

Plan de

Implantación

De La

ISO/IEC 27001:2005

Índice

[Introducción 4](#_Toc358364842)

[Empresa 4](#_Toc358364843)

[TIC 5](#_Toc358364844)

[Seguridad 6](#_Toc358364845)

[Introducción a la ISO/IEC 27001:2005 7](#_Toc358364846)

[Gestión de la seguridad de la información 7](#_Toc358364847)

[Cuatro fases del sistema de gestión de seguridad de la información 7](#_Toc358364848)

[Documentos de ISO 27001 8](#_Toc358364849)

[La Fase de planificación 8](#_Toc358364850)

[La Fase de implementación 9](#_Toc358364851)

[La Fase de verificación 9](#_Toc358364852)

[La fase de mantenimiento y mejora 10](#_Toc358364853)

[Otras normas relativas a la ISO27001 relacionadas con seguridad de la información 10](#_Toc358364854)

[Certificación ISO 27001 11](#_Toc358364855)

[Introducción al Esquema Nacional de Seguridad 12](#_Toc358364856)

[Objetivos 12](#_Toc358364857)

[Elementos del Esquema Nacional de Seguridad 13](#_Toc358364858)

[Ámbito de aplicación 13](#_Toc358364859)

[Adecuación al Esquema Nacional de Seguridad 14](#_Toc358364860)

[Introducción a la documentación CCN-STIC 15](#_Toc358364861)

[Plan director de Seguridad. 16](#_Toc358364862)

[Análisis Diferencial 17](#_Toc358364863)

[Resumen de cumplimiento 20](#_Toc358364864)

[Alcance 21](#_Toc358364865)

[Declaración de Política de seguridad 22](#_Toc358364866)

[Procedimiento de auditorías internas. 23](#_Toc358364867)

[Gestión de indicadores. 24](#_Toc358364868)

[Gestión de roles y responsabilidades de seguridad 25](#_Toc358364869)

[Procedimiento revisión por dirección. 26](#_Toc358364870)

[Metodología de análisis de riesgos. 27](#_Toc358364871)

[Declaración de aplicabilidad. 28](#_Toc358364872)

[Glosario 29](#_Toc358364873)

# Introducción

## Empresa

Las Mutuas de Accidentes de Trabajo y Enfermedades Profesionales de la Seguridad Social, somos asociaciones de empresarios sin ánimo de lucro que tenemos como misión más importante cuidar de tus trabajadores cuando sufren un accidente de trabajo o una enfermedad profesional, facilitándoles asistencia sanitaria para su recuperación y prestación económica durante el tiempo que están sin desarrollar su trabajo.

En la actualidad somos 20 Mutuas que cuidamos de más de 14 millones de trabajadores de las más de 1.630.000 empresas asociadas a las Mutuas, prácticamente el 98% de las empresas

**Misión**

LAMUTUA es una entidad colaboradora de la Seguridad Social de ámbito nacional que, bajo las directrices del Ministerio de Trabajo, gestiona las contingencias encomendadas, y cuyo objeto es proporcionar la recuperación sanitaria y las prestaciones económicas al colectivo protegido (trabajadores de las empresas mutualistas y autónomos), con todos los recursos sanitarios y administrativos y con las alianzas establecidas con otras mutuas.

**Visión**

Ser una mutua afianzada a nivel nacional reconocida por sus altos niveles de fidelización de clientes basados en nuestra excelente calidad sanitaria y de servicio, en la cercanía y accesibilidad para con nuestros usuarios, y en la aportación a la mejora de la competitividad como socio estratégico de los mutualistas, con una eficiente gestión de recursos y con unos buenos profesionales, motivados e implicados en los objetivos de la entidad.

**Valores**

* Servicio a la Administración.
* Servicio al mutualista: accesibilidad, cercanía, profesionalidad y eficacia.
* Servicio a la sociedad.
* Desarrollo y crecimiento de nuestras personas para el logro y alineación de los objetivos.
* Establecimiento de alianzas para la mejora de nuestra competitividad.
* Orientación a resultados, conservando la honestidad, rigor, austeridad y credibilidad en nuestras actuaciones.
* Compromiso de mantener un sistema de Calidad basado en los requisitos de la Norma UNE-EN-ISO 9001-2008, extendiéndolo a toda la organización.

