CERTIPROF CERTIFIED
ISO 27001 AUDITOR / LEAD AUDITOR
(I27001A/LA)

CERTIPROF CERTIFIED
CertiProf®
Professional Knowledge
ISO 27001 AUDITOR
I27001A

CERTIPROF CERTIFIED
CertiProf®
Professional Knowledge
ISO 27001 LEAD AUDITOR
I27001LA

CertiProf®
Professional Knowledge

www.certiprof.com

(I27001A/LA) VERSIÓN 072018

Esquema

Esquema

Esquema

Esquema

Esquema

Esquema

Objetivos

CertiProf®

Professional Knowledge

www.certiprof.com

Objetivos

- Alcance, propósito, términos y definiciones clave de la norma ISO/IEC 27001 y cómo puede ser utilizada.
- Requisitos de definición del alcance y aplicabilidad.
- Uso de controles para mitigar los riesgos de seguridad de la información.
- Certificación Profesional.

Introducción y Antecedentes

Introducción

- ISO/IEC 27001.
- Historia de la norma.
- Estado actual.
- Definiciones.

La norma ha sido diseñada para *"proporcionar los requisitos para establecer, implementar, mantener y mejorar continuamente un sistema de gestión de seguridad de la información".*

La norma ***"puede ser utilizada por partes internas y externas para evaluar la capacidad de la organización para cumplir con sus propios requisitos de seguridad de la información".***

La norma también incluye *"requisitos para la evaluación y el tratamiento de los riesgos en la seguridad de la información a la medida de las necesidades de la organización. Los requisitos establecidos en esta Norma Internacional son genéricos y se pretende que sean aplicables a todas las organizaciones, sin importar su tipo, tamaño o naturaleza".*

Historia de la Norma

- Código de Práctica.
- BS7799.
- BS7799 Ver 2.
- ISO 17799.
- BS7799 Parte 2.
- ISO 17799 Actualización.
- ISO 27001.
- ISO 27002.
- Desarrollo de la Serie y Actualizaciones.

ISO/IEC 27001:2013 - Estructura

La nueva estructura refleja la estructura de otras normas nuevas de gestión, tales como ISO 9000, ISO 20000 e ISO22301, que ayudan a las organizaciones a cumplir con varias normas.

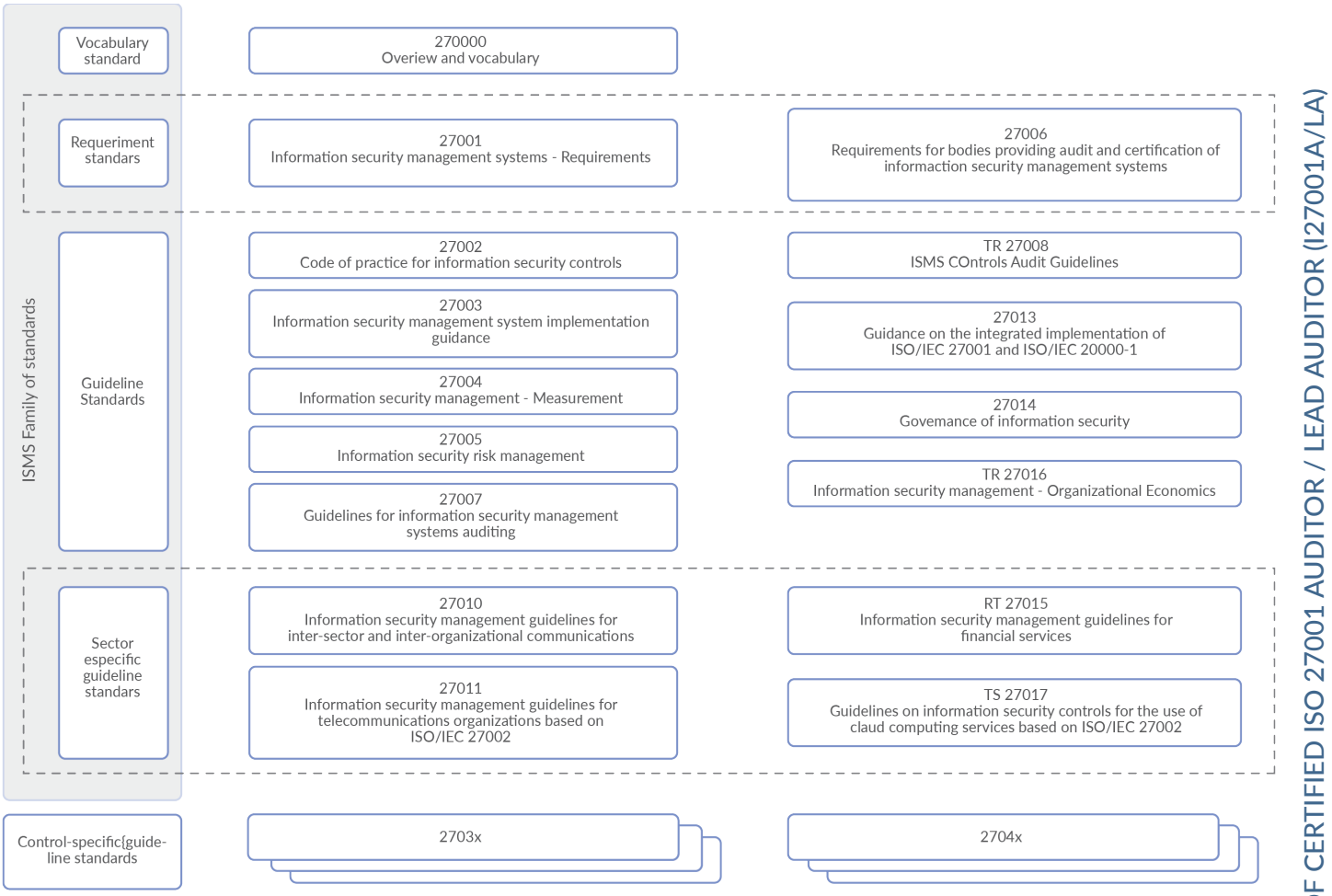
Los Anexos B y C del 27001: 2005 han sido eliminados.

Hay una sección adicional sobre la subcontratación.

El ciclo PDCA de mejora continua ya no es central. La Evaluación del riesgo más importante del contexto organizacional cambió.

Hay 114 controles en 14 grupos en comparación con los 133 controles en 11 grupos en la versión de 2005.

ISO 27000 Familia de Normas



Conceptos Claves

¿Qué es un SGSI?

Información y Principios Generales

Un **SGSI** (Sistema de Gestión de la Seguridad de la Información) consiste en un conjunto de políticas, procedimientos, guías y sus recursos y actividades asociados, que son gestionados de manera colectiva por una organización.

Un **SGSI** es un enfoque sistemático para establecer, implementar, operar, monitorizar, revisar, mantener y mejorar la seguridad de la información de una organización para alcanzar los objetivos de negocio.

Este enfoque está basado en una apreciación del riesgo y en los niveles de aceptación del riesgo de la organización diseñados para tratar y gestionar con eficacia los riesgos.

El análisis de los requisitos para la protección de los activos de la información y la aplicación de controles adecuados para garantizar la protección de estos activos de información, según sea necesario, contribuye a la exitosa implementación de un **SGSI**.

Los siguientes principios fundamentales también pueden contribuir a la implementación exitosa de un **SGSI**:

a) La conciencia de la necesidad de seguridad de la información;

b) La asignación de responsabilidades en seguridad de la información;

c) La incorporación del compromiso de la Dirección y los intereses de las partes interesadas;

d) La mejora de los valores sociales;

e) Apreciaciones de riesgo para determinar los controles adecuados para alcanzar niveles aceptables de riesgo;

f) La seguridad incorporada como un elemento esencial de los sistemas y redes de información;

g) La prevención y detección activas de incidentes de seguridad de la información;

h) El garantizar una aproximación exhaustiva a la gestión de la seguridad de la información; y

i) La evaluación continua de la seguridad de la información y la realización de modificaciones cuando corresponda.

Conceptos Claves

La Seguridad de la Información

La seguridad de la información incluye tres dimensiones principales: **la confidencialidad, la disponibilidad y la integridad**. Con el objetivo de garantizar el éxito empresarial sostenido así como su continuidad, y minimizar impactos, la seguridad de la información conlleva la aplicación y la gestión de medidas de seguridad adecuadas que implican la consideración de una amplia gama de amenazas.

La seguridad de la información se consigue mediante la implementación de un conjunto de controles aplicables, seleccionados a través del proceso de gestión de riesgo que se haya elegido y gestionado por medio de un **SGSI**, empleando políticas, procesos, procedimientos, estructuras organizativas, software y hardware para proteger los activos de información identificados.

Estos controles necesitan ser especificados, implementados, monitorizados, revisados y mejorados cuando sea necesario, para garantizar que la seguridad y los objetivos de negocio y de seguridad específicos se cumplan. Estos controles de seguridad de la información deben integrarse de forma coherente con los procesos de negocio de una organización.

El Sistema de Gestión

Un sistema de gestión utiliza un marco de recursos para alcanzar los objetos de una organización. El sistema de gestión incluye la estructura organizativa, las políticas, la planificación de actividades, responsabilidades, prácticas, procedimientos, procesos y recursos.

En términos de seguridad de la información, un sistema de gestión permite a una organización:

a) Satisfacer los requisitos de seguridad de los clientes y otras partes interesadas;

b) Mejorar los planes y actividades de la organización;

c) Cumplir con los objetivos de seguridad de información de la organización

d) Cumplir con las regulaciones, leyes y obligaciones sectoriales; y

e) Gestionar los activos de información de una manera organizada que facilita la mejora continua y la adaptación a las actuales metas de la organización y a su entorno.

Factores Críticos de Éxito de una SGSI

Un gran número de factores son fundamentales para la implementación exitosa de un **SGSI** que permite a una organización cumplir con sus objetivos de negocio. Algunos ejemplos de factores críticos de éxito son:

a) Que la política, los objetivos y actividades de seguridad de la información estén alineadas con los objetivos;

Conceptos Claves

b) Un enfoque y un marco para el diseño, ejecución, seguimiento, mantenimiento y mejora de la seguridad de la información en consonancia de la cultura de la organización.

c) El apoyo visible y el compromiso de todos los niveles de la Dirección, especialmente de alta Dirección;

d) EL conocimiento y entendimiento de los requisitos de protección de los activos de información obtenido mediante la aplicación de la gestión del riesgo de la seguridad de la información (véase la Norma ISO/IEC 27005);

e) Un programa efectivo de concienciación, formación y educación sobre seguridad de la información, informando a todos los empleados y otras partes pertinentes de sus obligaciones en seguridad de la información establecidas en las políticas de seguridad de la información, normas, etc., y motivarlos a actuar en consecuencia;

f) Un proceso eficaz de gestión de incidentes de seguridad de la información;

g) Un enfoque efectivo de gestión de la continuidad del negocio; y

h) Un sistema de medición utilizado para evaluar el desempeño en la gestión de la seguridad de la información y para proporcionar sugerencias de mejora.

Un **SGSI** aumenta la probabilidad de que una organización alcance de forma coherente los factores críticos de éxito para proteger sus activos de información.

Beneficios de la Familia de Normas SGSI

Los beneficios de implementar un **SGSI** producirán principalmente una reducción de los riesgos asociados a la seguridad de la información (es decir, reduciendo la probabilidad y/o el impacto causado por los incidentes de seguridad de la información). De una forma más específica los beneficios que para una organización produce la adopción exitosa de la familia de normas **SGSI** son:

a) Un apoyo al proceso de especificar, implementar, operar y mantener un SGSI, global, eficiente en costes, integrado y alineado que satisfaga las necesidades de la organización en diferentes operaciones y lugares;

b) Una ayuda para la dirección en la estructura de su enfoque hacia la gestión de la seguridad de la información, en el contexto de la gestión y gobierno del riesgo corporativo, incluidas las acciones de educación y formación en una gestión holística de la seguridad de la información a los propietarios del negocio y del sistema;

Conceptos Claves

c) La promoción de buenas prácticas de seguridad de la información, aceptadas a nivel mundial, de una manera no preceptiva, dando a las organizaciones la flexibilidad para adoptar y mejorar los controles aplicables, respetando sus circunstancias específicas y para mantenerlos de cada a futuros cambios internos y externos; y

d) Disponer de un lenguaje común y una base conceptual para seguridad de la información, haciendo más fácil confiar a los socios de un negocio que este en conforme a un SGSI, especialmente si requieren la certificación conforme a la Norma ISO/IEC 27001 por un organismo de certificación acreditado;

e) Aumentar la confianza en la organización por las partes interesadas;

f) Satisfacer necesidades y expectativas sociales; y

g) Una más eficaz gestión desde un punto de vista económico de las inversiones en seguridad de la información.

3. Términos y Definiciones

CertiProf®

Professional Knowledge

www.certiprof.com

3.1 Control de Acceso

Medios para asegurar que el acceso a los activos está autorizado y restringido en función de los requisitos de negocio y de seguridad.

3.2 Modelo Analítico

Algoritmo o cálculo que combina una o más **medidas básicas** (3.10) o **derivadas** (3.22) siguiendo los criterios de decisión a las mismas.

3.3 Ataque

Tentativa de destruir, exponer, alterar, inhabilitar, robar o acceder sin autorización o hacer un uso no autorizado de un activo.

3.4 Atributo

Propiedad característica de un **objeto** (3.55) que es cuantitativa o cualitativamente distinguible por medios humanos o automáticos.

[Adaptable de ISO/IEC 1539:2007]

3.5 Auditoría

Proceso (3.61) sistemático, independiente y documentado para obtener evidencias de auditoria y evaluarlas de manera objetiva con el fin de determinar el grado en el que se cumplen los criterios de auditoría.

NOTA 1: Una auditoría puede ser interna (de primera parte), o externa (de segunda o tercera parte), y puede ser combinada (combinando dos o más disciplinas).

NOTA 2: "*Evidencia de auditoría*" y "*criterios de auditoría*" se definen en la norma ISO 19011.

3.6 Alcance de la Auditoría

Extensión y límites de una **auditoría** (3.5).

[ISO 19011:2011]

3.7 Autenticación

Aportación de garantías de que son correctas las características que una entidad reivindica para sí misma.

3.8 Autenticidad

Propiedad consistente en que una entidad es lo que dice ser.

3.9 Disponibilidad

Propiedad de ser accesible y estar listo para su uso o demanda de una entidad autorizada.

3.10 Medida Básica

Medida (3.47) definida por medio de un **atributo** (3.4) y el método para cuantificarlo.

[ISO/IEC 1539:2007]

NOTA: Una medida básica es funcionalmente independiente de otras medidas.

3.11 Competencia

Capacidad para aplicar conocimientos y habilidades con el fin de lograr los resultados previstos.

3.12 Confidencialidad

Propiedad de la información por la que se mantiene inaccesible y no se revela a individuos, entidades o **procesos** (3.61) no autorizados.

3.13 Conformidad

Cumplimiento de un **requisito** (3.63).

3.14 Consecuencia

Resultado de un **suceso** (3.25) que afecta a los **objetivos** (3.56).

[Guía ISO 73:2009]

NOTA 1: Un suceso puede conducir a una serie de consecuencias.

NOTA 2: Una consecuencia puede ser cierta o incierta y normalmente es negativa en el contexto de la seguridad de la información.

NOTA 3: Las consecuencias se puede expresar de forma cualitativa o cuantitativa.

NOTA 4: Las consecuencias iniciales puede convertirse en reacciones en cadena.

3.15 Mejora Continua

Actividad recurrente para mejorar el **desempeño** (3.59).

3.16 Control

Medida que modifica un **riesgo** (3.68).

[ISO Guía 73:2090]

NOTA 1: Los controles incluyen cualquier proceso, política, dispositivo, práctica, u otras acciones que modifiquen un riesgo.

NOTA 2: Los controles no siempre pueden proporcionar el efecto de modificación previsto o asumirlo.

3.17 Objeto de Control

Declaración que describe lo que se quiere lograr como resultado de la implementación de **controles** (3.16).

3.18 Corrección

Acción para eliminar una **no conformidad** (3.53) detectada.

3.19 Acción Correctiva

Acción para eliminar la causa de una **no conformidad** (3.53) y prevenir que vuelva a ocurrir.

3.20 Datos

Conjunto de valores asociados a **medidas básicas** (3.10), **medida derivadas** (3.22) y/o **indicadores** (3.30).

[ISO/IEC 15939:2007]

NOTA: Esta definición solo se aplica en el contexto de la Norma ISO/IEC 27004:2009.

3.21 Criterios de Decisión

Umbrales, objetivos o patrones que se utilizan para determinar la necesidad de una acción o de una mayor investigación, o para describir el nivel de confianza en un resultado determinado.

[ISO/IEC 15939:2007]

3.22 Medida Derivada

Medida (3.47) que se define en función de dos o más valores de **medidas básicas** (3.10).

[ISO/IEC 15939:2007]

3.23 Información Documentada

Información que una **organización** (3.57) tiene que controlar y mantener, y el medio en el que está contenida.

NOTA 1: La información documentada puede estar en cualquier formato y medio, y puede provenir de cualquier fuente.

NOTA 2: La información documentada puede hacer referencia a:
- El **sistema de gestión** (3.46), incluidos los **procesos** (3.61) relacionados.
- La información creada para que la organización opere (documentación).
- La evidencia de los resultados alcanzados (registros).

3.24 Eficacia

Grado en el cual se realizan las actividades planificadas y se logran los resultados planificados.

3.25 Evento

Ocurrencia o cambio de un conjunto particular de circunstancias.

[Equivalente a "suceso" en Guía ISO 73:2009]

NOTA 1: Un evento puede ser único o repetirse, y se puede deber a varias causas.

NOTA 2: Un evento puede consistir en algo que no se llega a producir.

NOTA 3: Algunas veces, un evento se puede calificar como un "incidente" o un "accidente".

3.27 Contexto Externo

Entorno externo en el que la organización busca alcanzar sus objetivos.

[Guía ISO 73:2009]

NOTA: El entorno externo puede incluir:

- El entorno cultural, social, político, legal, regulatorio, financiero, tecnológico, económico, natural y competitivo, a nivel internacional, nacional, regional o local.
- Los factores y las tendencias que tengan impacto sobre los **objetivos** (3.56) de la **organización** (3.57), y
- Las relaciones con las **partes interesadas** externas (3.82), sus percepciones y sus valores.

