de seguridad adecuadas de protección contra los riesgos de la utilización de ordenadores portátiles y comunicaciones móviles.
A.11.7.2	Teletrabajo	*Control* Se debe redactar e implantar, una política de actividades de teletrabajo, así como los planes y procedimientos de operación correspondientes.
A.12 Adquisición, desarrollo y mantenimiento de los sistemas de información		
A.12.1 Requisitos de seguridad de los sistemas de información *Objetivo:* Garantizar que la seguridad está integrada en los sistemas de información.		
A.12.1.1	Análisis y especificación de los requisitos de seguridad	*Control* En las declaraciones de los requisitos de negocio para los nuevos sistemas de información, o para mejoras de los sistemas de información ya existentes, se deben especificar los requisitos de los controles de seguridad.
A.12.2 Tratamiento correcto de las aplicaciones *Objetivo:* Evitar errores, pérdidas, modificaciones no autorizadas o usos indebidos de la información en las aplicaciones		
A.12.2.1	Validación de los datos de entrada	*Control* La introducción de datos en las aplicaciones debe validarse para garantizar que dichos datos son correctos y adecuados.

A.12.2.2	Control del procesamiento interno	*Control* Para detectar cualquier corrupción de la información debida a errores de procesamiento o actos intencionados, se deben incorporar comprobaciones de validación en las aplicaciones.
A.12.2.3	Integridad de los mensajes	*Control* Se deben identificar los requisitos para garantizar la autenticidad y para proteger la integridad de los mensajes en las aplicaciones y se deben identificar e implantar los controles adecuados.
A.12.2.4	Validación de los datos de salida	*Control* Los datos de salida de una aplicación se deben validar para garantizar que el tratamiento de la información almacenada es correcto y adecuado a las circunstancias.
A.12.3 Controles criptográficos *Objetivo:* Proteger la confidencialidad, la autenticidad o la integridad de la información por medios criptográficos.		
A.12.3.1	Política de uso de los controles criptográficos	*Control* Se debe formular e implantar una política para el uso de los controles criptográficos para proteger la información.
A.12.3.2	Gestión de claves	*Control* Debe implantarse un sistema de gestión de claves para dar soporte al uso de técnicas criptográficas por parte de la organización.
A.12.4 Seguridad de los archivos de sistema *Objetivo:* Garantizar la seguridad de los archivos de sistema.		
A.12.4.1	Control del software en explotación	*Control* Deben estar implantados procedimientos para controlar la instalación de software en los sistemas operativos.
A.12.4.2	Protección de los datos de prueba del sistema	*Control* Los datos de prueba se deben seleccionar con cuidado y deben estar protegidos y controlados.
A.12.4.3	Control de acceso al código fuente de los programas	*Control* Se debe restringir el acceso al código fuente de los programas.
A.12.5 Seguridad en los procesos de desarrollo y soporte *Objetivo:* Mantener la seguridad del software y de la información de las aplicaciones		
A.12.5.1	Procedimientos de control de cambios	*Control* La implantación de cambios debe controlarse mediante el uso de procedimientos formales de control de cambios.
A.12.5.2	Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo	*Control* Cuando se modifiquen los sistemas operativos, las aplicaciones empresariales críticas deben ser revisadas y probadas para garantizar que no existen efectos adversos en las operaciones o en la seguridad de la organización.
A.12.5.3	Restricciones a los cambios en los paquetes de software	*Control* Se deben desaconsejar las modificaciones en los paquetes de software, limitándose a los cambios necesarios, y todos los cambios deben ser objeto de un control riguroso.
A.12.5.4	Fugas de información	*Control* Deben evitarse las situaciones que permitan que se produzcan fugas de información.
A.12.5.5	Externalización del desarrollo de software	*Control* La externalización del desarrollo de software debe ser supervisada y controlada por la organización.