**Dimensión**

LAMUTUA atesora en su servicio como Entidad Colaboradora en todo el ámbito nacional, con unos excelentes recursos humanos, (una plantilla de 1.289 trabajadores) y con unos medios materiales que cuentan con más de 80 centros asistenciales y dos hospitales propios que destacan por su valor humano y sus avanzados medios sanitarios dando servicio a un colectivo protegido de 519.066 trabajadores que suponen la protección a más de 84.682 empresas, que confían en nosotros. En este sentido, LAMUTUA ha apostado decisivamente por la tecnología para potenciar y perfeccionar la integración entre sistemas médicos, la evolución hacia la Historia Clínica Electrónica o la creación y mejora continua de una extranet para nuestros mutualistas, bajo una optimización de recursos y una mejora productiva que repercuta eficazmente en los trabajadores protegidos por LAMUTUA.

## TIC

El departamento TIC ha sufrido una evolución constante en base a las necesidades de LAMUTUA, así como una adaptación a la evolución tecnológica del entorno, tratando de cubrir los requerimientos de la empresa de un modo eficiente, sin ignorar los peligros y dificultades que plantean cada día las nuevas tecnologías.

El departamento TIC se encarga de mantener y dar soporte a la totalidad del parque informático compuesto por más de 1000 puestos de trabajo distribuidos en 100 delegaciones.

También se encarga del desarrollo de las aplicaciones de negocio y la gestión de todos los servidores y servicios asociados.

Para todo ello cuenta con un equipo humano y una infraestructura tecnológica compuesta por un CPD principal sito en Ciudad Real y 1 **CPD** de respaldo con funcionalidad **Disaster&Recovery** ubicado en Barcelona.

El departamento TIC está estructurado en dos áreas principales:

* Desarrollo
	+ Análisis y desarrollo de aplicaciones.
	+ Mantenimiento correctivo y evolutivo de aplicaciones.
	+ Análisis de implantación y coordinación de aplicaciones de terceros.
* Sistemas
	+ Administración de servidores y servicios.
	+ Operaciones.
	+ Infraestructuras y telecomunicaciones.
	+ Seguridad técnica. Gestión de usuarios.
	+ Infraestructuras y telecomunicaciones.
	+ Video vigilancia.
	+ Backup. Disaster&Recovery.

## Seguridad

En lo referente a la seguridad LAMUTUA es consciente de la necesidad de cumplir con los requerimientos legales que marca la LOPD y dar solución al crecimiento de amenazas actuales.

Como reflejo de esta preocupación LAMUTUA ha emprendido las siguientes acciones:

* LAMUTUA dispone de un departamento jurídico dentro del cual están asignadas las funciones relativas al cumplimiento LOPD de forma específica.
* Acciones formativas relativas a LOPD y seguridad.
* Implantación de video vigilancia.
* Auditorias de seguridad externas:
	+ Hacking ético
	+ Auditorías de Seguridad de la Seguridad Social.
* Inclusión de normas específicas de seguridad en el “**Documento de Bienvenida**”
* Implicación de dirección y RRHH en la gestión de usuarios y accesos.
* Importante presupuesto económico para medidas de seguridad planteadas por TIC entre las que cabe destacar:
	+ Doble cada de Firewall de seguridad y contenidos.
	+ Antivirus administrado tanto interna como externamente.
	+ Formación específica del personal TIC e inclusión en grupos de seguridad como **ISMS Fórum Spain.**
	+ Monitorización constante de servidores y servicios.
	+ Sistema centralizado de logs.
	+ Disaster&Recovery.

Y por último la firme decisión de estandarizar la seguridad elaborando un **Plan Director de Seguridad** cuyo principal punto es la implementación de la **ISO/IEC 27001:2005** de forma gradual con el objetivo de la certificación de la norma.

## Introducción a la ISO/IEC 27001:2005

### Gestión de la seguridad de la información

La norma ISO 27001 define cómo organizar la seguridad de la información en cualquier tipo de organización, con o sin fines de lucro, privada o pública, pequeña o grande. Es posible afirmar que esta norma constituye la base para la gestión de la seguridad de la información.

La ISO 27001 es para la seguridad de la información lo mismo que la ISO 9001 es para la calidad: es una norma redactada por los mejores especialistas del mundo en el campo de seguridad de la información y su objetivo es proporcionar una metodología para la implementación de la seguridad de la información en una organización. También permite que una organización sea certificada, lo cual significa que una entidad de certificación independiente ha confirmado que la seguridad de la información se ha implementado en esa organización de la mejor forma posible.

A raíz de la importancia de la norma ISO 27001, muchas legislaciones han tomado esta norma como base para confeccionar las diferentes normativas en el campo de la protección de datos personales, protección de información confidencial, protección de sistemas de información, gestión de riesgos operativos en instituciones financieras, etc.

### Cuatro fases del sistema de gestión de seguridad de la información

La norma ISO 27001 determina cómo gestionar la seguridad de la información a través de un sistema de gestión de seguridad de la información. Un sistema de gestión de este tipo, igual que las normas ISO 9001 o ISO 14001, está formado por cuatro fases que se deben implementar en forma constante para reducir al mínimo los riesgos sobre confidencialidad, integridad y disponibilidad de la información.