3.28 Gobernanza de la Seguridad de la Información

Conjunto de principios y **procesos** (3.61) mediante los cuales una **organización** (3.57) dirige y supervisa las actividades relacionadas con la seguridad de la información.

3.29 Órgano de Gobierno

Conjunto de personas que responden y rinden cuentas del **desempeño** (3.59) de la **organización** (3.57).

NOTA: En algunas jurisdicciones, el órgano de gobierno puede ser el consejo de administración.

3.30 Indicador

Medida (3.47) que proporciona una estimación o una evaluación de determinados **atributos** (3.4) usando un **modelo analítico** (3.2) para satisfacer unas determinadas **necesidades de información** (3.31).

3.31 Necesidades de la Información

Conocimiento necesario para gestionar los objetivos, las metas, el riesgo y los problemas.

[ISO/IEC 15939:2007]

3.32 Recursos (*instalaciones*) de Tratamiento de Información

Cualquier sistema de tratamiento de la información, servicios o infraestructura, o los lugares físicos que los albergan.

3.33 Seguridad de la Información

Preservación de la **confidencialidad** (3.12), la **integridad** (3.40) y la **disponibilidad** (3.9) de la información.

NOTA: Pudiendo, además, abarcar otras propiedades, como la **autenticidad** (2.8), la responsabilidad, el **no repudio** (3.54) y la **fiabilidad** (3.62).

3.34 Continuidad de la Seguridad de la Información

Procesos (3.61) y procedimientos para asegurar la continuidad de las actividades relacionadas con la **seguridad de la información** (3.33).

3.35 Evento o Suceso de Seguridad de la Información

Ocurrencia detectada en el estado de un sistema, servicio o red que indica una posible violación de la política de seguridad de la información, un fallo de los controles o una situación desconocida hasta el momento y que puede ser relevante para la seguridad.

3.36 Incidente de Seguridad de la Información

Evento singular o serie de **eventos de la seguridad de la información** (3.35), inesperados o no deseados, que tienen una probabilidad significativa de comprometer las operaciones del negocio y de amenazar la **seguridad de la información** (3.33).

3.37 Gestión de Incidentes de Seguridad de la Información

Procesos (3.61) para la detección, notificación, evaluación, respuesta, tratamiento, y aprendizaje de incidentes de la **seguridad de la información** (3.36).

3.38 Colectivo que Comparte Información

Grupo de organizaciones que acuerdan compartir información.

NOTA: Una organización puede ser un individuo.

3.39 Sistema de Información

Aplicaciones, servicios, activos de tecnologías de la información y otro compuestos para manejar información.

3.40 Integridad

Propiedad de exactitud y completitud.

3.41 Parte Interesada

Persona u **organización** (3.57) que puede afectar, estar afectada, o percibir que está afectada por una decisión o actividad.

3.42 Contexto Interno

Entorno interno en el que la organización busca alcanzar sus objetivos.

Guía ISO 73:2009]

NOTA: El contexto interno puede incluir:

- El gobierno, la estructura de la organización, las funciones y la obligación de rendir cuenta,
- Las políticas, los objetivos y las estrategias que se establecen para conseguirlo.
- Las capacidades, entendidas en términos de recursos y conocimientos (por ejemplo, capital, tiempo, personas, procesos, sistemas y tecnologías),
- Los sistemas de información, los flujos de información y los procesos de toma de decisiones (tanto formales como informales),
- Las relaciones con, y las percepciones y los valores de las partes interesadas internas,
- La cultura de la organización,
- Las normas, las directrices y los modelos adoptados por la organización, y
- La forma y amplitud de las relaciones contractuales.

3.43 Proyecto del SGSI

Actividades estructurales llevadas a cabo por una **organización** (3.57) para implementar un SGSI.

3.44 Nivel de Riesgo

Magnitud de un **riesgo** (3.68) o combinación de riesgos, expresados en términos de la combinación de las **consecuencias** (3.14) y de su **probabilidad** (3.45).

[Guía ISO 73:2009]

3.45 Probabilidad (*likehood*)

Posibilidad de que algún hecho se produzca.

[Guía ISO 73:2009]

3.46 Sistema de Gestión

Conjunto de elementos de una organización (3.57) interrelacionados o que interactúan para establecer políticas (3.60), objetivos (3.56) y procesos (3.61) para lograr estos objetivos.

NOTA 1: Un sistema de gestión puede tratar una sola disciplina o varias disciplinas.

NOTA 2: Los elementos del sistema incluyen la estructura de la organización, los roles y las responsabilidades, la planificación, la operación, etc.

NOTA 3: El alcance de un sistema de gestión puede incluir la totalidad de la organización, funciones especificas e identificadas de la organización, secciones especificas e identificadas de la organización, o una o más funciones dentro de un grupo de organizaciones.

3.47 Medida

Variable a la que se le asigna un valor como resultado de una **medición** (3.48).

[ISO/IEC 15939:2007]

NOTA: El termino "medidas" se utiliza para hacer referencia conjuntamente a medidas de base, de las derivadas, e indicadores.

3.48 Medición

Procesos (3.61) para determinar un valor.

NOTA: En el contexto de **seguridad de la información** (3.33), el proceso para determinar un valor requiere información sobre la **eficacia** (3.24) de un **sistema de gestión** (3.46) de seguridad de la información y sus correspondientes **controles** (3.16) utilizando un **método de medición** (3.50), una función de **medición** (3.49), un **modelo analítico** (3.2), y unos **criterios de decisión** (3.21).

3.49 Función de Medición

Algoritmo o cálculo realizado para combinar dos o más **medidas básicas** (3.1).

[ISO/IEC 1593:2007]

3.50 Método de Medición

Secuencia lógica de operaciones, descritas genéricamente, utilizada en la cuantificación de un **atributo** (3.4) con respecto a una **escala** (3.80) especificada.

[ISO/IEC 1593:2007]

NOTA: El tipo de método de medición depende de la naturaleza de las operaciones utilizadas para cuantificar un atributo. Se pueden distinguir dos tipo:

- Subjetivos: La cuantificación se basa en el juicio humano.
- Objetiva: La cuantificación se basa en reglas métricas.

3.51 Resultado de las Mediciones

Uno o más **indicadores** (3.30) y sus correspondientes interpretaciones que aborda una necesidad de **información** (3.31).

3.52 Supervisión, Seguimiento o Monitorización (*monitoring*)

Determinación del estado de un sistema, un **proceso** (3.61) o una actividad.

NOTA: Para determinar el estado puede ser necesario verificar, supervisar u observar en forma crítica.

3.53 No Conformidad

Incumplimiento de un **requisito** (3.63).

3.54 No Repudio

Capacidad para corroborar que es cierta la reivindicación de que ocurrió un cierto suceso o se realizó una cierta acción por parte de las entidades que lo originaron.

3.55 Objeto

Elemento caracterizado por medio de la **medición** (3.48) de sus **atributos** (3.4).

3.56 Objetivo

Resultado a lograr

NOTA 1: Un objetivo puede ser estratégico, táctico u operativo.

NOTA 2: Los objetivos pueden referirse a diferentes disciplinas (como financieras, de seguridad y salud y ambientales) y se pueden aplicar en diferentes niveles (como estratégicos, para toda la organización, para proyectos, productos y **procesos** (3.61)).

NOTA 3: Un objetivo se puede expresar de otras maneras, por ejemplo, como un resultado previsto, un propósito, un criterio operativo, un objetivo de seguridad de la información, o mediante el uso de términos con un significado similar (por ejemplo, finalidad o meta).

NOTA 4: En el contexto de sistemas de gestión de la seguridad de la información, la organización establece los objetivos de la seguridad de la información, en concordancia con la política de seguridad de la información, para lograr resultados específicos.

3.57 Organización

Persona o grupo de personas que tienen sus propias funciones con responsabilidades, autoridades y relaciones para el logro de sus **objetivos** (3.56).

NOTA: El concepto de organización incluye, pero no se limita a, empresarios unipersonales, empresas, corporaciones, firmas, autoridades, asociaciones, etc., en si mismas, parcialmente o grupo de ellas, sean públicas o privadas.

3.58 Contratar Externamente (*verbo*)

Establecer un acuerdo mediante el cual una **organización** (3.57) externa realiza parte de una función o proceso (3.61) de una organización.

NOTA: Una organización externa está fuera del alcance del **sistema de gestión** (3.46), aunque la función o proceso contratado externamente forme parte del alcance.

3.59 Desempeño

Resultado medible

NOTA 1: El desempeño se puede relacionar con hallazgos cuantitativos o cualitativos.

NOTA 2: El desempeño se puede relacionar con la gestión de actividades, **procesos** (3.61), productos (incluidos servicios), sistemas u **organizaciones** (3.57).

3.60 Política

Intenciones y dirección de una **organización** (3.57), como las expresa formalmente su **alta dirección** (3.84).

3.61 Proceso

Conjunto de actividades interrelacionadas o que interactúan, que transforma elementos de entrada en elementos de salida.

3.62 Fiabilidad

Propiedad relativa a la consistencia en el comportamiento y en los resultados deseados.

3.63 Requisito

Necesidad o expectativa que está establecida, generalmente implícita u obligatoria.

NOTA 1: "Generalmente implícita" significa que es una costumbre o práctica común en la organización y en las partes interesadas, que la necesidad o expectativa que se considera está implícita.

NOTA 2: Un requisito especifico es el que está declarado, por ejemplo, en información documentada.

3.64 Riesgo Residual

Riesgo (3.68) remanente después del **tratamiento del riesgo** (3.79).

NOTA 1: El riesgo residual puede contener riesgos no identificados.

NOTA 2: El riesgo residual también se puede conocer como "riesgo retenido".

3.65 Revisión

Actividad que se realiza para determinar la idoneidad, la adecuación y la **eficacia** (3.24) del tema estudiado para conseguir los objetivos establecidos.

[Guía ISO 73:2009]

3.66 Objeto en Revisión

Elemento especifico que está siendo revisado.

3.67 Objetivo de la Revisión

Declaración que describe lo que se quiere lograr como resultado de una revisión.

3.68 Riesgo

Efecto de la incertidumbre sobre la consecución de los objetivos.

[Guía ISO 73:2009]

NOTA 1: Un efecto es una desviación, positiva y/o negativa, respecto a lo provisto.

NOTA 2: La incertidumbre es el estado, incluso parcial, de deficiencia en la información relativa a la compresión o al conocimiento de un **suceso** (3.25), de sus **consecuencias** (3.14) o de su **probabilidad** (3.45).

NOTA 3: Con frecuencia, el riesgo se caracteriza por referencia a **sucesos** (3.25) potenciales y a sus **consecuencias** (3.14) o una combinación de ambos.

NOTA 4: Con frecuencia, el riesgo se expresa en términos de combinación de las **consecuencias** (3.14) de un suceso (incluyendo los cambios en las circunstancias) y de su **probabilidad** (3.45).

NOTA 5: En el contexto de sistema de gestión de la seguridad de la información, los riesgos de seguridad de la información se pueden expresas como el efecto de la incertidumbre sobre los objetivos de seguridad de la información.

NOTA 6: El riesgo de seguridad de la información se relaciona con la posibilidad de que las **amenazas** (3.83) exploten **vulnerabilidades** (3.89) de un activo o grupo de activos de información y causen daño a una organización.

3.69 Aceptación del Riesgo

Decisión informada en favor de tomar un riesgo (3.68) particular.

[Guía ISO 73:2009]

NOTA 1: La aceptación del riesgo puede tener lugar sin que exista tratamiento del **riesgo** (3.79) o durante el proceso de tratamientos del riesgo.

NOTA 2: Los riesgos aceptados son objeto de **seguimiento** (3.52) y **revisión** (3.65).

3.70 Análisis del Riesgo

Proceso que permite comprender la **naturaleza del riesgo** (3.68) y determinar el nivel de **riesgo** (3.44).

[Guía ISO 73:2009]

NOTA 1: El análisis del riesgo proporciona las bases para la **evaluación del riesgo** (3.74) y para tomar las decisiones relativas al **tratamiento del riesgo** (3.79).

NOTA 2: El análisis del riesgo incluye la estimación del riesgo.

3.71 Apreciación del Riesgo

Proceso (3.61) global que comprende la **identificación del riesgo** (3.75), el **análisis del riesgo** (3.70) y la **evaluación del riesgo** (3.74).

[Guía ISO 73:2009]

3.72 Comunicación y Consulta del Riesgo

Procesos iterativos y continuos que realiza una organización para proporcionar, compartir u obtener información ya para establecer el diálogo con las **parte interesadas** (3.82), en relación con la gestión del **riesgo** (3.67).

[Guía ISO 73:2009]

NOTA 1: La información puede corresponder a la existencia, la naturaleza, la forma, la probabilidad, la importancia, la evaluación, la aceptabilidad y el tratamiento de la gestión del riesgo.

NOTA 2: La consulta constituye un proceso de comunicación informada de doble sentido entre una organización y sus parte interesadas, sobre una cuestión antes de tomar una decisión o determinar una orientación sobre dicha cuestión. La consulta es:

- Un proceso que impacta sobre una decisión a través de la influencia más que por la autoridad, y
- Una contribución para una toma de decisión, u no una toma de decisión conjunta.

3.73 Criterios de Riesgo

Términos de referencia respecto a los que se evalúa la importancia de un **riesgo** (3.68).

[Guía ISO 73:2009]

NOTA 1: Los criterios de riesgo se basan en los objetivos de la organización y en el contexto interno y externo.

NOTA 2: Los criterios de riesgo se puede obtener de normas, leyes, políticas y otro requisitos.

3.74 Evaluación del Riesgo

Proceso (3.61) de comparación de los resultados del **análisis de riesgo** (3.70) con los **criterios de riesgo** (3.73) para determinar si el **riesgo** (3.68) y/o su magnitud son aceptables o tolerables.

[Guía ISO 73:2009]

NOTA: La evaluación del riesgo ayuda a la toma de decisiones sobre el **tratamiento del riesgo** (3.79).

3.75 Identificación del Riesgo

Proceso que comprende la búsqueda, el reconocimiento y la descripción de los **riesgos** (3.68).

[Guía ISO 73:2009]

NOTA 1: La identificación del riesgo implica la identificación de las fuentes de los riesgos, los sucesos, sus causas y sus consecuencias potenciales.

NOTA 2: La identificación del riesgo puede implicar datos históricos, análisis teóricos, opiniones informadas y de expertos, así como necesidades del las partes interesadas.

3.76 Gestión del Riesgo

Actividades coordinadas para dirigir y controlar una **organización** (3.57) en lo relativo al **riesgo** (3.68).

[Guía ISO 73:2009]

3.77 Proceso de Gestión del Riesgo

Aplicación sistemática de políticas, procedimientos y prácticas de gestión a las actividades de comunicación, consulta, establecimiento del contexto, e identificación, análisis, evaluación, tratamiento, seguimiento y revisión del riesgo (3.68).

[Guía ISO 73:2009]

NOTA: La norma ISO/IEC 27005 utiliza el término "proceso" para describir la gestión integral del riesgo. Los elementos dentro del proceso de gestión del riesgo se denominan "actividades".

3.78 Dueño del Riesgo

Persona o entidad que tiene la responsabilidad y autoridad para gestionar un **riesgo** (3.68).

[Guía ISO 73:2009]

3.79 Tratamiento del Riesgo

Proceso (3.61) destinado a modificar el riesgo (3.68).

[Guía ISO 73:2009]

NOTA 1: El tratamiento del riesgo puede implicar:

- Evitar el riesgo, decidiendo no iniciar o continuar con la actividad que motiva el riesgo.
- Aceptar o aumentar el riesgo con el objeto de buscar una oportunidad.
- Eliminar la fuente de riesgo.
- Cambiar la probabilidad.
- Cambiar las consecuencias.
- Compartir el riesgo con otra u otras partes (incluyendo los contratos y la financiación del riesgo), y
- Mantener el riesgo en base a una decisión informada.

NOTA 2: Los tratamientos del riesgo que conducen a consecuencias negativas, en ocasiones se citan como "mitigación del riesgo", "eliminación del riesgo", "prevención del riesgo" y "reducción del riesgo".

NOTA 3: El tratamiento del riesgo puede originar nuevos riesgos o modificar los riesgos existentes.

3.80 Escala

Conjunto ordenado de valores, continuo o discreto, o un conjunto de categorías a las que se asigna el **atributo** (3.4).

[ISO/IEC 15939:2007]

NOTA: El tipo de escala depende de la naturaleza de la relación entre los valores de la escala. Comúnmente se identifican cuatro tipos de escala:

- Nominal: Los valores de medición son categorías.
- Ordinal: Los valores de medición son categorías ordenadas.
- Intervalo: Los valores de las mediciones se ajustan a rangos de valores cuantitativos del atributo.
- Proporción: Los valores de las mediciones son relativos y proporcionales al valor de otro atributo; correspondiendo el valor cero al valor cero del atributo.

Estos son solo ejemplos de tipos de escala.

3.81 Norma de Implementación de la Seguridad

Documento que especifica las formas autorizadas para satisfacer las necesidades de seguridad.

3.82 Parte Interesada

Persona u organización que puede afectar, estar afectada, o percibir que está afectada por una decisión o actividad.

[ISO/IEC 73:2009]

3.84 Alta Dirección

Persona o grupo de personas que dirigen y controlan una **organización** (3.57) al más alto nivel.

NOTA 1: La alta dirección tiene el poder para delegar autoridad y proporcionar recursos dentro de la organización.

NOTA 2: Si el alcance del **sistema de gestión** (3.46) comprende solo una parte de una organización, entonces "alta dirección" se refiere a quienes dirigen y controlan esa parte de la organización.

3.85 Entidad de Confianza para la Comunicación de la Información

Organización independiente que sustenta el intercambio de información dentro de un colectivo que comparte información.

3.86 Unidad de Medida

Cantidad concreta, definida y adoptada por convenio, con la cual se comparan otras cantidades de la misma naturaleza a fin de expresar su magnitud en relación a dicha cantidad.

[ISO/IEC 15939:2007]

3.87 Validación

Confirmación mediante la aportación de evidencia objetiva de que se han cumplido los requisitos para una utilización o aplicación específica prevista.

