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).