A.12.6 Gestión de la vulnerabilidad técnica		
Objetivo: Reducir los riesgos resultantes de la explotación de las vulnerabilidades técnicas publicadas.		
A.12.6.1	Control de las vulnerabilidades técnicas	*Control* Se debe obtener información oportuna acerca de las vulnerabilidades técnicas de los sistemas de información que están siendo utilizados, evaluar la exposición de la organización a dichas vulnerabilidades y adoptar las medidas adecuadas para afrontar el riesgo asociado.
A.13 Gestión de incidentes de seguridad de la información		
A.13.1 Notificación de eventos y puntos débiles de la seguridad de la información		
Objetivo: Asegurarse de que los eventos y las vulnerabilidades de la seguridad de la información, asociados con los sistemas de información, se comunican de manera que sea posible emprender las acciones correctivas oportunas.		
A.13.1.1	Notificación de los eventos de seguridad de la información	*Control* Los eventos de seguridad de la información se deben notificar a través de los canales adecuados de gestión lo antes posible.
A.13.1.2	Notificación de los puntos débiles de la seguridad	*Control* Todos los empleados, contratistas, y terceros que sean usuarios de los sistemas y servicios de información deben estar obligados a anotar y notificar cualquier punto débil que observen o que sospechen exista, en dichos sistemas o servicios.
A.13.2 Gestión de incidentes de seguridad de la información y mejoras		
Objetivo: Garantizar que se aplica un enfoque coherente y efectivo a la gestión de los incidentes de seguridad de la información.		
A.13.2.1	Responsabilidades y procedimientos	*Control* Se deben establecer las responsabilidades y procedimientos de gestión para garantizar una respuesta rápida, efectiva y ordenada a los incidentes de seguridad de la información.
A.13.2.2	Aprendizaje de los incidentes de seguridad de la información	*Control* Deben existir mecanismos que permitan cuantificar y supervisar los tipos, volúmenes y costes de los incidentes de seguridad de la información.
A.13.2.3	Recopilación de evidencias	*Control* Cuando se emprenda una acción contra una persona u organización, después de un incidente de seguridad de la información, que implique acciones legales (tanto civiles como penales), deben recopilarse las evidencias, conservarse y presentarse conforme a las normas establecidas en la jurisdicción correspondiente.
A.14 Gestión de la continuidad del negocio		
A.14.1 Aspectos de seguridad de la información en la gestión de la continuidad del negocio		
Objetivo: Contrarrestar las interrupciones de las actividades empresariales y proteger los procesos críticos de negocio de los efectos derivados de fallos importantes o catastróficos de los sistemas de información, así como garantizar su oportuna reanudación		
A.14.1.1	Inclusión de la seguridad de la información en el proceso de gestión de la continuidad del negocio	*Control* Debe desarrollarse y mantenerse un proceso para la continuidad del negocio en toda la organización, que gestione los requisitos de seguridad de la información necesarios para la continuidad del negocio.

A.14.1.2	Continuidad del negocio y evaluación de riesgos	*Control* Deben identificarse los eventos que puedan causar interrupciones en los procesos de negocio, así como la probabilidad de que se produzcan tales interrupciones, sus efectos y sus consecuencias para la seguridad de la información.
A.14.1.3	Desarrollo e implantación de planes de continuidad que incluyan la seguridad de la información	*Control* Deben desarrollarse e implantarse planes para mantener o restaurar las operaciones y garantizar la disponibilidad de la información en el nivel y en el tiempo requeridos, después de una interrupción o un fallo de los procesos de negocio críticos.
A.14.1.4	Marco de referencia para la planificación de la continuidad del negocio	*Control* Debe mantenerse un único marco de referencia para los planes de continuidad del negocio, para asegurar que todos los planes sean coherentes, para cumplir los requisitos de seguridad de la información de manera consistente y para identificar las prioridades de realización de pruebas y de mantenimiento.
A.14.1.5	Pruebas, mantenimiento y reevaluación de los planes de continuidad del negocio	*Control* Los planes de continuidad del negocio deben probarse y actualizarse periódicamente para asegurar que están al día y que son efectivos.
A.15 Cumplimiento		
A.15.1 Cumplimiento de los requisitos legales *Objetivo:* Evitar incumplimientos de las leyes o de las obligaciones legales, reglamentarias o contractuales y de los requisitos de seguridad.		
A.15.1.1	Identificación de la legislación aplicable	*Control* Todos los requisitos pertinentes, tanto legales como reglamentarios o contractuales, y el enfoque de la organización para cumplir dichos requisitos, deben estar definidos, documentados y mantenerse actualizados de forma explícito para cada sistema de información de la organización.
A.15.1.2	Derechos de propiedad intelectual (DPI) [*Intellectual Property Rights* (IPR)]	*Control* Deben implantarse procedimientos adecuados para garantizar el cumplimiento de los requisitos legales, reglamentarios y contractuales sobre el uso de material, con respecto al cual puedan existir derechos de propiedad intelectual y sobre el uso de productos de software/propietario.
A.15.1.3	Protección de los documentos[3)] de la organización	*Control* Los documentos importantes deben estar protegidos contra la pérdida, destrucción y falsificación de acuerdo con los requisitos legales, regulatorios, contractuales y empresariales.
A.15.1.4	Protección de datos y privacidad de la información personal	*Control* Debe garantizarse la protección y la privacidad de los datos según se requiera en la legislación y las regulaciones y, en su caso, en las cláusulas contractuales pertinentes.
A.15.1.5	Prevención del uso indebido de los recursos de tratamiento de la información	*Control* Se debe impedir que los usuarios utilicen los recursos de tratamiento de la información para fines no autorizados.