[ISO/IEC 9000:2005]

3.88 Verificación

Confirmación mediante la aportación de evidencia objetiva de que se han cumplido los requisitos especificados.

[ISO/IEC 9000:2007]

3.89 Vulnerabilidad

Debilidad de un activo o de un control (3.16) que puede ser explotada por una o más **amenazas** (3.83).

4. Contexto de la Organización

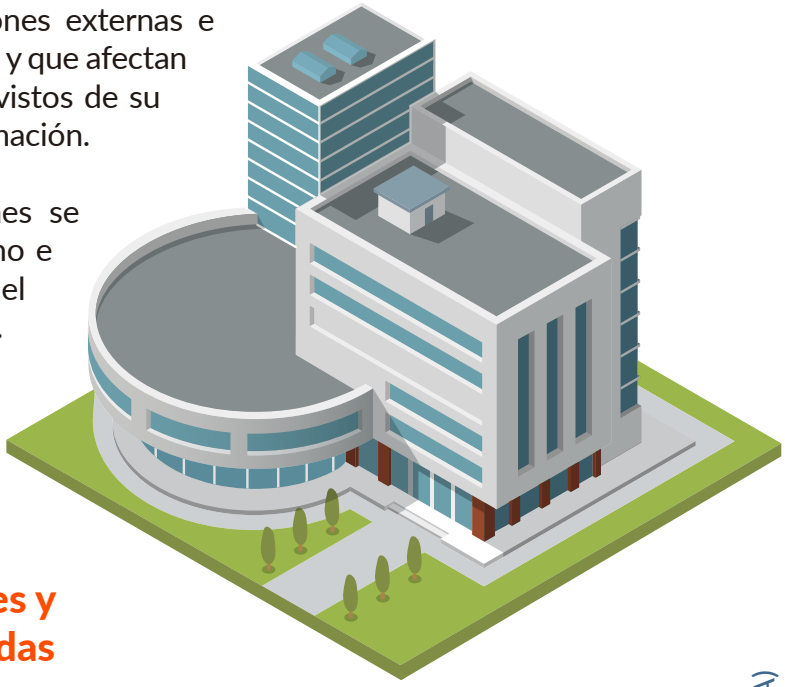
CertiProf®

Professional Knowledge

www.certiprof.com

4.1 Comprensión de la Organización y de su Contexto

La organización debe determinar las cuestiones externas e internas que son pertinentes para su propósito y que afectan a su capacidad para lograr los resultados previstos de su sistema de gestión de la seguridad de la información.



NOTA: La determinación de estas cuestiones se refiere al establecimiento del contexto externo e interno de la organización considerando el apartado 5.3 de la Norma ISO 31000:2009[5].

4.2 Comprensión de las Necesidades y Expectativas de las Partes Interesadas

La organización debe determinar:

a) Las partes interesadas que son relevantes para el sistema de gestión de la seguridad de la información; y

b) Los requisitos de estas partes interesadas que son relevantes para la seguridad de la información.

NOTA: Los requisitos de las partes interesadas pueden incluir requisitos legales y regulatorios, así como obligaciones contractuales.

4.3 Determinación del Alcance del Sistema de Gestión de la Seguridad de la Información

La organización debe determinar los límites y la aplicabilidad del sistema de gestión de la seguridad de la información para establecer su alcance.

Cuando se determina este alcance, la organización debe considerar:

a) Las cuestiones externas e internas referidas en el apartado **4.1**;

b) Los requisitos referidos en el apartado **4.2**;

c) Las interfaces y dependencias entre las actividades realizadas por la organización y las que se llevan a cabo por otras organizaciones.

El alcance debe estar disponible como información documentada.

4.4 Sistema de Gestión de la Seguridad de la Información

La organización debe establecer, implementar, mantener y mejorar de manera continua un sistema de gestión de la seguridad de la información, de acuerdo con los requisitos de esta norma internacional.

5. Liderazgo

CertiProf®

Professional Knowledge

www.certiprof.com

5.1 Liderazgo y Compromiso

La alta dirección debe demostrar liderazgo y compromiso con respecto al sistema de gestión de la seguridad de la información:

a) Asegurando que se establecen la política y los objetivos de seguridad de la información y que estos sean compatibles con la dirección estratégica de la organización;

b) Asegurando la integración de los requisitos del sistema de gestión de la seguridad de la información en los procesos de la organización;

c) Asegurando que los recursos necesarios para el sistema de gestión de la seguridad de la información estén disponibles;

d) Comunicando la importancia de una gestión de la seguridad de la información eficaz y conforme con los arequisitos del sistema de gestión de la seguridad de la información;

e) Asegurando que el sistema de gestión de la seguridad de la información consigue los resultados previstos;

f) Dirigiendo y apoyando a las personas, para contribuir a la eficacia del sistema de gestión de la seguridad de la información;

g) Promoviendo la mejora continua; y

h) Apoyando otros roles pertinentes de la dirección, para demostrar su liderazgo aplicado a sus áreas de responsabilidad.

5.2 Política

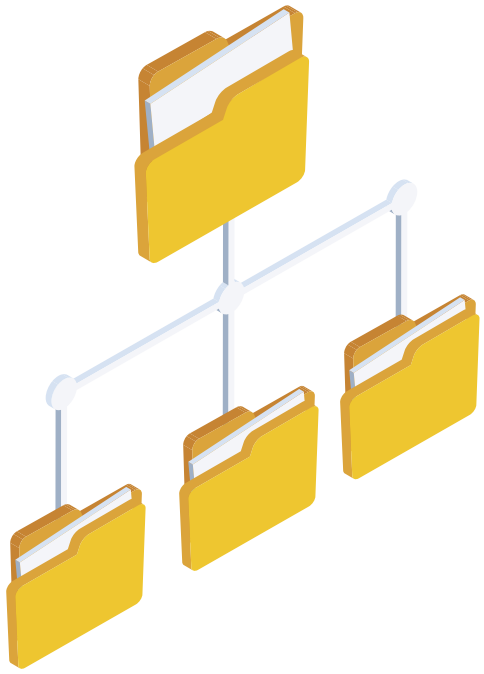
La alta dirección debe establecer una política de seguridad de la información que:

a) Sea adecuada al propósito de la organización;

b) Incluya objetivos de seguridad de la información (véase 6.2) o proporcione un marco de referencia para el establecimiento de los objetivos de seguridad de la información;

c) Incluya el compromiso de cumplir con los requisitos aplicables a la seguridad de la información; e

d) Incluya el compromiso de mejora continua del sistema de gestión de la seguridad de la información.



La política de seguridad de la información debe:

e) Estar disponible como información documentada;

f) Comunicarse dentro de la organización; y

g) Estar disponible para las partes interesadas, según sea apropiado.

5.3 Roles, Responsabilidades y Autoridades en la Organización

La alta dirección debe asegurarse que las responsabilidades y autoridades para los roles pertinentes a la seguridad de la información se asignen y comuniquen dentro de la organización.

La alta dirección debe asignar la responsabilidad y autoridad para:

a) Asegurarse que el sistema de gestión de la seguridad de la información es conforme con los requisitos de esta norma internacional; e

b) Informar a la alta dirección sobre el comportamiento del sistema de gestión de la seguridad de la información.

NOTA: La alta dirección también puede asignar responsabilidades y autoridades para informar sobre el comportamiento del sistema de gestión de la seguridad de la información dentro de la organización.

6. Planificación

CertiProf®

Professional Knowledge

www.certiprof.com

6.1 Acciones para Tratar los Riesgos y Oportunidades

6.1.1 Consideraciones Generales

Al planificar el sistema de gestión de la seguridad de la información, la organización debe considerar las cuestiones a las que se hace referencia en el apartado **4.1** y los requisitos incluidos en el apartado **4.2**, y determinar los riesgos y oportunidades que es necesario tratar con el fin de:

a) Asegurar que el sistema de gestión de la seguridad de la información pueda conseguir sus resultados previstos;

b) Prevenir o reducir efectos indeseados; y

c) Lograr la mejora continua.

La organización debe planificar:

d) Las acciones para tratar estos riesgos y oportunidades; y

e) La manera de:
1. Integrar e implementar las acciones en los procesos del sistema de gestión de la seguridad de la información, y
2. Evaluar la eficacia de estas acciones.

6.1.2 Apreciación de Riesgos de Seguridad de la Información

La organización debe definir y aplicar un proceso de apreciación de riesgos de seguridad de la información que:

a) Establezca y mantenga criterios sobre riesgos de seguridad de la información incluyendo:
1. Los criterios de aceptación de los riesgos, y
2. Los criterios para llevar a cabo las apreciaciones de los riesgos de seguridad de la información;

b) Asegure que las sucesivas apreciaciones de los riesgos de seguridad de la información generan resultados consistentes, válidos y comparables;

c) **I**dentifique los riesgos de seguridad de la información:

1. Llevando a cabo el proceso de apreciación de riesgos de seguridad de la información para identificar los riesgos asociados a la pérdida de confidencialidad, integridad y disponibilidad de la información en el alcance del sistema de gestión de la seguridad de la información,

2. Identificando a los dueños de los riesgos;

6.1 Acciones para Tratar los Riesgos y Oportunidades

d) Analice los riesgos de seguridad de la información:

1. Valorando las posibles consecuencias que resultarían si los riesgos identificados en el punto 6.1.2 c) 1) llegasen a materializarse,

2. Valorando de forma realista la probabilidad de ocurrencia de los riesgos identificados en el punto 6.1.2 c) 1),

3. Determinando los niveles de riesgo;

e) Evalúe los riesgos de seguridad de la información:

1. Comparando los resultados del análisis de riesgos con los criterios de riesgo establecidos en el punto 6.1.2 a),

2. Priorizando el tratamiento de los riesgos analizados.

La organización debe conservar información documentada sobre el proceso de apreciación de riesgos de seguridad de la información.

6.1.3 Tratamiento de los Riesgos de Seguridad de la Información

La organización debe definir y efectuar un proceso de tratamiento de los riesgos de seguridad de la información para:

a) Seleccionar las opciones adecuadas de tratamiento de riesgos de seguridad de la información teniendo en cuenta los resultados de la apreciación de riesgos;

b) Determinar todos los controles que sean necesarios para implementar la(s) opción(es) elegida(s) de tratamiento de riesgos de seguridad de la información;

NOTA: Las organizaciones pueden diseñar controles según sea necesario, o identificarlos a partir de cualquier fuente.

c) Comparar los controles determinados en el punto 6.1.3 b) con los del anexo A y comprobar que no se han omitido controles necesarios;

NOTA 1: El anexo A contiene una amplia lista de objetivos de control y controles. Se indica a los usuarios de esta norma internacional que se dirijan al anexo A para asegurar que no se pasan por alto controles necesarios.

NOTA 2: Los objetivos de control se incluyen implícitamente en los controles seleccionados. Los objetivos de control y los controles enumerados en el anexo A no son exhaustivos, por lo que pueden ser necesarios objetivos de control y controles adicionales.

6.1 Acciones para Tratar los Riesgos y Oportunidades

d) Elaborar una "Declaración de Aplicabilidad" que contenga:

- Los controles necesarios [véase 6.1.3 b) y c)];
- La justificación de las inclusiones;
- Si los controles necesarios están implementados o no; y
- La justificación de las exclusiones de cualquiera de los controles del anexo A.

e) Formular un plan de tratamiento de riesgos de seguridad de la información; y

f) Obtener la aprobación del plan de tratamiento de riesgos de seguridad de la información y la aceptación de los riesgos residuales de seguridad de la información por parte de los dueños de los riesgos.

La organización debe conservar información documentada sobre el proceso de tratamiento de riesgos de seguridad de la información.

NOTA: La apreciación de los riesgos de seguridad de la información y el proceso de tratamiento recogido en esta norma internacional se alinean con los principios y directrices genéricas definidos en la Norma ISO 31000[5].

6.2 Objetivos de Seguridad de la Información y Planificación para su Consecución

La organización debe establecer los objetivos de seguridad de la información en las funciones y niveles pertinentes.

Los objetivos de seguridad de la información deben:

a) Ser coherentes con la política de seguridad de la información;

b) Ser medibles (si es posible);

c) Tener en cuenta los requisitos de seguridad de la información aplicables y los resultados de la apreciación y del tratamiento de los riesgos;

d) Ser comunicados; y

e) Ser actualizados, según sea apropiado.

La organización debe conservar información documentada sobre los objetivos de seguridad de la información.

Cuando se hace la planificación para la consecución de los objetivos de seguridad de la información, la organización debe determinar:

f) Lo que se va a hacer;

g) Qué recursos se requerirán;

h) Quién será responsable;

i) Cuándo se finalizará; y

j) Cómo se evaluarán los resultados.

7. Soporte

CertiProf®

Professional Knowledge

www.certiprof.com

7.1 Recursos

La organización debe determinar y proporcionar los recursos necesarios para el establecimiento, implementación, mantenimiento y mejora continua del sistema de gestión de la seguridad de la información.

7.2 Competencia

La organización debe:

a) Determinar la competencia necesaria de las personas que realizan, bajo su control, un trabajo que afecta a su desempeño en seguridad de la información; y

b) Asegurarse que estas personas sean competentes, basándose en la educación, formación o experiencia adecuadas;

c) Cuando sea aplicable, poner en marcha acciones para adquirir la competencia necesaria y evaluar la eficacia de las acciones llevadas a cabo; y

d) Conservar la información documentada apropiada, como evidencia de la competencia.

NOTA: Las acciones aplicables pueden incluir, por ejemplo: la formación, la tutoría o la reasignación de las personas empleadas actualmente; o la contratación de personas competentes.

7.3 Concienciación

Las personas que trabajan bajo el control de la organización deben ser conscientes de:

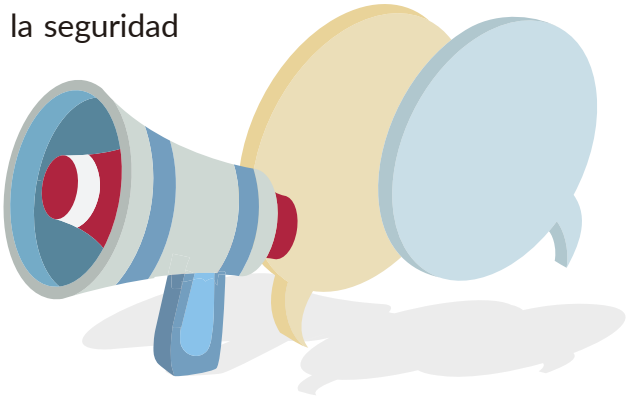
a) La política de la seguridad de la información;

b) Su contribución a la eficacia del sistema de gestión de la seguridad de la información, incluyendo los beneficios de una mejora del desempeño en seguridad de la información;

c) Las implicaciones de no cumplir con los requisitos del sistema de gestión de la seguridad de la información.

7.4 Comunicación

La organización debe determinar la necesidad de comunicaciones internas y externas pertinentes al sistema de gestión de la seguridad de la información, que incluyan:



a) El contenido de la comunicación;

b) Cuándo comunicar;

c) A quién comunicar;

d) Quién debe comunicar;

e) Los procesos por los que debe efectuarse la comunicación.

7.5 Información Documentada

7.5.1 Consideraciones Generales

El sistema de gestión de la seguridad de la información de la organización debe incluir:

a) La información documentada requerida por esta norma internacional;

b) La información documentada que la organización ha determinado que es necesaria para la eficacia del sistema de gestión de la seguridad de la información.

NOTA: El alcance de la información documentada para un sistema de gestión de la seguridad de la información puede ser diferente de una organización a otra, debido a:

1. El tamaño de la organización y a su tipo de actividades, procesos, productos y servicios,
2. La complejidad de los procesos y sus interacciones, y
3. La competencia de las personas.

7.5.2 Creación y Actualización

Cuando se crea y actualiza la información documentada, la organización debe asegurarse, en la manera que corresponda, de lo siguiente:

a) La identificación y descripción (por ejemplo, título, fecha, autor o número de referencia);

b) El formato (por ejemplo, idioma, versión del software, gráficos) y sus medios de soporte (por ejemplo, papel, electrónico);

c) La revisión y aprobación con respecto a la idoneidad y adecuación.

7.5 Información Documentada

7.5.3 Control de la Información Documentada

La información documentada requerida por el sistema de gestión de la seguridad de la información y por esta norma internacional se debe controlar para asegurarse que:

a) Esté disponible y preparada para su uso, dónde y cuándo se necesite;

b) Esté protegida adecuadamente (por ejemplo, contra pérdida de la confidencialidad, uso inadecuado, o pérdida de integridad).

Para el control de la información documentada, la organización debe tratar las siguientes actividades, según sea aplicable:

c) Distribución, acceso, recuperación y uso;

d) Almacenamiento y preservación, incluida la preservación de la legibilidad;

e) Control de cambios (por ejemplo, control de versión);

f) Retención y disposición.

La información documentada de origen externo, que la organización ha determinado que es necesaria para la planificación y operación del sistema de gestión de la seguridad de la información se debe identificar y controlar, según sea adecuado.

NOTA: El acceso implica una decisión concerniente al permiso solamente para consultar la información documentada, o el permiso y la autoridad para consultar y modificar la información documentada, etc.

8. Operación

CertiProf®

Professional Knowledge

www.certiprof.com

8.1 Planificación y Control Operacional

La organización debe planificar, implementar y controlar los procesos necesarios para cumplir los requisitos de seguridad de la información y para implementar las acciones determinadas en el apartado **6.1**. La organización debe implementar también planes para alcanzar los objetivos de seguridad de la información determinados en el apartado **6.2**.

En la medida necesaria la organización debe mantener información documentada, para tener la confianza de que los procesos se han llevado a cabo según lo planificado.

La organización debe controlar los cambios planificados y revisar las consecuencias de los cambios no previstos, llevando a cabo acciones para mitigar los efectos adversos, cuando sea necesario.

La organización debe garantizar que los procesos contratados externamente estén controlados.

8.2 Apreciación de los Riesgos de Seguridad de la Información

La organización debe efectuar apreciaciones de riesgos de seguridad de la información a intervalos planificados, y cuando se propongan o se produzcan modificaciones importantes, teniendo en cuenta los criterios establecidos en el punto **6.1.2 a).**

La organización debe conservar información documentada de los resultados de las apreciaciones de riesgos de seguridad de información.