Las fases son las siguientes:

* La Fase de planificación: esta fase sirve para planificar la organización básica y establecer los objetivos de la seguridad de la información y para escoger los controles adecuados de seguridad (la norma contiene un catálogo de 133 posibles controles).
* La Fase de implementación: esta fase implica la realización de todo lo planificado en la fase anterior.
* La Fase de revisión: el objetivo de esta fase es monitorear el funcionamiento del SGSI mediante diversos “canales” y verificar si los resultados cumplen los objetivos establecidos.
* La Fase de mantenimiento y mejora: el objetivo de esta fase es mejorar todos los incumplimientos detectados en la fase anterior.

El ciclo de estas cuatro fases nunca termina, todas las actividades deben ser implementadas cíclicamente para mantener la eficacia del SGSI.

### Documentos de ISO 27001

La norma ISO 27001 requiere los siguientes documentos:

* el alcance del SGSI;
* la política del SGSI;
* procedimientos para control de documentación, auditorías internas y procedimientos para medidas correctivas y preventivas;
* todos los demás documentos, según los controles aplicables;
* metodología de evaluación de riesgos;
* informe de evaluación de riesgos;
* declaración de aplicabilidad;
* plan de tratamiento del riesgo;
* registros.

La cantidad y exactitud de la documentación depende del tamaño y de las exigencias de seguridad de la organización; esto significa que una docena de documentos serán suficientes para una pequeña organización, mientras que las organizaciones grandes y complejas tendrán varios cientos de documentos en su SGSI.

### La Fase de planificación

Esta fase está formada por los siguientes pasos:

* determinación del alcance del SGSI;
* redacción de una Política de SGSI;
* identificación de la metodología para evaluar los riesgos y determinar los criterios para la aceptabilidad de riesgos;
* identificación de activos, vulnerabilidades y amenazas;
* evaluación de la magnitud de los riesgos;
* identificación y evaluación de opciones para el tratamiento de riesgos;
* selección de controles para el tratamiento de riesgos;
* obtención de la aprobación de la gerencia para los riesgos residuales;
* obtención de la aprobación de la gerencia para la implementación del SGSI;
* redacción de una declaración de aplicabilidad que detalle todos los controles aplicables, determine cuáles ya han sido implementados y cuáles no son aplicables.

### La Fase de implementación

Esta fase incluye las siguientes actividades:

* redacción de un plan de tratamiento del riesgo que describe quién, cómo, cuándo y con qué presupuesto se deberían implementar los controles correspondientes;
* implementación de un plan de tratamiento del riesgo;
* implementación de los controles de seguridad correspondientes;
* determinación de cómo medir la eficacia de los controles;
* realización de programas de concienciación y capacitación de empleados;
* gestión del funcionamiento normal del SGSI;
* gestión de los recursos del SGSI;
* implementación de procedimientos para detectar y gestionar incidentes de seguridad.

### La Fase de verificación

Esta fase incluye lo siguiente:

* implementación de procedimientos y demás controles de supervisión y control para determinar cualquier violación, procesamiento incorrecto de datos, si las actividades de seguridad se desarrollan de acuerdo a lo previsto, etc.;
* revisiones periódicas de la eficacia del SGSI;
* medición la eficacia de los controles;
* revisión periódica de la evaluación de riesgos;
* auditorías internas planificadas;
* revisiones por parte de la dirección para asegurar el funcionamiento del SGSI y para identificar oportunidades de mejoras;
* actualización de los planes de seguridad para tener en cuenta otras actividades de supervisión y revisión;
* mantenimiento de registros de actividades e incidentes que puedan afectar la eficacia del SGSI.

### La fase de mantenimiento y mejora

Esta fase incluye lo siguiente:

* implementación en el SGSI de las mejoras identificadas;
* toma de medidas correctivas y preventivas y aplicación de experiencias de seguridad propias y de terceros;
* comunicación de actividades y mejoras a todos los grupos de interés;
* asegurar que las mejoras cumplan los objetivos previstos.

### Otras normas relativas a la ISO27001 relacionadas con seguridad de la información

Además de la ISO 27001 (antiguamente BS 7799-2), la norma ISO 27002 (antiguamente ISO 17799) es una norma “auxiliar” que proporciona más información sobre cómo implementar los controles de seguridad especificados en la ISO 27001.

Otras normas que también pueden resultar útiles son la ISO 27005, que describe los procedimientos de evaluación de riesgos con mayor profundidad, y la [BS 25999-2](http://www.iso27001standard.com/index.php?option=com_content&view=article&id=303:sto-je-bs-25999-2&catid=9), que proporciona una descripción detallada de la gestión de la continuidad del negocio.