3) NOTA NACIONAL Según recoge la Norma UNE-ISO 15489-1, el inglés posee tres términos distintos (documents, records y archives), para designar lo que en castellano, como en el resto de lenguas latinas, cuenta con una única voz (documentos). Así, document es el equivalente de documento en su significado genérico, como mera información registrada. Por el contrario, los términos records y archives designan de manera específica a aquellos documentos producidos como prueba y reflejo de las actividades de la organización que los ha creado, reservándose el empleo de este último a los documentos de carácter histórico.

A.15.1.6	Regulación de los controles criptográficos	*Control* Los controles criptográficos se deben utilizar de acuerdo con todos los contratos, leyes y regulaciones pertinentes.
A.15.2 Cumplimiento de las políticas y normas de seguridad y cumplimiento técnico *Objetivo:* Asegurar que los sistemas cumplen las políticas y normas de seguridad de la organización.		
A.15.2.1	Cumplimiento de las políticas y normas de seguridad	*Control* Los directores deben asegurarse de que todos los procedimientos de seguridad dentro de su área de responsabilidad se realizan correctamente con el fin de cumplir las políticas y normas de seguridad.
A.15.2.2	Comprobación del cumplimiento técnico	*Control* Debe comprobarse periódicamente que los sistemas de información cumplen las normas de aplicación de la seguridad.
A.15.3 Consideraciones sobre la auditoria de los sistemas de información *Objetivo:* Lograr que el proceso de auditoria de los sistemas de información alcance la máxima eficacia con las mínimas interferencias.		
A.15.3.1	Controles de auditoria de los sistemas de información	*Control* Los requisitos y las actividades de auditoria que impliquen comprobaciones en los sistemas operativos deben ser cuidadosamente planificados y acordados para minimizar el riesgo de interrupciones en los procesos de empresariales.
A.15.3.2	Protección de las herramientas de auditoria de los sistemas de información	*Control* El acceso a las herramientas de auditoria de los sistemas de información debe estar protegido para evitar cualquier posible peligro o uso indebido.

ANEXO B (Informativo)

LOS PRINCIPIOS DE LA OCDE Y ESTA NORMA INTERNACIONAL

Los principios recogidos en las Directrices de la OCDE para la seguridad de los sistemas y redes de información se aplican a todas las políticas y a todos los niveles de operación que rigen la seguridad de los sistemas y redes de información. Esta norma internacional constituye el marco del sistema de gestión de la seguridad de la información para implementar algunos de los principios de la OCDE utilizando el modelo PDCA y los procesos descritos en los capítulos 4, 5, 6 y 8, según se indica en la tabla B.1.