8.3 Tratamiento de los Riesgos de Seguridad de la Información

La organización debe implementar el plan de tratamiento de los riesgos de seguridad de la información.

La organización debe conservar información documentada de los resultados del tratamiento de los riesgos de seguridad de la información.

9. Evaluación del Desempeño

CertiProf®

Professional Knowledge

www.certiprof.com

9.1 Seguimiento, Medición, Análisis y Evaluación

La organización debe evaluar el desempeño de la seguridad de la información y la eficacia del sistema de gestión de la seguridad de la información.

La organización debe determinar:

a) A qué es necesario hacer seguimiento y qué es necesario medir, incluyendo procesos y controles de seguridad de la información;

b) Los métodos de seguimiento, medición, análisis y evaluación, según sea aplicable, para garantizar resultados válidos;

NOTA: Los métodos seleccionados deben producir resultados comparables y reproducibles para ser considerados válidos.

c) Cuándo se deben llevar a cabo el seguimiento y la medición;

d) Quién debe hacer el seguimiento y la medición;

e) Cuándo se deben analizar y evaluar los resultados del seguimiento y la medición;

f) Quién debe analizar y evaluar esos resultados.

La organización debe conservar la información documentada adecuada como evidencia de los resultados.

9.2 Auditoría Interna

La organización debe llevar a cabo auditorías internas a intervalos planificados, para proporcionar información acerca de si el sistema de gestión de la seguridad de la información:

a) Cumple con:

1. Los requisitos propios de la organización para su sistema de gestión de la seguridad de la información,
2. Los requisitos de esta norma internacional,

b) Está implementado y mantenido de manera eficaz.

La organización debe:

c) Planificar, establecer, implementar y mantener uno o varios programas de auditoría que incluyan la frecuencia, los métodos, las responsabilidades, los requisitos de planificación, y la elaboración de informes. Los programas de auditoría deben tener en cuenta la importancia de los procesos involucrados y los resultados de las auditorías previas;

d) Para cada auditoría, definir sus criterios y su alcance;

e) Seleccionar los auditores y llevar a cabo auditorías para asegurarse de la objetividad y la imparcialidad del proceso de auditoría;

f) Asegurarse de que se informa a la dirección pertinente de los resultados de las auditorías; y

g) Conservar información documentada como evidencia de la implementación del programa de auditoría y de los resultados de ésta.

9.3 Revisión por la Dirección

La alta dirección debe revisar el sistema de gestión de la seguridad de la información de la organización a intervalos planificados, para asegurarse de su conveniencia, adecuación y eficacia continuas.

La revisión por la dirección debe incluir consideraciones sobre:

a) El estado de las acciones desde anteriores revisiones por la dirección;

b) Los cambios en las cuestiones externas e internas que sean pertinentes al sistema de gestión de la seguridad de la información;

c) La información sobre el comportamiento de la seguridad de la información, incluidas las tendencias relativas a:

1. No conformidades y acciones correctivas,
2. Seguimiento y resultados de las mediciones,
3. Resultados de auditoría, y
4. El cumplimiento de los objetivos de seguridad de la información,

d) Los comentarios provenientes de las partes interesadas;

e) Los resultados de la apreciación de los riesgos y el estado del plan de tratamiento de riesgos; y

f) Las oportunidades de mejora continua.

Los elementos de salida de la revisión por la dirección deben incluir las decisiones relacionadas con las oportunidades de mejora continua y cualquier necesidad de cambio en el sistema de gestión de la seguridad de la información.

La organización debe conservar información documentada como evidencia de los resultados de las revisiones por la dirección.

10. Mejora

CertiProf®

Professional Knowledge

www.certiprof.com

10.1 No Conformidad y Acciones Correctivas

Cuando ocurra una no conformidad, la organización debe:

a) Reaccionar ante la no conformidad, y según sea aplicable:

1. Llevar a cabo acciones para controlarla y corregirla, y
2. Hacer frente a las consecuencias,

b) Evaluar la necesidad de acciones para eliminar las causas de la no conformidad, con el fin de que no vuelva a ocurrir, ni ocurra en otra parte, mediante:

1. La revisión de la no conformidad,
2. La determinación de las causas de la no conformidad, y
3. La determinación de si existen no conformidades similares, o que potencialmente podrían ocurrir;

c) Implementar cualquier acción necesaria;

d) Revisar la eficacia de las acciones correctivas llevadas a cabo; y

e) Si es necesario, hacer cambios al sistema de gestión de la seguridad de la información.

Las acciones correctivas deben ser adecuadas a los efectos de las no conformidades encontradas.

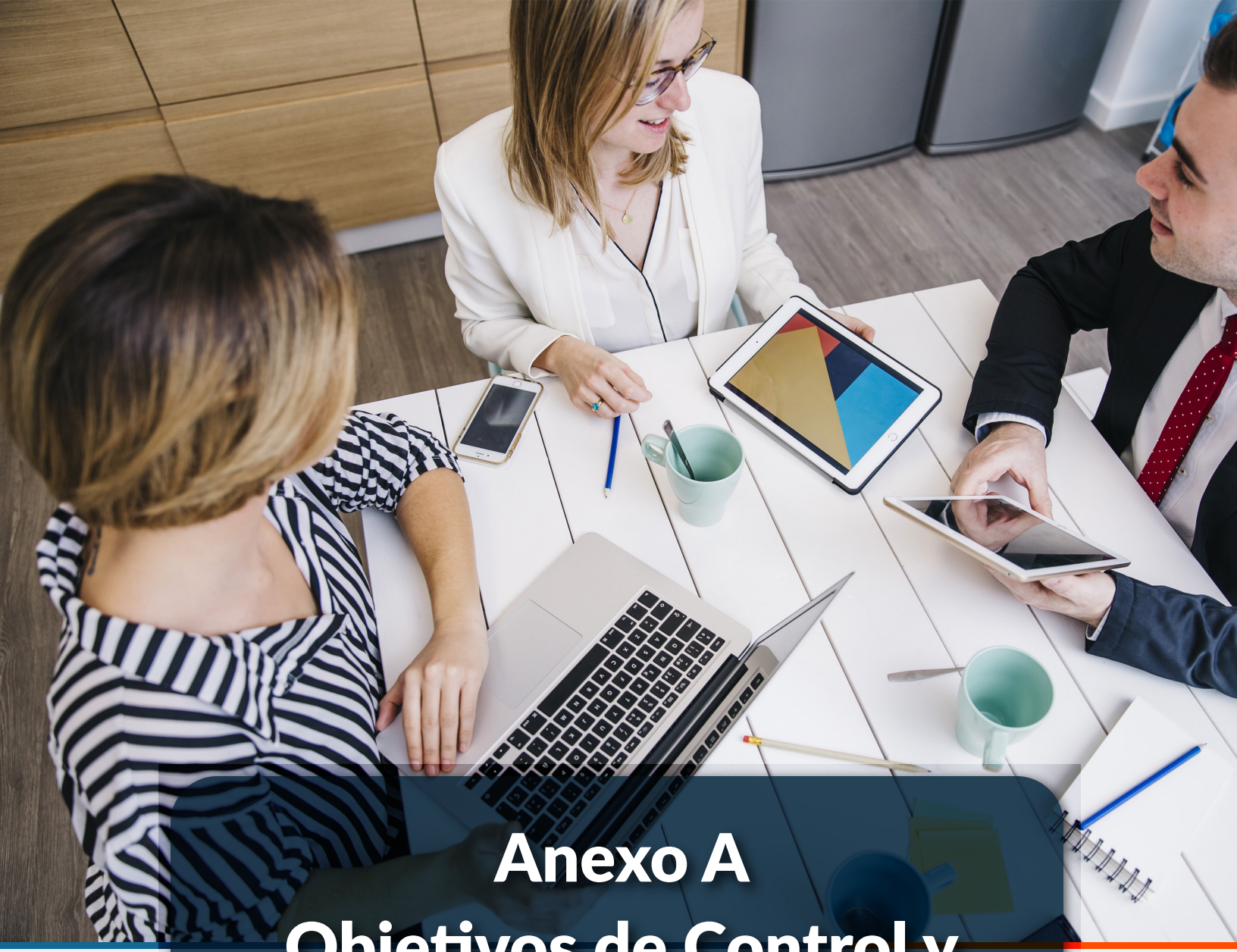
La organización debe conservar información documentada, como evidencia de:

f) La naturaleza de las no conformidades y cualquier acción posterior llevada a cabo; y

g) Los resultados de cualquier acción correctiva.

10.1 No conformidad y Acciones Correctivas

La organización debe mejorar de manera continua la idoneidad, adecuación y eficacia del sistema de gestión de la seguridad de la información.



Anexo A
Objetivos de Control y Controles de Referencia

CertiProf®
Professional Knowledge

www.certiprof.com

ANEXO A.1 OBJETIVOS DE CONTROL Y CONTROLES DE REFERENCIA - ISO 27001

5. Políticas de seguridad de la información
5.1 Directrices de gestión de la seguridad de la información
5.1.1 Políticas para la seguridad de la información
5.1.2 Revisión de las políticas para la seguridad de la información

6. Organización de la seguridad de la información
6.1 Organización interna
6.1.1 Roles y responsabilidades en seguridad de la información
6.1.2 Segregación de tareas
6.1.3 Contacto con las autoridades
6.1.4 Contacto con grupos de interés especial
6.1.5 Seguridad de la información en la gestión de proyectos
6.2 Los dispositivos móviles y el teletrabajo
6.2.1 Política de dispositivos móviles
6.2.2 Teletrabajo

7. Seguridad relativa a los recursos humanos
7.1 Antes del empleo
7.1.1 Investigación de antecedentes
7.1.2 Términos y condiciones del empleo
7.2 Durante el empleo
7.2.1 Responsabilidades de gestión
7.2.2 Concienciación, educación y capacitación en seguridad de la información
7.2.3 Proceso disciplinario
7.3 Finalización del empleo o cambio en el puesto de trabajo
7.3.1 Responsabilidades ante la finalización o cambio

8. Gestión de activos
8.1 Responsabilidad sobre los activos
8.1.1 Inventario de activos
8.1.2 Propiedad de los activos
8.1.3 Uso aceptable de los activos
8.1.4 Devolución de activos
8.2 Clasificación de la información
8.2.1 Clasificación de la información
8.2.2 Etiquetado de la información
8.2.3 Manipulado de la información
8.3 Manipulación de los soportes
8.3.1 Gestión de soportes extraíbles
8.3.2 Eliminación de soportes
8.3.3 Soportes físicos en tránsito

9. Control de acceso
9.1 Requisitos de negocio para el control de acceso
9.1.1 Política de control de acceso
9.1.2 Acceso a las redes y a los servicios de red
9.2 Gestión de acceso de usuario
9.2.1 Registro y baja de usuario
9.2.2 Provisión de acceso de usuario
9.2.3 Gestión de privilegios de acceso
9.2.4 Gestión de la información secreta de autenticación de los usuarios
9.2.5 Revisión de los derechos de acceso de usuario
9.2.6 Retirada o reasignación de los derechos de acceso
9.3 Responsabilidades del usuario
9.3.1 Uso de la información secreta de autenticación
9.4 Control de acceso a sistemas y aplicaciones
9.4.1 Restricción del acceso a la información
9.4.2 Procedimientos seguros de inicio de sesión
9.4.3 Sistema de gestión de contraseñas
9.4.4 Uso de utilidades con privilegios del sistema
9.4.5 Control de acceso al código fuente de los programas

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

11. Seguridad física y del entorno
11.1 Áreas seguras
11.1.1 Perímetro de seguridad física
11.1.2 Controles físicos de entrada
11.1.3 Seguridad de oficinas, despachos y recursos
11.1.4 Protección contra las amenazas externas y ambientales
11.1.5 El trabajo en áreas seguras
11.1.6 Áreas de carga y descarga
11.2 Seguridad de los equipos
11.2.1 Emplazamiento y protección de equipos
11.2.2 Instalaciones de suministro
11.2.3 Seguridad del cableado
11.2.4 Mantenimiento de los equipos
11.2.5 Retirada de materiales propiedad de la empresa
11.2.6 Seguridad de los equipos fuera de las instalaciones
11.2.7 Reutilización o eliminación segura de equipos
11.2.8 Equipo de usuario desatendido
11.2.9 Política de puesto de trabajo despejado y pantalla limpia

12. Seguridad de las operaciones
12.1 Procedimientos y responsabilidades operacionales
12.1.1 Documentación de procedimientos operacionales
12.1.2 Gestión de cambios
12.1.3 Gestión de capacidades
12.1.4 Separación de los recursos de desarrollo, prueba y operación
12.2 Protección contra el software malicioso (malware)
12.2.1 Controles contra el código malicioso
12.3 Copias de seguridad
12.3.1 Copias de seguridad de la información
12.4 Registros y supervisión
12.4.1 Registro de eventos
12.4.2 Protección de la información del registro
12.4.3 Registros de administración y operación
12.4.4 Sincronización del reloj
12.5 Control del software en explotación
12.5.1 Instalación del software en explotación
12.6 Gestión de la vulnerabilidad técnica
12.6.1 Gestión de las vulnerabilidades técnicas
12.6.2 Restricción en la instalación de software
12.7 Consideraciones sobre la auditoria de sistemas de información
12.7.1 Controles de auditoría de sistemas de información

13. Seguridad de las comunicaciones
13.1 Gestión de la seguridad de las redes
13.1.1 Controles de red
13.1.2 Seguridad de los servicios de red
13.1.3 Segregación en redes
13.2 Intercambio de información
13.2.1 Políticas y procedimientos de intercambio de información
13.2.2 Acuerdos de intercambio de información
13.2.3 Mensajería electrónica
13.2.4 Acuerdos de confidencialidad o no revelación

14. Adquisición, desarrollo y mantenimiento de los sistemas de información
14.1 Requisitos de seguridad en los sistemas de información
14.1.1 Análisis de requisitos y especificaciones de seguridad de la información
14.1.2 Asegurar los servicios de aplicaciones en redes públicas
14.1.3 Protección de las transacciones de servicios de aplicaciones
14.2 Seguridad en el desarrollo y en los procesos de soporte
14.2.1 Política de desarrollo seguro
14.2.2 Procedimiento de control de cambios en sistemas
14.2.3 Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo
14.2.4 Restricciones a los cambios en los paquetes de software
14.2.5 Principios de ingeniería de sistemas seguros
14.2.6 Entorno de desarrollo seguro
14.2.7 Externalización del desarrollo de software
14.2.8 Pruebas funcionales de seguridad de sistemas
14.2.9 Pruebas de aceptación de sistemas
14.3 Datos de prueba
14.3.1 Protección de los datos de prueba

15. Relación con proveedores
15.1 Seguridad en las relaciones con proveedores
15.1.1 Política de seguridad de la información en las relaciones con los proveedores
15.1.2 Requisitos de seguridad en contratos con terceros
15.1.3 Cadena de suministro de tecnología de la información y de las comunicaciones
15.2 Gestión de la provisión de servicios del proveedor
15.2.1 Control y revisión de la provisión de servicios del proveedor
15.2.2 Gestión de cambios en la provisión del servicio del proveedor

16. Gestión de incidentes de seguridad de la información
16.1 Gestión de incidentes de seguridad de la información y mejoras
16.1.1 Responsabilidades y procedimientos
16.1.2 Notificación de los eventos de seguridad de la información
16.1.3 Notificación de puntos débiles de la seguridad
16.1.4 Evaluación y decisión sobre los eventos de seguridad de información
16.1.5 Respuesta a incidentes de seguridad de la información
16.1.6 Aprendizaje de los incidentes de seguridad de la información
16.1.7 Recopilación de evidencias

17. Aspectos de seguridad de la información para la gestión de la continuidad de negocio
17.1 Continuidad de la seguridad de la información
17.1.1 Planificación de la continuidad de la seguridad de la información
17.1.2 Implementar la continuidad de la seguridad de la información
17.1.3 Verificación, revisión y evaluación de la continuidad de la seguridad de la información
17.2 Redundancias.
17.2.1 Disponibilidad de los recursos de tratamiento de la información

18. Cumplimiento
18.1 Cumplimiento de los requisitos legales y contractuales
18.1.1 Identificación de la legislación aplicable y de los requisitos contractuales
18.1.2 Derechos de Propiedad Intelectual (DPI)
18.1.3 Protección de los registros de la organización
18.1.4 Protección y privacidad de la información de carácter personal
18.1.5 Regulación de los controles criptográficos
18.2 Revisiones de la seguridad de la información
18.2.1 Revisión independiente de la seguridad de la información
18.2.2 Cumplimiento de las políticas y normas de seguridad
18.2.3 Comprobación del cumplimiento técnico

CertiProf®
Professional Knowledge

Anexo A (Normativo)

Objetivos de control y controles de referencia

Los objetivos de control y controles que se enumeran en la tabla A.1 se corresponden directamente con los que figuran en la Norma ISO/IEC 27002:2013[1], capítulos 5 a 18, y deben ser empleados en el contexto del apartado 6.1.3.

Tabla A.1 – Objetivos de control y controles

A.5 Políticas de seguridad de la información		
A.5.1 Directrices de gestión de la seguridad de la información		
Objetivo: Proporcionar orientación y apoyo a la gestión de la seguridad de la información de acuerdo con los requisitos del negocio, las leyes y normativa pertinentes.		
A.5.1.1	Políticas para la seguridad de la información	*Control* Un conjunto de políticas para la seguridad de la información debe ser definido, aprobado por la dirección, publicado y comunicado a los empleados y partes externas relevantes.
A.5.1.2	Revisión de las políticas para la seguridad de la información	*Control* Las políticas de seguridad de la información deben 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 Organización de la seguridad de la información		
A.6.1 Organización interna		
Objetivo: Establecer un marco de gestión para iniciar y controlar la implementación y operación de la seguridad de la información dentro de la organización.		
A.6.1.1	Roles y responsabilidades en seguridad de la información	*Control* Todas las responsabilidades en seguridad de la información deben ser definidas y asignadas.
A.6.1.2	Segregación de tareas	*Control* Las funciones 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.6.1.3	Contacto con las autoridades	*Control* Deben mantenerse los contactos apropiados con las autoridades pertinentes.
A.6.1.4	Contacto con grupos de interés especial	*Control* Deben mantenerse los contactos apropiados con grupos de interés especial, u otros foros y asociaciones profesionales especializados en seguridad.

A.6.1.5	Seguridad de la información en la gestión de proyectos	*Control* La seguridad de la información debe tratarse dentro de la gestión de proyectos, independientemente de la naturaleza del proyecto.
A.6.2 Los dispositivos móviles y el teletrabajo		
Objetivo: Garantizar la seguridad en el teletrabajo y en el uso de dispositivos móviles.		
A.6.2.1	Contacto con las autoridades	*Control* Se debe adoptar una política y unas medidas de seguridad adecuadas para la protección contra los riesgos de la utilización de dispositivos móviles.
A.6.2.2	Teletrabajo	*Control* Se debe implementar una política y unas medidas de seguridad adecuadas para proteger la información accedida, tratada o almacenada en emplazamientos de teletrabajo.
A.7 Seguridad relativa a los recursos humanos		
A.7.1 Antes del empleo		
Objetivo: Para asegurarse que los empleados y contratistas entiendan sus responsabilidades y son adecuados para las funciones para las que se consideran.		
A.7.1.1	Investigación de antecedentes	*Control* La comprobación de los antecedentes de todos los candidatos al puesto de trabajo se debe llevar a cabo de acuerdo con las leyes, normativa y códigos éticos que sean de aplicación y debe ser proporcional a las necesidades del negocio, la clasificación de la información a la que se accede y los riesgos percibidos.
A.7.1.2	Términos y condiciones del empleo	*Control* Cómo parte de sus obligaciones contractuales, los empleados y contratistas deben establecer los términos y condiciones en su contrato de trabajo en lo que respecta a la seguridad de la información, tanto hacia el empleado como hacia la organización.
A.7.2 Durante el empleo		
Objetivo: Asegurar que los empleados y contratistas conozcan y cumplan con sus responsabilidades en seguridad de la información.		
A.7.2.1	Responsabilidades de gestión	*Control* La dirección debe exigir a los empleados y contratistas, que apliquen la seguridad de la información de acuerdo con las políticas y procedimientos establecidos en la organización.
A.7.2.2	Concienciación, educación y capacitación en seguridad de la información	*Control* Todos los empleados de la organización y, cuando corresponda, los contratistas, deben recibir una adecuada educación, concienciación y capacitación con actualizaciones periódicas sobre las políticas y procedimientos de la organización, según corresponda a su puesto de trabajo.

A.7.2.3	Proceso disciplinario	*Control* Debe existir un proceso disciplinario formal que haya sido comunicado a los empleados, que recoja las acciones a tomar ante aquellos que hayan provocado alguna brecha de seguridad.
A.7.3 Finalización del empleo o cambio en el puesto de trabajo		
Objetivo: Proteger los intereses de la organización como parte del proceso de cambio o finalización del empleo.		
A.7.3.1	Responsabilidades ante la finalización o cambio	*Control* Las responsabilidades en seguridad de la información y obligaciones que siguen vigentes después del cambio o finalización del empleo se deben definir, comunicar al empleado o contratista y se deben cumplir.
A.8 Gestión de activos		
A.8.1 Responsabilidad sobre los activos		
Objetivo: Identificar los activos de la organización y definir las responsabilidades de protección adecuadas.		
A.8.1.1	Inventario de activos	*Control* La información y otros activos asociados a la información y a los recursos para el tratamiento de la información deben estar claramente identificados y debe elaborarse y mantenerse un inventario.
A.8.1.2	Propiedad de los activos	*Control* Todos los activos que figuran en el inventario deben tener un propietario.
A.8.1.3	Uso aceptable de los activos	*Control* Se deben identificar, documentar e implementar las reglas de uso aceptable de la información y de los activos asociados con los recursos para el tratamiento de la información.
A.8.1.4	Devolución de activos	*Control* Todos los empleados y terceras partes deben devolver todos los activos de la organización que estén en su poder al finalizar su empleo, contrato o acuerdo.
A.8.2 Clasificación de la información		
Objetivo: Asegurar que la información reciba un nivel adecuado de protección de acuerdo con su importancia para la organización.		
A.8.2.1	Clasificación de la información	*Control* La información debe ser clasificada en términos de la importancia de su revelación frente a requisitos legales, valor, sensibilidad y criticidad ante revelación o modificación no autorizadas.
A.8.2.2	Etiquetado de la información	*Control* Debe desarrollarse e implantarse un conjunto adecuado de procedimientos para etiquetar la información, de acuerdo con el esquema de clasificación adoptado por la organización.

A.8.2.3	Manipulado de la información	*Control* Debe desarrollarse e implantarse un conjunto adecuado de procedimientos para la manipulación de la información, de acuerdo con el esquema de clasificación adoptado por la organización.
A.8.3 Manipulación de los soportes		
Objetivo: Evitar la revelación, modificación, eliminación o destrucción no autorizadas de la información almacenada en soportes.		
A.8.3.1	Gestión de soportes extraíbles	*Control* Se deben implementar procedimientos para la gestión de los soportes extraíbles, de acuerdo con el esquema de clasificación adoptado por la organización.
A.8.3.2	Eliminación de soportes	*Control* Los soportes deben eliminarse de forma segura cuando ya no vayan a ser necesarios, mediante procedimientos formales.
A.8.3.3	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.9 Control de acceso		
A.9.1 Requisitos de negocio para el control de acceso		
Objetivo: Limitar el acceso a los recursos de tratamiento de la información y a la información.		
A.9.1.1	Política de control de acceso	*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.9.1.2	Acceso a las redes y a los servicios de red	*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.9.2 Gestión de acceso de usuario		
Objetivo: Garantizar el acceso de usuarios autorizados y evitar el acceso no autorizado a los sistemas y servicios.		
A.9.2.1	Registro y baja de usuario	*Control* Debe implantarse un procedimiento formal de registro y retirada de usuarios que haga posible la asignación de los derechos de acceso.
A.9.2.2	Provisión de acceso de usuario	*Control* Debe implantarse un procedimiento formal para asignar o revocar los derechos de acceso para todos los tipos de usuarios de todos los sistemas y servicios.
A.9.2.3	Gestión de privilegios de acceso	*Control* La asignación y el uso de privilegios de acceso debe estar restringida y controlada.

A.9.2.4	Gestión de la información secreta de autenticación de los usuarios	*Control* La asignación de la información secreta de autenticación debe ser controlada a través de un proceso formal de gestión.
A.9.2.5	Revisión de los derechos de acceso de usuario	*Control* Los propietarios de los activos deben revisar los derechos de acceso de usuario a intervalos regulares.
A.9.2.6	Retirada o reasignación de los derechos de acceso	*Control* Los derechos de acceso de todos los empleados y terceras partes, a la información y a los recursos de tratamiento de la información deben ser retirados a la finalización del empleo, del contrato o del acuerdo, o ajustados en caso de cambio.
A.9.3 Responsabilidades del usuario		
Objetivo: Para que los usuarios se hagan responsables de salvaguardar su información de autenticación.		
A.9.3.1	Uso de la información secreta de autenticación	*Control* Se debe requerir a los usuarios que sigan las prácticas de la organización en el uso de la información secreta de autenticación.
A.9.4 Control de acceso a sistemas y aplicaciones		
Objetivo: Prevenir el acceso no autorizado a los sistemas y aplicaciones.		
A.9.4.1	Restricción del acceso a la información	*Control* Se debe restringir el acceso a la información y a las funciones de las aplicaciones, de acuerdo con la política de control de acceso definida.
A.9.4.2	Procedimientos seguros de inicio de sesión	*Control* Cuando así se requiera en la política de control de acceso, el acceso a los sistemas y a las aplicaciones se debe controlar por medio de un procedimiento seguro de inicio de sesión.
A.9.4.3	Sistema de gestión de contraseñas	*Control* Los sistemas para la gestión de contraseñas deben ser interactivos y establecer contraseñas seguras y robustas.
A.9.4.4	Uso de utilidades con privilegios del sistema	*Control* Se debe restringir y controlar rigurosamente el uso de utilidades que puedan ser capaces de invalidar los controles del sistema y de la aplicación.
A.9.4.5	Control de acceso al código fuente de los programas	*Control* Se debe restringir el acceso al código fuente de los programas.
A.10 Criptografía		
A.10.1 Controles criptográficos		
Objetivo: Garantizar un uso adecuado y eficaz de la criptografía para proteger la confidencialidad, autenticidad y/o integridad de la información.		
A.10.1.1	Política de uso de los controles criptográficos	*Control* Se debe desarrollar e implementar una política sobre el uso de los controles criptográficos para proteger la información.

A.10.1.2	Gestión de claves	*Control* Se debe desarrollar e implementar una política sobre el uso, la protección y la duración de las claves de cifrado a lo largo de todo su ciclo de vida.
A.11 Seguridad física y del entorno		
A.11.1 Áreas seguras		
Objetivo: Prevenir el acceso físico no autorizado, los daños e interferencia a la información de la organización y a los recursos de tratamiento de la información.		
A.11.1.1	Perímetro de seguridad física	*Control* Se deben utilizar perímetros de seguridad para proteger las áreas que contienen información sensible así como los recursos de tratamiento de la información.
A.11.1.2	Controles físicos de entrada	*Control* Las áreas seguras deben estar protegidas mediante controles de entrada adecuados, para asegurar que únicamente se permite el acceso al personal autorizado.
A.11.1.3	Seguridad de oficinas, despachos y recursos	*Control* Para las oficinas, despachos y recursos, se debe diseñar y aplicar la seguridad física.
A.11.1.4	Protección contra las amenazas externas y ambientales	*Control* Se debe diseñar y aplicar una protección física contra desastres naturales, ataques provocados por el hombre o accidentes.
A.11.1.5	El trabajo en áreas seguras	*Control* Se deben diseñar e implementar procedimientos para trabajar en las áreas seguras.
A.11.1.6	Áreas de carga y descarga	*Control* Deben controlarse los puntos de acceso tales como las áreas de carga y descarga y otros puntos, donde pueda acceder personal no autorizado a las instalaciones, y si es posible, aislar dichos puntos de los recursos de tratamiento de la información para evitar accesos no autorizados.
A.11.2 Seguridad de los equipos		
Objetivo: Evitar la pérdida, daño, robo o el compromiso de los activos y la interrupción de las operaciones de la organización.		
A.11.2.1	Emplazamiento y protección de equipos	*Control* Los equipos deben situarse o protegerse de forma que se reduzcan los riesgos de las amenazas y los riesgos ambientales así como las oportunidades de que se produzcan accesos no autorizados.
A.11.2.2	Instalaciones de suministro	*Control* Los equipos deben estar protegidos contra fallos de alimentación y otras alteraciones causadas por fallos en las instalaciones de suministro.

A.11.2.3	Seguridad del cableado	*Control* El cableado eléctrico y de telecomunicaciones que transmite datos o que sirve de soporte a los servicios de información debe estar protegido frente a interceptaciones, interferencias o daños.
A.11.2.4	Mantenimiento de los equipos	*Control* Los equipos deben recibir un mantenimiento correcto que asegure su disponibilidad y su integridad continuas.
A.11.2.5	Retirada de materiales propiedad de la empresa	*Control* Sin autorización previa, los equipos, la información o el software no deben sacarse de las instalaciones.
A.11.2.6	Seguridad de los equipos fuera de las instalaciones	*Control* Deben aplicarse medidas de seguridad a los equipos situados fuera las instalaciones de la organización, teniendo en cuenta los diferentes riesgos que conlleva trabajar fuera de dichas instalaciones.
A.11.2.7	Reutilización o eliminación segura de equipos	*Control* Todos los soportes de almacenamiento deben ser comprobados para confirmar que todo dato sensible y software bajo licencia se ha eliminado de manera segura, antes de deshacerse de ellos.
A.11.2.8	Equipo de usuario desatendido	*Control* Los usuarios deben asegurarse que el equipo desatendido tiene la protección adecuada.
A.11.2.9	Política de puesto de trabajo despejado y pantalla limpia	*Control* Debe adoptarse una política de puesto de trabajo despejado de papeles y medios de almacenamiento desmontables y una política de pantalla limpia para los recursos de tratamiento de la información.
A.12 Seguridad de las operaciones		
A.12.1 Procedimientos y responsabilidades operacionales		
Objetivo: Asegurar el funcionamiento correcto y seguro de las instalaciones de tratamiento de la información.		
A.12.1.1	Documentación de procedimientos operacionales	*Control* Deben documentarse y mantenerse procedimientos operacionales y ponerse a disposición de todos los usuarios que los necesiten.
A.12.1.2	Gestión de cambios	*Control* Los cambios en la organización, los procesos de negocio, instalaciones de tratamiento de la información y los sistemas que afectan a la seguridad de la información deben ser controlados.
A.12.1.3	Gestión de capacidades	*Control* Se debe supervisar y ajustar la utilización de los recursos, así como realizar proyecciones de los requisitos futuros de capacidad, para garantizar el rendimiento requerido del sistema.

A.12.1.4	Separación de los recursos de desarrollo, prueba y operación	*Control* Deben separarse los recursos de desarrollo, pruebas y operación, para reducir los riesgos de acceso no autorizado o los cambios del sistema en producción.
A.12.2 Protección contra el software malicioso (malware)		
Objetivo: Asegurar que los recursos de tratamiento de información y la información están protegidos contra el malware.		
A.12.2.1	Controles contra el código malicioso	*Control* Se deben implementar los controles de detección, prevención y recuperación que sirvan como protección contra el código malicioso, así como procedimientos adecuados de concienciación al usuario.
A.12.3 Copias de seguridad		
Objetivo: Evitar la pérdida de datos.		
A.12.3.1	Copias de seguridad de la información	*Control* Se deben realizar copias de seguridad de la información, del software y del sistema y se deben verificar periódicamente de acuerdo a la política de copias de seguridad acordada.
A.12.4 Registros y supervisión		
Objetivo: Registrar eventos y generar evidencias.		
A.12.4.1	Registro de eventos	*Control* Se deben registrar, proteger y revisar periódicamente las actividades de los usuarios, excepciones, fallos y eventos de seguridad de la información.
A.12.4.2	Protección de la información del registro	*Control* Los dispositivos de registro y la información del registro deben estar protegidos contra manipulaciones indebidas y accesos no autorizados.
A.12.4.3	Registros de administración y operación	*Control* Se deben registrar, proteger y revisar regularmente las actividades del administrador del sistema y del operador del sistema.
A.12.4.4	Sincronización del reloj	*Control* Los relojes de todos los sistemas de tratamiento de la información dentro de una organización o de un dominio de seguridad, deben estar sincronizados con una única fuente de tiempo precisa y acordada.
A.12.5 Control del software en explotación		
Objetivo: Asegurar la integridad del software en explotación.		
A.12.5.1	Instalación del software en explotación	*Control* Se deben implementar procedimientos para controlar la instalación del software en explotación.

A.12.6 Gestión de la vulnerabilidad técnica		
Objetivo: Reducir los riesgos resultantes de la explotación de las vulnerabilidades técnicas.		
A.12.6.1	Gestión de las vulnerabilidades técnicas	*Control* Se debe obtener información oportuna acerca de las vulnerabilidades técnicas de los sistemas de información utilizados, evaluar la exposición de la organización a dichas vulnerabilidades y adoptar las medidas adecuadas para afrontar el riesgo asociado.
A.12.6.2	Restricción en la instalación de software	*Control* Se deben establecer y aplicar reglas que rijan la instalación de software por parte de los usuarios.
A.12.7 Consideraciones sobre la auditoria de sistemas de información		
Objetivo: Minimizar el impacto de las actividades de auditoría en los sistemas operativos.		
A.12.7.1	Controles de auditoría de sistemas de información	*Control* Los requisitos y las actividades de auditoría que impliquen comprobaciones en los sistemas operativos deben ser cuidadosamente planificados y acordados para minimizar el riesgo de interrupciones en los procesos de negocio.
A.13 Seguridad de las comunicaciones		
A.13.1 Gestión de la seguridad de las redes		
Objetivo: Asegurar la protección de la información en las redes y los recursos de tratamiento de la información.		
A.13.1.1	Controles de red	*Control* Las redes deben ser gestionadas y controladas para proteger la información en los sistemas y aplicaciones.
A.13.1.2	Seguridad de los servicios de red	*Control* Se deben identificar los mecanismos de seguridad, los niveles de servicio, y los requisitos de gestión de todos los servicios de red y se deben incluir en cualquier acuerdo de servicios de red, tanto si estos servicios se prestan dentro de la organización como si se subcontratan.
A.13.1.3	Segregación en redes	*Control* Los grupos de servicios de información, los usuarios y los sistemas de información deben estar segregados en redes distintas.
A.13.2 Intercambio de información		
Objetivo: Mantener la seguridad de la información que se transfiere dentro de una organización y con cualquier entidad externa.		
A.13.2.1	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.13.2.2	Acuerdos de intercambio de información	*Control* Deben establecerse acuerdos para el intercambio seguro de información del negocio y software entre la organización y terceros.