Tabla B.1 – Los principios de la OCDE y el modelo PDCA

Principio de la OCDE	Proceso del SGSI y fase del PDCA correspondientes
Concienciación Los participantes deben concienciarse de la necesidad de garantizar la seguridad de los sistemas y redes de información y saber qué pueden hacer ellos para mejorar la seguridad	Esta actividad es parte de la fase **Hacer (Do)** (véanse 4.2.2 y **5.2.2**).
Responsabilidad Todos los participantes son responsables de la seguridad de los sistemas y redes de información.	Esta actividad es parte de la fase **Hacer (Do)** (véanse 4.2.2 y **5.1**).
Respuesta Los participantes deben actuar de forma oportuna y coordinada para prevenir, detectar y responder a los incidentes de seguridad.	Esto es en parte una actividad de supervisión de la fase **Verificar (Check)** (véase 4.2.3 y 6 a 7.3) y una actividad de respuesta de la fase **Actuar (Act)** (véase 4.2.4 y 8.1 a 8.3). También puede tener que ver con algunos aspectos de las fases **Planificar (Plan)** y **Verificar (Check)**.
Evaluación de riesgos Los participantes deben llevar a cabo evaluaciones de riesgos.	Esta actividad es parte de la fase **Planificar (Plan)** (véase 4.2.1) y la reevaluación del riesgo es parte de la fase **Verificar (Check)** (véase 4.2.3 y 6 a 7.3).
Diseño e implantación de la seguridad Los participantes deben incorporar la seguridad como un elemento esencial de los sistemas y redes de información	Una vez que finalizada la evaluación de riesgos, se seleccionan los controles para el tratamiento de los riesgos como parte de la fase **Planificar (Plan)** (véase 4.2.1). La fase **Hacer (Do)** (véase 4.2.2 y 5.2) comprende la implantación y el uso operativo de estos controles.
Gestión de la seguridad Los participantes deben adoptar criterios detallados de mantenimiento, revisión y auditoría.	La gestión del riesgo es un proceso que incluye la prevención, detección y respuesta a los incidentes, y la gestión continuada de la seguridad. Todos estos aspectos están comprendidos en las fases **Planificar (Plan), Hacer (Do), Verificar (Check)** y **Actuar (Act)**.
Reevaluación Los participantes deben revisar y reevaluar la seguridad de los sistemas y redes de información, y efectuar las modificaciones apropiadas de las políticas, prácticas, medidas y procedimientos de seguridad	La reevaluación de la seguridad de la información es parte de la fase **Verificar (Check)** (véase 4.2.3 y 6 a 7.3), en la cual deben llevarse a cabo revisiones periódicas para comprobar la eficacia del sistema de gestión de seguridad de la información, y la mejora de la seguridad es parte de la fase **Actuar (Act)** (véase 4.2.4 y 8.1 a 8.3).

ANEXO C (Informativo)

CORRESPONDENCIA ENTRE LAS NORMAS ISO 9001:2000, ISO 14001:2004 Y ESTA NORMA INTERNACIONAL

La tabla C.1 muestra la correspondencia entre las normas ISO 9001:2000 e ISO 14001:2004 y esta norma internacional.

Tabla C.1 – Correspondencia entre las normas ISO 9001:2000 e ISO 14001:2004 y esta norma internacional

Esta norma internacional	ISO 9001:2000	ISO 14001:2004
0 Introducción	**0 Introducción**	**Introducción**
0.1 Generalidades	0.1 Generalidades	
0.2 Enfoque del proceso	0.2 Enfoque del proceso	
	0.3 Relación con la Norma ISO 9004	
0.3 Compatibilidad con otros sistemas de gestión	0.4 Compatibilidad con otros sistemas de gestión	
1 Objeto y campo de aplicación	**1 Objeto y campo de aplicación**	**1 Objeto y campo de aplicación**
1.1 Generalidades	1.1 Generalidades	
1.2 Aplicación	1.2 Aplicación	
2 Normas para consulta	**2 Normas para consulta**	**2 Normas para consulta**
3 Términos y definiciones	**3 Términos y definiciones**	**3 Términos y definiciones**
4 Seguridad de la información	**4 Sistema de gestión de la calidad**	**4 Sistema de gestión de los requisitos del SGA**
4.1 Requisitos generales	4.1 Requisitos generales	4.1 Requisitos generales
4.2 Creación y gestión del SGSI		
4.2.1 Creación del SGSI		
4.2.2 Implantación y operación del SGSI		4.4 Implantación y operación
4.2.3 Supervisión y revisión del SGSI	8.2.3 Supervisión y medición de los procesos	4.5.1 Supervisión y medición
	8.2.4 Supervisión y medición del producto	
4.2.4 Mantenimiento y mejora del SGSI		
4.3 Requisitos de la documentación	4.2 Requisitos de documentación	
4.3.1 Generalidades	4.2.1 Generalidades	
	4.2.2 Manual de calidad	
4.3.2 Control de documentos	4.2.3 Control de documentos	4.4.5 Control de documentación
4.3.3 Control de registros	4.2.4 Control de registros	4.5.4 Control de registros