A.13.2.3	Mensajería electrónica	*Control* La información que sea objeto de mensajería electrónica debe estar adecuadamente protegida.
A.13.2.4	Acuerdos de confidencialidad o no revelación	*Control* Deben identificarse, documentarse y revisarse regularmente los requisitos de los acuerdos de confidencialidad o no revelación.
A.14 Adquisición, desarrollo y mantenimiento de los sistemas de información		
A.14.1 Requisitos de seguridad en los sistemas de información		
Objetivo: Garantizar que la seguridad de la información sea parte integral de los sistemas de información a través de todo el ciclo de vida. Esto también incluye los requisitos para los sistemas de información que proporcionan los servicios a través de redes públicas.		
A.14.1.1	Análisis de requisitos y especificaciones de seguridad de la información	*Control* Los requisitos relacionados con la seguridad de la información deben incluirse en los requisitos para los nuevos sistemas de información o mejoras a los sistemas de información existentes.
A.14.1.2	Asegurar los servicios de aplicaciones en redes públicas	*Control* La información involucrada en aplicaciones que pasan a través de redes públicas debe ser protegida de cualquier actividad fraudulenta, disputa de contrato, revelación y modificación no autorizadas.
A.14.1.3	Protección de las transacciones de servicios de aplicaciones	*Control* La información involucrada en las transacciones de servicios de aplicaciones debe ser protegida para prevenir la transmisión incompleta, errores de enrutamiento, alteración no autorizada del mensaje, revelación, duplicación, o reproducción de mensaje no autorizadas.
A.14.2 Seguridad en el desarrollo y en los procesos de soporte		
Objetivo: Garantizar la seguridad de la información que se ha diseñado e implementado en el ciclo de vida de desarrollo de los sistemas de información.		
A.14.2.1	Política de desarrollo seguro	*Control* Se deben establecer y aplicar reglas dentro de la organización para el desarrollo de aplicaciones y sistemas.
A.14.2.2	Procedimiento de control de cambios en sistemas	*Control* La implantación de cambios a lo largo del ciclo de vida del desarrollo debe controlarse mediante el uso de procedimientos formales de control de cambios.
A.14.2.3	Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo	*Control* Cuando se modifiquen los sistemas operativos, las aplicaciones de negocio críticas deben ser revisadas y probadas para garantizar que no existen efectos adversos en las operaciones o la seguridad de la organización.
A.14.2.4	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.14.2.5	Principios de ingeniería de sistemas seguros	*Control* Principios de ingeniería de sistemas seguros se deben establecer, documentar, mantener y aplicarse a todos los esfuerzos de implementación de sistemas de información.
A.14.2.6	Entorno de desarrollo seguro	*Control* Las organizaciones deben establecer y proteger adecuadamente los entornos de desarrollo seguro para el desarrollo del sistema y los esfuerzos de integración que cubren todo el ciclo de vida de desarrollo del sistema.
A.14.2.7	Externalización del desarrollo de software	*Control* El desarrollo de software externalizado debe ser supervisado y controlado por la organización.
A.14.2.8	Pruebas funcionales de seguridad de sistemas	*Control* Se deben llevar a cabo pruebas de la seguridad funcional durante el desarrollo.
A.14.2.9	Pruebas de aceptación de sistemas	*Control* Se deben establecer programas de pruebas de aceptación y criterios relacionados para nuevos sistemas de información, actualizaciones y nuevas versiones.
A.14.3 Datos de prueba		
Objetivo: Asegurar la protección de los datos de prueba.		
A.14.3.1	Protección de los datos de prueba	*Control* Los datos de prueba se deben seleccionar con cuidado y deben ser protegidos y controlados.
A.15 Relación con proveedores		
A.15.1 Seguridad en las relaciones con proveedores		
Objetivo: Asegurar la protección de los activos de la organización que sean accesibles a los proveedores.		
A.15.1.1	Política de seguridad de la información en las relaciones con los proveedores	*Control* Los requisitos de seguridad de la información para la mitigación de los riesgos asociados con el acceso del proveedor a los activos de la organización deben acordarse con el proveedor y quedar documentados.
A.15.1.2	Requisitos de seguridad en contratos con terceros	*Control* Todos los requisitos relacionados con la seguridad de la información deben establecerse y acordarse con cada proveedor que puede acceder, tratar, almacenar, comunicar, o proporcionar componentes de la infraestructura de Tecnología de la Información.
A.15.1.3	Cadena de suministro de tecnología de la información y de las comunicaciones	*Control* Los acuerdos con proveedores deben incluir requisitos para hacer frente a los riesgos de seguridad de la información relacionados con las tecnologías de la información y las comunicaciones y con la cadena de suministro de productos.

A.15.2 Gestión de la provisión de servicios del proveedor		
Objetivo: Mantener un nivel acordado de seguridad y de provisión de servicios en línea con acuerdos con proveedores.		
A.15.2.1	Control y revisión de la provisión de servicios del proveedor	*Control* Las organizaciones deben controlar, revisar y auditar regularmente la provisión de servicios del proveedor.
A.15.2.2	Gestión de cambios en la provisión del servicio del proveedor	*Control* Se deben gestionar los cambios en la provisión del servicio, incluyendo el mantenimiento y la mejora de las políticas, los procedimientos y controles de seguridad de la información existentes, teniendo en cuenta la criticidad de los procesos y sistemas de negocio afectados así como la reapreciación de los riesgos.
A.16 Gestión de incidentes de seguridad de la información		
A.16.1 Gestión de incidentes de seguridad de la información y mejoras		
Objetivo: Asegurar un enfoque coherente y eficaz para la gestión de incidentes de seguridad de la información, incluida la comunicación de eventos de seguridad y debilidades.		
A.16.1.1	Responsabilidades y procedimientos	*Control* Se deben establecer las responsabilidades y procedimientos de gestión para garantizar una respuesta rápida, efectiva y adecuada a los incidentes de seguridad dela información.
A.16.1.2	Notificación de los eventos de seguridad de la información	*Control* Los eventos de seguridad de la información se deben notificar por los canales de gestión adecuados lo antes posible.
A.16.1.3	Notificación de puntos débiles de la seguridad	*Control* Todos los empleados, contratistas, terceras partes usuarias de los sistemas y servicios de información deben ser obligados a anotar y notificar cualquier punto débil que observen o que sospechen que exista, en los sistemas o servicios.
A.16.1.4	Evaluación y decisión sobre los eventos de seguridad de información	*Control* Los eventos de seguridad de la información deben ser evaluados y debe decidirse si se clasifican como incidentes de seguridad de la información.
A.16.1.5	Respuesta a incidentes de seguridad de la información	*Control* Los incidentes de seguridad de la información deben ser respondidos de acuerdo con los procedimientos documentados.
A.16.1.6	Aprendizaje de los incidentes de seguridad de la información	*Control* El conocimiento obtenido a partir del análisis y la resolución de incidentes de seguridad de la información debe utilizarse para reducir la probabilidad o el impacto de los incidentes en el futuro.
A.16.1.7	Recopilación de evidencias	*Control* La organización debe definir y aplicar procedimientos para la identificación recogida, adquisición y preservación de la información que puede servir de evidencia.

A.17 Aspectos de seguridad de la información para la gestión de la continuidad de negocio		
A.17.1 Continuidad de la seguridad de la información		
Objetivo: La continuidad de la seguridad de la información debe formar parte de los sistemas de gestión de la continuidad de negocio de la organización.		
A.17.1.1	Planificación de la continuidad de la seguridad de la información	*Control* La organización debe determinar sus necesidades de seguridad de la información y de continuidad para la gestión de la seguridad de la información en situaciones adversas, por ejemplo, durante una crisis o desastre.
A.17.1.2	Implementar la continuidad de la seguridad de la información	*Control* La organización debe establecer, documentar, implementar y mantener procesos, procedimientos y controles para asegurar el nivel requerido de continuidad de la seguridad de la información durante una situación adversa.
A.17.1.3	Verificación, revisión y evaluación de la continuidad de la seguridad de la información	*Control* La organización debe comprobar los controles establecidos e implementados a intervalos regulares para asegurar que son válidos y eficaces durante situaciones adversas.
A.17.2 Redundancias.		
Objetivo: Asegurar la disponibilidad de los recursos de tratamiento de la información.		
A.17.2.1	Disponibilidad de los recursos de tratamiento de la información	*Control* Los recursos de tratamiento de la información deben ser implementados con la redundancia suficiente para satisfacer los requisitos de disponibilidad.
A.18 Cumplimiento		
A.18.1 Cumplimiento de los requisitos legales y contractuales		
Objetivo: Evitar incumplimientos de las obligaciones legales, estatutarias, reglamentarias o contractuales relativas a la seguridad de la información o de los requisitos de seguridad.		
A.18.1.1	Identificación de la legislación aplicable y de los requisitos contractuales	*Control* Todos los requisitos pertinentes, tanto legales como regulatorios, estatutarios o contractuales, y el enfoque de la organización para cumplirlos, deben definirse de forma explícita, documentarse y mantenerse actualizados para cada sistema de información de la organización.
A.18.1.2	Derechos de Propiedad Intelectual (DPI)	*Control* Deben implementarse procedimientos adecuados para garantizar el cumplimiento de los requisitos legales, regulatorios y contractuales sobre el uso de materiales, con respecto a los cuales puedan existir derechos de propiedad intelectual y sobre el uso de productos de software patentados.

A.18.1.3	Protección de los registros de la organización	*Control* Los registros deben estar protegidos contra la pérdida, destrucción, falsificación, revelación o acceso no autorizados de acuerdo con los requisitos legales, regulatorios, contractuales y de negocio.
A.18.1.4	Protección y privacidad de la información de carácter personal	*Control* Debe garantizarse la protección y la privacidad de los datos, según se requiera en la legislación y la reglamentación aplicables.
A.18.1.5	Regulación de los controles criptográficos	*Control* Los controles criptográficos se deben utilizar de acuerdo con todos los contratos, leyes y regulaciones pertinentes.
A.18.2 Revisiones de la seguridad de la información		
Objetivo: Garantizar que la seguridad de la información se implementa y opera de acuerdo con las políticas y procedimientos de la organización.		
A.18.2.1	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, objetivos de control, controles, políticas, procesos y 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.18.2.2	Cumplimiento de las políticas y normas de seguridad	*Control* Los directivos deben asegurarse 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 y cualquier otro requisito de seguridad aplicable.
A.18.2.3	Comprobación del cumplimiento técnico	*Control* Debe comprobarse periódicamente que los sistemas de información cumplen las políticas y normas de seguridad de la información de la organización.

Auditoría

CertiProf®

Professional Knowledge

www.certiprof.com

Auditor

"*Proceso sistemático, independiente, documentado, para obtener evidencia y evaluarla objetivamente, con el fin de determinar en qué grado se cumplen los criterios de la auditoria*" ISO 19011

Sistemático: No aleatorio, las auditorías usualmente son una actividad planificada y programada.

Independiente: Los auditores son libres de seleccionar las áreas a auditar.

Documentado: El proceso de auditoría ha sido publicado como un procedimiento escrito.

Evidencia: Pruebas de lo indicado por el auditado.

Se cumplen: Ocurren realmente.

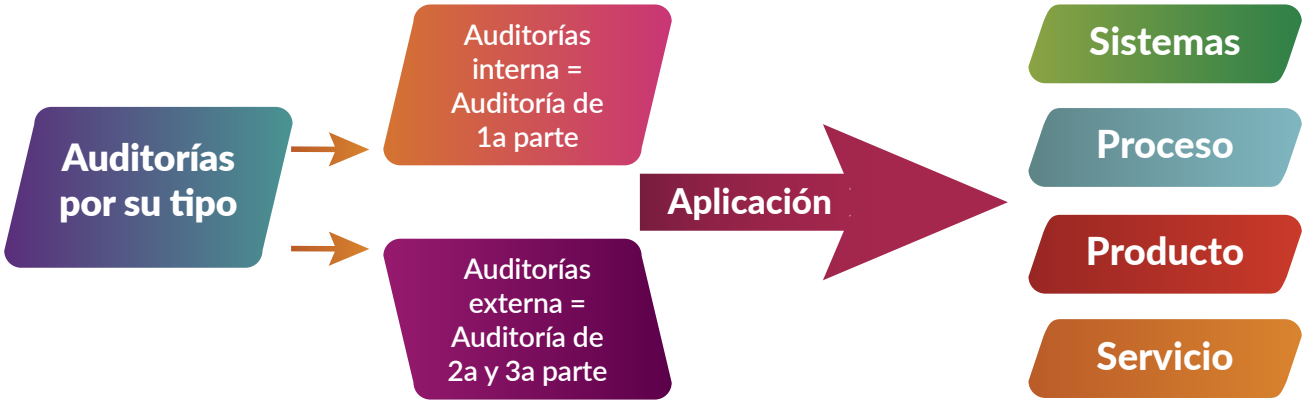
Evaluarla objetivamente: Comparar la evidencia con los criterios de auditoría, usando hechos antes que percepciones subjetivas, opiniones, sentimientos.

Criterios de auditoría: Los requisitos de la auditoría.

Términos y Definiciones ISO 19011:2011

Auditoría:

Es un proceso llevado a cabo por profesionales especialmente capacitados para el efecto, y que consiste en recoger, agrupar y evaluar evidencias para determinar si un sistema de información salvaguarda el activo empresarial, mantiene la integridad de los datos, lleva a cabo eficazmente los fines de la organización, utiliza eficientemente los recursos, y cumple con las leyes y regulaciones establecidas.



Tipos

- Primera parte
- Segunda parte
- Tercera parte

Criterios de Auditoría

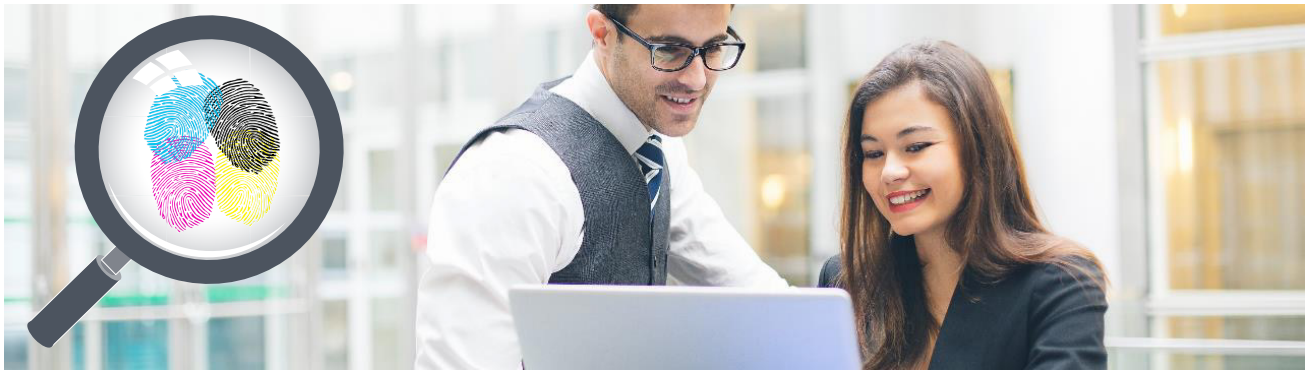
Grupo de políticas, procedimientos o requisitos usados como referencia y contra los cuales se compara la evidencia de auditoría.

Criterios:

- Normas (integral).
- Políticas.
- Procedimientos.
- Regulaciones.
- Legislación.
- Requisitos de la Norma.
- Requisitos contractuales.
- Códigos de conducta del sector comercial.

Evidencia de la Auditoría

Registros, declaraciones de hechos o cualquier otra información que son pertinentes para los criterios de auditoría y que son verificables.



Hallazgos de la Auditoría

Resultados de la evaluación de la evidencia de la auditoría recopilada frente a los criterios de auditoría, Si los criterios de auditoría son seleccionados de requisitos legales o de otra índole, los hallazgos de auditoría se denominan Cumplimiento o Incumplimiento.

- Hallazgo de cumplimiento.
- Requisitos (Norma, legal, reglamentario, contractual).
- El elemento se ajusta a la exigencia.
- La implantación corresponde a la intención.
- La implantación es eficaz.

Mejores prácticas:

- Verificar los hechos verbales.
- Definir la naturaleza de la no conformidad con el auditado, detallando la evidencia de auditoría.
- Tomar notas y consultarlas posteriormente para realizar el reporte.
- Hacer un bosquejo del reporte de hallazgos durante la toma de alimentos o al finalizar.
- Cada jornada y luego terminar en la revisión privada.

Conclusiones de la Auditoría

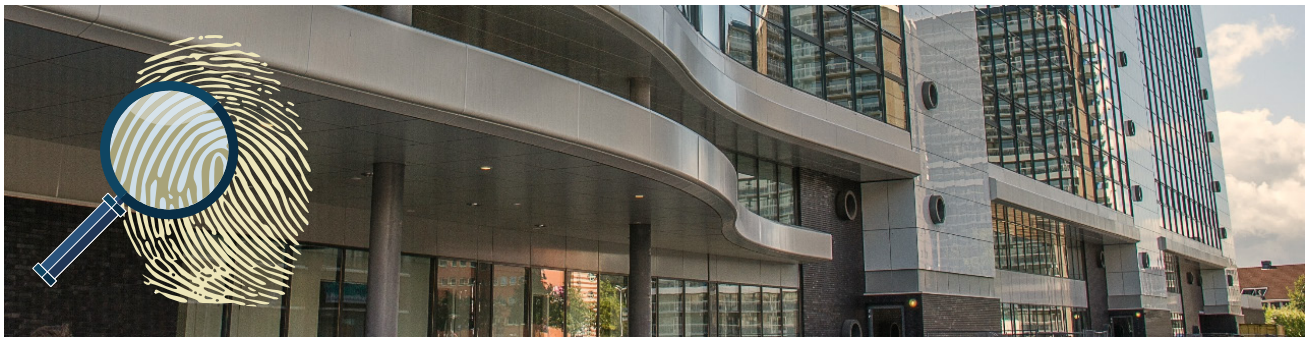
Resultado de una auditoría, tras considerar los objetivos de la auditoría y todos los hallazgos de la auditoría.

Cliente de la Auditoría

Organización o persona que solicita una auditoría.

Auditado

Organización que está siendo auditada.



Auditor

Persona que lleva a cabo una auditoría.

Equipo Auditor

Uno o más auditores que llevan a cabo una auditoría, con el apoyo, si es necesario, de expertos técnicos.

Experto Técnico

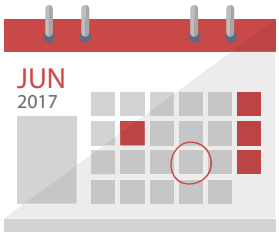
Persona que aporta conocimientos o experiencia específicos al equipo auditor.

Observador

Persona que acompaña al equipo auditor pero no audita.

Guía

Persona nombrada por el auditado para asistir al equipo auditor.



Programa de Auditoría

Conjunto de una o más auditorías planificadas para un periodo de tiempo determinado y dirigidas hacia un propósito específico.

Alcance de la Auditoría

Extensión y límites de una auditoría, el alcance de la auditoría incluye generalmente una descripción de las ubicaciones, las unidades de la organización, las actividades y los procesos, así como el período de tiempo cubierto.

Plan de Auditoría

Descripción de las actividades y de los detalles acordados de una auditoría.

Riesgo

Efecto de la incertidumbre en los objetivos.

Competencia

Habilidad para aplicar conocimientos y habilidades para alcanzar los resultados esperados.

Conformidad

Cumplimiento de un requisito.

★★★★★

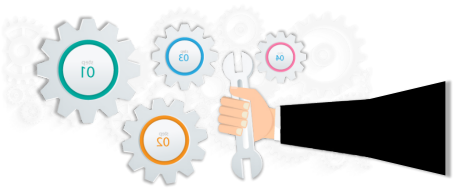
No Conformidad

Incumplimiento de un requisito.

★★★★★

Sistema de Gestión

Sistema para establecer políticas y objetivos y para alcanzar dichos objetivos.



Taller

Tiempo Estimado: 25 Minutos

CertiProf®

Professional Knowledge

www.certiprof.com

Programa de Auditoría

Auditorías	Enero	Febrero	Marzo	Abril	Mayo
Auditoría No. 1					
Auditoría No. 2					
Auditoría No. 3					
Auditoría No. 4					
Auditoría No. 5					

Principios de Auditoría

El Auditor

Conducta ética: (Profesionalidad), la confianza, integridad, confidencialidad y discreción son esenciales para el auditor.

Presentación ecuánime: Los hallazgos, conclusiones e informes de la auditoría reflejan con veracidad y exactitud las actividades de la auditoria.

Debido cuidado profesional: Actuar de acuerdo con la importancia de la tarea que desempeñan y la confianza depositada en ellos.

Atributos de los Auditores

Auditoría y Evidencia

Auditoría

Independencia:

Independencia de la actividad auditada. Deben mantenerse libres de cualquier perjuicio o conflicto de intereses.

Actitud objetiva para asegurarse de que los hallazgos y conclusiones de la auditoria están basados solo en evidencia de la auditoría.

Evidencia

Enfoque basado en la evidencia:

La evidencia de la auditoria es verificable. Basada en muestras de la información disponible.

El uso apropiado del muestreo esta estrechamente relacionado con la confianza que puede depositarse en las conclusiones de la auditoría.

Reunión de Apertura

- Presentación auditores al personal.
- Revisar alcance.
- Revisar objetivos de la auditoría interna.
- Confirmar Plan de auditoría.
- Registros de reunión de apertura.
- Proporcionar un breve resumen de cómo se llevarán a cabo las actividades de auditoría.
- Conductos oficiales de comunicación.
- Métodos utilizados en la auditoría.
- Necesidad de recursos especiales.
- Hora y fecha de reunión de cierre.
- Proporcionar al auditado la oportunidad de realizar preguntas.

Taller

Tiempo Estimado: 25 Minutos

CertiProf®

Professional Knowledge

www.certiprof.com

Establecer un Programa de Auditoría

Propósito:

- Presentación auditores al personal.
- Revisar alcance.
- Revisar objetivos de la auditoría interna.
- Confirmar Plan de auditoría.
- Registros de reunión de apertura.
- Proporcionar un breve resumen de cómo se llevarán a cabo las actividades de auditoría.
- Conductos oficiales de comunicación.
- Métodos utilizados en la auditoría.
- Necesidad de recursos especiales.
- Hora y fecha de reunión de cierre.
- Proporcionar al auditado la oportunidad de realizar preguntas.

Competencias de los Auditores

- Determinación de las competencias de auditor requeridas para satisfacer las necesidades del programa de auditoría.
- Establecimiento de criterios de evaluación del auditor.
- Selección del método apropiado de evaluación del auditor.
- Realización de la evaluación del auditor.
- Mantenimiento y mejora de la competencia del auditor.

Métodos de Auditoría Aplicables

Grado de interacción entre el auditor y el auditado	Ubicación del auditor	
	En sitio	Remota
Interacción humana	· Conducir entrevistas. · Completar listas de verificación y cuestinarios con la participación del auditado. · Revisión documental con participación del auditado. · Muestreo.	A través de medios de comunicación interactiva: · Entrevistas. · Completar listas de chequeo y cuestionarios. · Revisión documental con participación del auditado.
Sin interacción humana	· Revisión documental (Ej. Registros, análisis de datos). · Observación del trabajo realizado. · Visita del sitio. · Completar listas de verificación. · Muestreo (Ej. Productos).	· Revisión documental (Ej. Registros, análisis de datos). · Observación de trabajo a través de medios de vigilancia, teniendo en cuenta requisitos legales y sociales. · Análisis de datos.

Objetivos de la Auditoría Interna

Auditorías Internas

Todas las normas tienen como requisito realizar auditorías internas, a intervalos planificados, para determinar si el sistema de gestión cumple con los requisitos de esta parte del estándar que se esta auditando (Ejemplo. ISO/IEC 20000, ISO 22301 etc).

Las auditorias ayudan en la mejora continua de los sistemas de gestión.

Auditoría Interna Evidencia Objetiva

- Evidencia que existe.
- No influenciada por emociones o perjuicios.
- Puede ser documentada.
- Puede ser basada en la observación.
- Debe estar relacionada con el SGSI.
- Puede ser cuantificada y cualitativa.
- Puede verificarse.

Actividades de Auditoría

Inicio de Auditoría

- Revisión de Documentos.
- Preparación.
- Realización.
- Preparación y Entrega de Informes.
- Finalización.

Preparación de las Actividades Auditoría en Sitio

- Designación del jefe/líder.
- Definición, de los objetivos, alcance, criterios de auditoría.
- Determinación de la viabilidad de la auditoría.
- Selección de equipo auditor (auditor, auditores expertos).
- Establecimiento del contacto inicial con el auditado.
- Preparación del plan de auditoría.
- Asignación de tareas al equipo auditor.
- Preparación de los documentos de trabajo.

Responsabilidades del Auditor Líder

- Dirección del proceso de auditoría.
- Ayuda en la selección del personal del equipo.
- Responsable por todas las etapas de la auditoría.
- Preparar el plan de auditoría.
- Representación del equipo auditor ante la dirección.
- Preparación y entrega del informe final de auditoría.
- Dirección de las actividades de seguimiento.
- Trato de la información con la discreción debida.

Responsabilidades del Co-Auditor

- Conservar y salvaguardar la documentación de la auditoría.
- Reportar los resultados de la auditoría.
- Verificar la eficacia de las acciones aplicadas como resultado de la auditoría.
- Cumplir con el 100 % de los requisitos de auditoría.
- Realizar efectivamente las actividades asignadas.
- Documentar los hallazgos de auditoría.
- Cooperación y soporte al auditor.

Taller

Tiempo Estimado: 25 Minutos

CertiProf®

Professional Knowledge

www.certiprof.com

Preparación Individual del Auditor

- Lea los procedimientos con anticipación.
- Determina donde se realizan inspecciones.
- Utiliza listas de verificación.
- Conozca la responsabilidad y posición de las personas auditadas.
- Saber que pistas puede seguir.

Plan de Auditoría

- Objetivos y alcance.
- Documento de referencia.
- Lugares (direcciones) y contactos claves.
- Áreas o dependencias que serán auditadas.
- Determinación de las cláusulas claves para preparar la lista de verificación.
- Personas de contacto.
- Definición de los roles del grupo de auditores.
- Fechas.
- Hora y duración esperada para cada actividad principal.
- Programación de reuniones.
- Requisitos de confidencialidad.
- Distribución del informe y fecha esperada de la publicación.
- Elaboración y preparación de los documentos de trabajo.

Listas de Chequeo o Verificación

- Optimizar tiempo.
- Es una guía.
- Utilización de preguntas.
- Herramienta para recolección de evidencias.
- Ayuda para identificar elementos y procesos.
- Valorar el estado actual del SGCN.
- Adecuar las preguntas al proceso a ser auditado.

Preguntas Claves del Auditor

Tipo de Preguntas

CERRADAS

Suministran información puntual: un responsable, una fecha, un lugar SI / NO.

Las preguntas cerradas están diseñadas para obtener respuestas breves del auditado.

ABIERTAS

Permiten obtener descripciones de procesos o actividades.

Las preguntas abiertas estimulan al auditado a ser el que hable más, y así se reduce el número de preguntas que el auditor debe formular.

Cerradas

- ¿Realizaron auditorías internas?
- ¿Existe una política del sistema de gestión?
- ¿El sistema de gestión ha sido comunicado?
- ¿Es usted parte del grupo auditor interno?
- ¿El proceso se ejecuta como está documentado?

Abiertas

- ¿En donde registra la información?
- ¿Cuál procedimiento?
- ¿Conoce la política?
- ¿Cumple la legislación?

Recolección de Evidencia Objetiva

Obtener pruebas tangibles de que el sistema de calidad funciona correcta y eficazmente.

EVIDENCIA OBJETIVA

- Un procedimiento
- Un registro
- Verificación de observaciones

Ejecutando la Auditoría

- Haga un muestreo de actividades, no se centre en una.
- Busque evidencia observando lo que ocurre y revisando registros.
- Haga anotaciones completas.
- Escuche las explicaciones del auditado.
- Anote y confirme los hallazgos u observaciones. Si tiene dudas sobre el cumplimiento de un requisito podría hacer algunas preguntas abiertas adicionales.
- Siempre escriba los detalles de lo observado o evidenciado, por ejemplo, debería anotar el procedimiento auditado, los identificadores de los registros, numero de órdenes, identificación de lotes, códigos de documentos etc.
- Auditoría abierta y amigable resultará en un acuerdo de que el problema existe.
- Verifique si la No Conformidad es o no puntual.

Fuentes de Información

- Entrevistas con empleados y otras personas.
- Observación de actividades y ambiente de trabajo.
- Documentación.
- Política, objetivos, procedimientos, normas y riesgos.
- Actas de reunión, informes de auditoría, seguimiento y mediciones.
- Indicadores de gestión.
- Retroalimentación de partes interesadas.
- Bases de datos e Internet.

Realización de Entrevistas

- Sea Amigable.
- Haga sentir cómodo al auditado.
- Explicar las razones de la entrevista y de las notas tomadas.
- Iniciar con una descripción de las actividades.
- No realizar preguntas inductivas (Evita preguntas cuya respuesta sea SI o NO).
- Agradecer a los auditados.

Técnicas de Entrevista del Auditor

El auditor debe:

- Solicitar explicación de las situaciones.
- Escuchar cuidadosamente.
- Tener contacto cara a cara.
- Mostrarse interesado.
- Tomar nota en corto tiempo.
- Observar el lenguaje corporal.
- Hablar clara y cuidadosamente.
- Conocer sus preguntas.

El auditor debe:

- Ser sistemático al preguntar.
- Expresar en otra forma la pregunta si no es bien entendida.
- Usar preguntas abiertas y confirmar.
- Entender por completo.
- Agradecer al auditado.

Actitudes a Tomar para Controlar la Auditoría

Actitudes a tomar:

- Permanecer seguro.
- Administrar el tiempo adecuadamente.
- No dejarse conducir o engañar.
- Ser detallista y eficiente.
- Evitar apartarse del tema y saturarse.

Actitudes a evitar:

- Ser controvertido.
- Negativo.
- Crítico.
- Sarcástico.
- Discutir.
- Comparar al auditado.

¿Cómo entorpecer la Auditoría (Auditado)?

- Perdida de tiempo.
- Manejar al auditor.
- Situaciones inesperadas.
- Probar el carácter del auditor.
- Respuestas limitadas.
- Engañar al auditor.

Administración del Tiempo

- Realizar primero las actividades más complejas o difíciles.
- Asignar trabajo a los otros auditores.
- Adquirir el habito de hacerlo de inmediato.
- Conocer curva de cansancio del auditado y auditor.
- Establecer limite de tiempo y cumplirlo.
- Ser creativo.

Manejo de Situaciones Difíciles

- A la reunión de apertura no se presenta el responsable del proceso o actividad auditada.
- En la auditoría se tenía previsto visitar dos instalaciones y no hay disponibles vehículos, ni acompañantes.
- El auditado desvía la pregunta del auditor. Ejemplo: pregunta por la forma como se controlan los documentos y el auditado explica la forma como se controlan los registros, dado que los documentos son un tipo de registro.
- El auditado suministra poca información. Ejemplo: se solicita información sobre los resultados de enero a mayo y solo presenta los resultados del último mes.
- El auditado reformula las preguntas del auditor.
- El auditado cuestiona las preguntas del auditor. Ejemplo: lo que usted pregunta no tiene sentido.
- En la reunión de apertura no hay acuerdo con el objeto y alcance de la auditoría.

Resultados de la Auditoría

Hallazgo

- Resultados de la evaluación de la evidencia objetiva recopilada frente al conjunto de políticas, procedimientos o requisitos utilizados como referencia.
- Es registrado en la lista de verificación como respuesta a los cuestionamientos que han sido preparados.

Tipos de Hallazgos

No conformidad.

Incumplimiento de un requisito especificado.

Observación.

Situación que potencialmente puede afectar el sistema de gestión de calidad.

Incumplimientos más Comunes

- Documentación no encontrada.
- Competencias de recurso humano no evaluada.
- Controles implementados inadecuados.
- No conformidades por auditorías internas sin cierre eficaz.
- Acciones correctivas sin revisión de la dirección.
- Deficiencia en metodología de análisis de riesgo.
- Incumplimiento de procedimientos.

Taller

Tiempo Estimado: 25 Minutos

CertiProf®

Professional Knowledge

www.certiprof.com

La Reunión de Cierre

- Dirigida por el auditor líder.
- Es una actividad posterior a la actividad de campo.
- Permite presentar las conclusiones del equipo auditor al auditado y a la gerencia de la cual depende.
- Durante los primeros ciclos de auditoría se recomienda efectuar una reunión previa del equipo auditor para obtener consenso sobre no conformidades y observaciones.
- En la reunión de cierre únicamente se presentan las no conformidades y observaciones redactadas por consenso del equipo auditor.
- Debe darse énfasis a la obtención de un acuerdo con los auditados sobre no conformidades y observaciones identificadas por el equipo auditor.

Dirigida por el Auditor Líder

- Agradecimientos.
- Confirmar alcance, representante y dirección.
- Resumen del alcance de auditoria.
- No todas las No Conformidades se pueden descubrir.
- Objetivo y método usado.
- Preguntas y discusiones al final.
- Presentación de las No Conformidades por el equipo (hechos solamente).
- Explicación del seguimiento por el Auditor Líder.
- Acuerdo de las fechas para terminación de las acciones correctivas.
- Registros.
- Preguntas con respecto.

Informe de Auditoría

- Traduce fielmente las conclusiones de la reunión de cierre.
- Recuerda el objetivo y alcance de la auditoría.
- Indica la fecha de la auditoría.
- Define no conformidades puntuales.
- Puntos fuertes de la actividad auditada.

¿Qué no incluir en el informe de auditoría?

- Opiniones subjetivas.
- Información confidencial.
- Critica hacia individuos.
- Declaraciones ambiguas.
- Detalles triviales.
- Observaciones o no conformidades no discutidas en la reunión de cierre.

Plantilla de Informe

Auditoría No.
Fecha
Lugar
Auditor Líder
Auditor
Experto Técnico
Norma
Objetivos de la Auditoría
Procesos auditados y resultados de evidencia
Relación de los resultados y hallazgos
Firma de los auditores

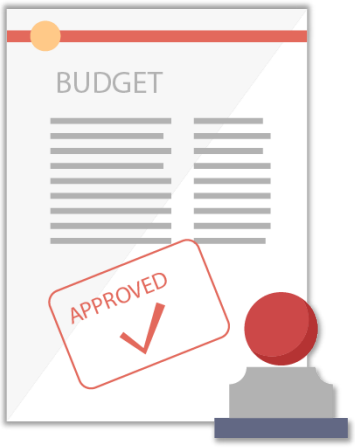
Acciones Correctivas

- Lectura de la no conformidad.
- Investigación del problema.
- Determinación de las causas fundamentales.
- Elaboración del plan de acción para corregirla.
- Actividades, responsable, recursos y fecha de ejecución.
- Fecha de seguimiento para cierre.
- Evaluación de la eficacia de la acción correctiva.
- Responsable del cierre.

Las Auditorías de Seguimiento

Responsabilidades del auditor:

- Acordar la fecha de la auditoría de seguimiento.
- Desarrollar la auditoría de seguimiento de acuerdo con las acciones correctivas y preventivas.
- Presentar e informar los resultados de la auditoría de seguimiento.
- Evaluar la eficacia de las acciones correctivas y preventivas implantadas.



Redacción de las No Conformidades

- **La Evidencia**

Lista de hallazgos, respaldados con evidencias objetivas o atestiguadas por el auditado.

- **La Referencia**

Al requisito de la norma y/o manual de calidad o procedimiento. Un requisito a la vez, el que más aplica.

- **La Conclusión**

Genérica, breve, precisa y aceptada por el auditado.

Formula de Redacción de No Conformidades

Reporte debe contener como mínimo:

- Una visión general del hallazgo.
- Descripción completa y precisa de lo observado.
- Ejemplos de la evidencia de auditoría.
- Referencia a la cláusula del estándar/documento de la organización.
- Explicación de los requisitos de la cláusula/documento.
- Las discrepancias deben atribuirse solamente a una cláusula de la norma, la más aplicable.
- En ocasiones, la única referencia es la documentación de la organización.