Esta norma internacional	ISO 9001:2000	ISO 14001:2004
5 Responsabilidad de la Dirección	**5 Responsabilidad de la Dirección**	
5.1 Compromiso de la Dirección	5.1 Compromiso de la Dirección	
	5.2 Orientación al cliente	
	5.3 Política de calidad	4.2 Política ambiental
	5.4 Planificación	4.3 Planificación
	5.5 Responsabilidad, autoridad y comunicación	
5.2 Gestión de los recursos	**6 Gestión de los recursos**	
5.2.1 Provisión de los recursos	6.1 Provisión de los recursos	
	6.2 Recursos humanos	
5.2.2 Concienciación, formación y competencia	6.2.2 Competencia, concienciación y formación	4.4.2 Competencia, formación, y concienciación
	6.3 Infraestructura	
	6.4 Entorno de trabajo	
6 Auditorías internas del SGSI	8.2.2 Auditoría interna	4.5.5 Auditoría interna
7 Revisión del SGSI por la Dirección	**5.6 Revisión por la Dirección**	**4.6 Revisión por la Dirección**
7.1 Generalidades	5.6.1 Generalidades	
7.2 Datos iniciales de la revisión	5.6.2 Datos iniciales de la revisión	
7.3 Resultados de la revisión	5.6.3 Resultados de la revisión	
8 Mejora del SGSI	**8.5 Mejora**	
8.1 Mejora continua	8.5.1 Mejora continua	
8.2 Acción correctiva	8.5.3 Acciones correctivas	4.5.3 Disconformidad, acción correctiva y acción preventiva
8.3 Acción preventiva	8.5.3 Acciones preventivas	
Anexo A Objetivos de control y controles		**Anexo A Guía de uso de esta norma internacional**
Anexo B Los principios de la OCDE y esta norma internacional		
Anexo C Correspondencia entre las Normas ISO 9001:2000 e ISO 14001:2004 y esta norma internacional	**Anexo A Correspondencia entre las Normas ISO 9001:2000 e ISO 14001:1996**	**Anexo B Correspondencia entre las Normas ISO 14001:2004 e ISO 9001:2000**

BIBLIOGRAFÍA

Publicaciones de normas

[1] ISO 9001:2000 *Sistemas de gestión de la calidad. Requisitos.*

[2] ISO/IEC 13335-1:2004 *Tecnologías de la información. Técnicas de seguridad. Gestión de la seguridad de las tecnologías de la información y las comunicaciones. Parte 1: Conceptos y modelos para la gestión de la seguridad de las tecnologías de la información y las comunicaciones.*

[3] ISO/IEC TR 13335-3:1998 *Tecnologías de la información. Directrices para la gestión de la seguridad de las TI. Parte 3: Técnicas para la gestión de la seguridad de las TI.*

[4] ISO/IEC TR 13335-4:2000 *Tecnologías de la información. Directrices para la gestión de la seguridad de las TI. Parte 4: Selección de salvaguardias.*

[5] ISO 14001:2004 *Sistemas de gestión ambiental. Requisitos y orientaciones de uso.*

[6] ISO/IEC TR 18044:2004 *Tecnologías de la información. Técnicas de seguridad. Gestión de incidentes de seguridad de la información.*

[7] ISO 19011:2002 *Directrices para auditorías de calidad o de sistemas de gestión ambiental.*

[8] ISO/IEC Guía 62:1996 *Requisitos generales para entidades encargadas de la evaluación y certificación o registro de sistemas de calidad.*

[9] ISO/IEC Guía 73:2002 *Gestión de riesgos. Vocabulario. Directrices de uso en normas.*

Otras publicaciones

[1] OCDE, *Directrices para la seguridad de los sistemas y redes de información. Hacia una cultura de la seguridad. París: OCDE, julio de 2002. www.oecd.org*

[2] NIST SP 800-30, *Guía de gestión de riesgos para sistemas de tecnologías de la información.*

[3] Deming W.E., *Out of the Crisis, Cambridge, Mass: MIT, Center for Advanced Engineering Study, 1986.*

AENOR Asociación Española de Normalización y Certificación

Dirección C Génova, 6
28004 MADRID-España

Teléfono 91 432 60 00

Fax 91 310 40 32