Fases de la Auditoría

Conclusiones

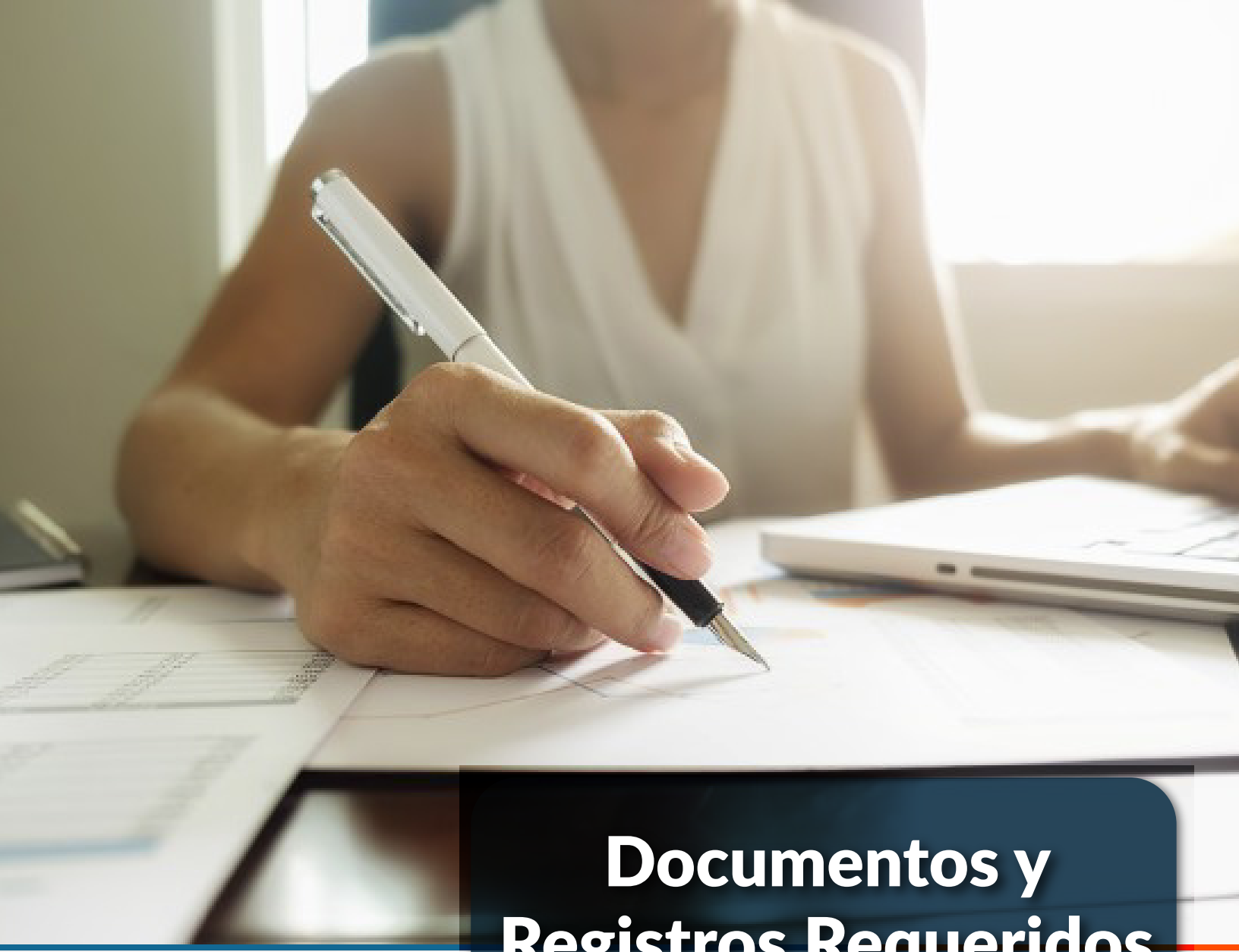
CertiProf®

Professional Knowledge

www.certiprof.com

Conclusiones

La continuidad del negocio no se limita a los sistemas de información, este va más allá, tomando en cuenta la integridad de las personas que laboran en la compañía ya que son ellas los que alimentan a los sistemas de información y por ende nuestro activo principal.



Documentos y Registros Requeridos por ISO 27001

CertiProf®

Professional Knowledge

www.certiprof.com

Documentos y Registros Requeridos por ISO 27001:2013

La lista a continuación muestra el conjunto mínimo de documentos y registros requeridos por ISO 27001: 2013.

Bajo las definiciones la norma se refiere a documentos y registros como información documentada.

Recuerde que los documentos del Anexo A son obligatorios solo si existen riesgos que requerirían su implementación.

Documentos y registros	Número de cláusula ISO 27001
Alcance del SGSI.	4.3
Política y objetivos de seguridad de la información.	5.2 y 6.2
Metodología de evaluación de riesgos y tratamiento de riesgos.	6.1.2
Plan de tratamiento de riesgos.	6.1.3 y 6.2
Informe de evaluación de riesgos.	8.2
Definición de roles y responsabilidades de seguridad.	A.7.1.2 y A.13.2.4
Inventario de activos.	A.8.1.1
Uso aceptable de activos.	A.8.1.3
Política de control de acceso.	A.9.1.1
Procedimientos operativos para la gestión de TI.	A.12.1.1

Principios de ingeniería de sistemas seguros.	A.14.2.5
Política de seguridad del proveedor.	A.15.1.1
Procedimiento de gestión de incidentes.	A.16.1.5
Procedimientos de continuidad del negocio.	A.17.1.2
Requisitos legales, reglamentarios y contractuales.	A.18.1.1
Registros de entrenamiento, habilidades, experiencia y calificaciones.	7.2
Resultados de monitoreo y medición.	9.1
Programa de auditoría interna.	9.2
Resultados de las auditorías internas.	9.2
Resultados de la revisión de la gestión.	9.3
Resultados de las acciones correctivas.	10.1
Registros de actividades del usuario, excepciones y eventos de seguridad.	A.12.4.1 y A.12.4.3

Prácticas Recomendadas

CertiProf®

Professional Knowledge

www.certiprof.com

Auditor/ Auditor Líder ISO 27001

Certiprof® en conjunto con algunos partners ha desarrollado el material base inicial de certificación en auditor en la norma ISO 27001.

Este material no es exhaustivo y es desarrollado con el fin de tener un fundamento para iniciar entrenamientos.

Muchas practicas pueden ser realizadas, recomendamos las siguientes durante la formación.

Prácticas Recomendadas ISO 27001

1. Analizar por parte de los candidatos los componentes de la cláusula 6.1 Y 6.2 de la norma.
2. Asignar a los candidatos la identificación de requisitos de la norma (debes).
3. Usando la norma buscar en ella la palabra “planes” o “plan” y hacer una lista.
4. Identificación de Documentos.
5. Identificación de Políticas.
6. Identificación de Procedimientos.
7. Se recomienda hacer lectura en grupos asignados de los controles del anexo A, pedir un análisis ligero donde se considere pensando en la empresa que trabajan o trabajaron que posibles controles no se debían incluir en el alcance de la implementación y explicar la razón.
8. Seleccionar una cláusula de la norma, asígnela a un grupo de 2 o 3 candidatos y hacer que se realice una lista de chequeo que se muestre al grupo.

Nota: Algunos entrenadores usan Post-it por cada documento identificado y los pegan en rotafolio durante el curso.

Los post-it se pueden agrupar bajo el tipo de documento.

Preguntas de Apoyo

CertiProf®

Professional Knowledge

www.certiprof.com

Preguntas de apoyo para el curso de CertiProf Certified ISO 27001 Auditor / Lead Auditor

Examen de ejemplo Selección Múltiple.

1. ¿Cuál de los siguientes no es un control del Anexo A?

A. Políticas de seguridad de la información.
B. La protección y la privacidad de los datos.
C. Políticas de continuidad del servicio.
D. Procedimientos y controles para asegurar el nivel requerido de continuidad de la seguridad de la información.

2. ¿Cuáles son controles del anexo A según la norma ISO 27001?

A. Derechos de Propiedad Intelectual (DPI).
B. Externalización del desarrollo de software.
C. Acuerdos de confidencialidad o no revelación.
D. Solo A y B.
E. Solo B y C.
F. A, B y C son correctas.

3. ¿Cuál es la definición de disponibilidad según la familia de normas ISO 27000?

A. Propiedad de ser accesible y estar listo para su uso o demanda de una entidad autorizada.
B. Propiedad consistente en que una entidad es lo que dice ser.
C. Propiedad de la información por la que se mantiene inaccesible.
D. Ninguna de la anteriores.

4. ¿Cuál de los siguientes no es un requisito explícito de la norma ISO 27001?

A. La información documentada incluye la información documentada requerida por esta norma internacional.
B. La organización debe establecer los objetivos de seguridad de la información en las funciones y niveles pertinentes.
C. Elaborar una “Declaración de Aplicabilidad” excluyendo los controles que no serán implementados.
D. La organización debe conservar información documentada sobre el proceso de tratamiento de riesgos de seguridad de la información.

5. ¿Basados en la ISO 19011, actividades dentro de la preparación de la auditoría incluyen?

A. Revisar la documentación.
B. Preparar el plan de auditoría.
C. Asignar el trabajo al equipo auditor.
D. Preparar los documentos de trabajo.
E. Ninguna de las anteriores, esto tópicos son de la etapa de conducir la auditoría.
F. Todas las anteriores.

6. ¿Cuál de las siguientes son parte de establecer el programa de auditoría?

A. Establecer competencia de la persona que gestiona el programa de auditoría.
B. Establecer la extensión del programa de auditoría.
C. Identificar y evaluar los riesgos del programa de auditoría.
D. Solo A y B.
E. Solo A y C.
F. A, B y C son correctas.

7. ¿Todos los controles del anexo A se deben implementar en un sistema de gestión de seguridad de la información?

A. VERDADERO.
B. FALSO.

8. ¿Cuál(es) son requisitos de documentación en la norma ISO 27001 y/o su anexo?

A. Declaración de aplicabilidad.
B. Plan de tratamiento de riesgos.
C. Informe de evaluación de riesgos.
D. Solo A y B.
E. Solo A y C.
F. A, B y C son correctas.

9. ¿Qué auditor es encargado de liderar el equipo de auditoría?

A. El Co-auditor.
B. El representante de la dirección.
C. El auditor líder.
D. El auditor interno.

10. ¿Forma parte del equipo auditor, pero no audita?

A. Auditor Junior.
B. Auditor Interno.
C. Observador.
D. Auditor Líder.

11. ¿Conjunto de una o más auditorias planificadas en un periodo?

A. Plan de auditoría.
B. Programa de auditoría.
C. Lista de chequeo general.
D. Sistema de gestión.

12. ¿Qué es una no conformidad en una auditoría?

A. El incumplimiento al plan de la auditoría planeada.
B. El no cumplimiento de un requisito de la norma.
C. Hacer una lista de chequeo y no usarla durante la auditoría.
D. Un requisito que el auditor cree que no se cumple y por eso no indaga sobre el.

13. ¿Son principios del auditor?

A. Discreción como parte de su comportamiento ético.
B. Exactitud en los informes de auditoría.
C. Debido cuidado profesional.
D. Todos los anteriores.

14. ¿Durante una reunión de apertura de auditoría de tercera parte se debe?

A. No existe auditoria de tercera parte.
B. Revisar el alcance.
C. Determinar que el único punto de contacto con el acreditador es el auditor líder.
D. No responder preguntas del proceso hasta no iniciar la auditoría.

15. ¿Dentro de los métodos de auditoría existen?

A. Auditoria remota.
B. Auditoria en sitio.
C. Solo A.
D. Solo B.
E. A y B son correctas.

16. Seleccione la mejor respuesta, las auditorías internas son realizadas al interior de una organización para:

A. Determinar la conformidad del sistema de gestión y determinar oportunidades de mejora.
B. Determinar la posibilidad de certificarse ante un proveedor de servicios.
C. Buscar incumplimientos bajo el criterio del auditor.
D. Dar cumplimiento al requisito de la norma.

17. Para auditores líderes de más de 3 años ejerciendo como auditor, es posible que por su experiencia no se hagan un plan de auditoría.

A. Falso.
B. Verdadero.

18. ¿Cómo se puede definir una lista de chequeo?

A. Listado exhaustivo de los requisitos de la norma.
B. Guía usada por el auditor para evaluar algunos requisitos de la norma.
C. Listado de actividades a realizar durante la reunión de apertura.
D. Insumo requerido para el programa de auditoría.

19. ¿Solo se documentan las no conformidades de un sistema de gestión si estas son mayores a dos?

A. Verdadero, porque dos no conformidades determinan que el sistema está fuera de control.
B. Verdadero, porque dos no conformidades son requeridas para no certificar un sistema.
C. Falso, todas las no conformidades se deben documentar.
D. Falso, solo a partir de 3 no cumplimientos de un requisito se documenta una no conformidad.

20. Se define como "Situación que potencialmente puede afectar el sistema de gestión de calidad."

A. No conformidad menor.
B. Hallazgo.
C. Observación.
D. Registro de Mejora.

21. ¿Durante una reunión de cierre de una auditoría externa NO se debe?

A. Hacer un resumen del proceso.
B. Explicar bajo la óptica del auditor líder por qué se incumplió el requisito.
C. Acordar fechas para cierre de acciones correctivas.
D. Confirmar el alcance de la auditoría.

22. ¿No son importantes en la redacción de no conformidades?

A. Las opiniones del auditor.
B. La evidencia.
C. La referencia a los requisitos de la norma.
D. La redactar sobre un requisito a la vez.

23. La norma ISO 27001, es la única forma como una compañía puede evaluar la capacidad de la organización para cumplir con sus propios requisitos de seguridad.

Falso.
Verdadero.

24. De acuerdo a la norma ISO 27001, Los requisitos de las partes interesadas que son relevantes para la seguridad de la información deben ser:

A. Requisitos internos.
B. Requisitos externos.
C. Requisitos contractuales.
D. Solo A y C.
E. Solo B y C.
F. A, B y C son correctas.

25. ¿Son parte del implementar el programa de auditoría?

A. Definir los objetivos, alcance y criterios para una auditoría individual.
B. Seleccionar los métodos de auditoría.
C. Seleccionar los miembros del equipo auditor.
D. Asignar responsabilidades para una auditoría individual al líder del equipo auditor.
E. Todos los anteriores.

26. ¿Son procedimientos documentados requeridos en la norma ISO 27001 o su anexo dependiendo de la declaración de aplicabilidad?

A. Procedimiento de gestión de incidentes.
B. Procedimientos de continuidad del negocio.
C. Procedimientos operativos para la gestión de TI.
D. Solo A y B.
E. Solo A y C.
F. Solo B y C.

27. ¿La norma ISO 27001 y/o su anexo donde aplique exige como requisito?

A. Programa de tratamiento de riesgos internos.
B. Plan de tratamiento de riesgos.
C. Cronograma de tratamiento de riesgos.
D. Política específica de tratamiento de riesgos.

28. ¿Son registros exigidos por la norma ISO 27001 o por la aplicación de un control del anexo?

A. Registros de entrenamiento, habilidades, experiencia y calificaciones.
B. Registros de eventos de seguridad.
C. Solo A.
D. Solo B.
E. A y B son registros requeridos.

29. ¿Son resultados exigidos por los controles de la norma que podrían ser sujetos de auditoría?

A. Resultados de monitoreo y medición.
B. Resultados de las auditorías internas.
C. Resultados de la revisión de la gestión.
D. Resultados de las acciones correctivas.
E. Todas son correctas excepto A.
F. Todas son correctas excepto C.
G. A, B, C y D son correctos.

30. ¿Es posible tener que crear una Política de control de acceso en el momento de aplicar controles de la Norma?

A. Verdadero
B. Falso

31. La Declaración de aplicabilidad es MEJOR resumida como:

A. Un requisito de la norma.
B. La forma de establecer que no se va a incluir en el alcance.
C. El principal documento a evaluar en una auditoría.
D. La justificación de las exclusiones de cualquiera de los controles del anexo A.

32. La organización debe determinar la necesidad de comunicaciones internas y externas que incluyan:

A. Quién comunica.
B. A quién se comunica.
C. Qué se comunica.
D. Todos los anteriores.

33. ¿El tamaño de la organización y su tipo de actividades, procesos, productos y servicios pueden determinar el alcance de la información documentada en la ISO 27001?

A. VERDADERO.
B. FALSO.

34. Los procesos contratados externamente estén fuera del alcance de control siempre y cuando se documente esto dentro de las exclusiones del sistema de gestión.

A. VERDADERO.
B. FALSO.

35. ¿Planificar, establecer, implementar y mantener un único programa de auditoría es requerido por la norma ISO 27001?

A. VERDADERO.
B. FALSO.

36. ¿El requisito de la norma frente a que la alta dirección que se refiere a que se debe revisar el sistema de gestión de la seguridad de la información de la organización, está establecido para hacerse?

A. Al menos cada seis meses.
B. Al menos en cada auditoría interna.
C. A intervalo planificados definidos en el sistema.
D. No se hace revisión del sistema de la seguridad de la información.

37. De acuerdo a la ISO 27001, basado en las tendencias actuales y manteniendo siempre en un enfoque proactivo no se debe excluir el control de Teletrabajo.

A. VERDADERO.
B. FALSO.

38. La siguiente es la definición de que concepto. "Evento singular o serie de eventos de la seguridad de la información, inesperados o no deseados".

A. Problema de seguridad de la información.
B. Incidencia de seguridad de la información.
C. Alerta de seguridad de la información.
D. Ninguna de las anteriores.

39. De acuerdo a la ISO 27000, la siguiente definición corresponde a:

Aplicaciones, servicios, activos de tecnologías de la información y otros compuestos para manejar información.

A. Sistema de seguridad de la información.
B. Sistema de información.
C. Sistema de gestión de seguridad de la información.
D. Ninguna de las anteriores.

40. La definición "Magnitud de un riesgo o combinación de riesgos, expresados en términos de la combinación de las consecuencias y de su probabilidad". Se refiere a:

A. Declaración de aplicabilidad.
B. Análisis de riesgos.
C. Nivel de riesgos.
D. Gestión de riesgos.

Respuestas

1. C
2. F
3. A
4. C
5. F
6. F
7. B
8. F
9. C
10. C
11. B
12. B
13. D
14. B
15. E
16. A
17. FALSO
18. B
19. C
20. C
21. B
22. A
23. FALSO
24. F
25. E
26. G
27. B
28. E
29. G
30. VERDADERO
31. A
32. D
33. VERDADERO
34. FALSO
35. FALSO
36. C
37. FALSO
38. B
39. B
40. C

Colaboradores en el desarrollo y revisión de
CERTIPROF CERTIFIED
ISO 27001 AUDITOR / LEAD AUDITOR
(I27001A/LA)

iSec
Seguridad de la información
Continuidad del negocio
Gobierno de TI

GOBERNACION DE
TECNOLOGIA DE INFORMACION

IT MLC

Con su ayuda logramos siempre **resultados extraordinarios.**

¡Gracias!

CERTIPROF CERTIFIED
ISO 27001 AUDITOR / LEAD AUDITOR
(I27001A/LA)

CertiProf®

Professional Knowledge

certiprof.com @Certiprof @CertiProf CertiProf Certiprof_llc

www.certiprof.com