### Certificación ISO 27001

La norma ISO 27001, al igual que su antecesora BS 7799-2, es certificable.

Esto quiere decir que la organización que tenga implantado un SGSI puede solicitar una auditoría a una entidad certificadora acreditada y, caso de superar la misma con éxito, obtener una certificación del sistema según ISO 27001.

El número de certificaciones ha aumentado considerablemente en los últimos años como demostración de la relevancia que tiene la protección de la información para el desarrollo de las actividades de las organizaciones y para mantener y desarrollar el tejido industrial de los diferentes países y en todo el mundo.



Existe información regular aportada por ISO en el documento ISO Survey “database\_iso\_27001\_iso\_survey\_2011” donde se informa de manera detallada y a año vencido (p.ej. la publicación del año 2012 refleja los totales para el año 2011 completo) del resultado en el número de certificaciones acreditadas con referencia a las regiones, países, sectores industriales de mayor implantación, entre otros, tanto para ISO/IEC 27001 como para otros sistemas de gestión (ISO/IEC 9001, ISO 14001, ISO 22000, ISO 50001, entre otros).

## Introducción al Esquema Nacional de Seguridad

El Esquema Nacional de Seguridad (ENS), regulado por el Real Decreto 3/2010, de 8 de enero, determina la política de seguridad que se ha de aplicar en la utilización de los medios electrónicos. El ENS está constituido por los principios básicos y requisitos mínimos para una protección adecuada de la información. Será aplicado por las AA.PP. para asegurar el acceso, integridad, disponibilidad, autenticidad, confidencialidad, trazabilidad y conservación de los datos, informaciones y servicios utilizados en medios electrónicos que gestiones en el ejercicio de sus competencias.

### Objetivos

El Esquema Nacional de Seguridad (ENS) persigue los siguientes objetivos:

* Crear las condiciones necesarias de confianza en el uso de los medios electrónicos, a través de medidas para garantizar la seguridad de la información y los servicios electrónicos, que permita a los ciudadanos y a las Administraciones Públicas, el ejercicio de derechos y el cumplimiento de deberes a través de estos medios.
* Establecer la política de seguridad en la utilización de medios electrónicos en el ámbito de la Ley 11/2007, que estará constituida por los principios básicos y los requisitos mínimos para una protección adecuada de la información.
* Introducir los elementos comunes que han de guiar la actuación de las Administraciones públicas en materia de seguridad de las tecnologías de la información.
* Aportar un lenguaje común para facilitar la interacción de las Administraciones públicas, así como la comunicación de los requisitos de seguridad de la información a la Industria.
* Aportar un tratamiento homogéneo de la seguridad que facilite la cooperación en la prestación de servicios de administración electrónica cuando participan diversas entidades.
* Facilitar un tratamiento continuado de la seguridad.

En el Esquema Nacional de Seguridad se concibe la seguridad como una actividad integral, en la que no caben actuaciones puntuales o tratamientos coyunturales, debido a que la debilidad de un sistema la determina su punto más frágil y, a menudo, este punto es la coordinación entre medidas individualmente adecuadas pero deficientemente ensambladas.

### Elementos del Esquema Nacional de Seguridad

Los elementos principales del ENS son los siguientes:

* Los principios básicos a considerar en las decisiones en materia de seguridad.
* Los requisitos mínimos que permitan una protección adecuada de la información.
* El mecanismo para lograr el cumplimiento de los principios básicos y de los requisitos mínimos mediante la adopción de medidas de seguridad proporcionadas a la naturaleza de la información y los servicios a proteger.
* Las comunicaciones electrónicas.
* La auditoría de la seguridad.
* La respuesta ante incidentes de seguridad.
* La certificación de la seguridad.
* La conformidad.

El aspecto principal del ENS es, sin duda, que todos los órganos superiores de las AA.PP. deberán disponer de su política de seguridad que se establecerá en base a los principios básicos y que se desarrollará aplicando los requisitos mínimos.

### Ámbito de aplicación

Su ámbito de aplicación es el establecido en el artículo 2 de la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos.

Estarán excluidos los sistemas que tratan información clasificada regulada por Ley 9/1968 de 5 de abril, de Secretos Oficiales, modificada por Ley 48/1978, de 7 de octubre y normas de desarrollo

### Adecuación al Esquema Nacional de Seguridad

En la disposición transitoria del Real Decreto 3/2010 se articula un mecanismo escalonado para la adecuación a lo previsto en el Esquema Nacional de Seguridad de manera que los sistemas de las administraciones deberán estar adecuados a este Esquema en unos plazos en ningún caso superiores a 48 meses desde la entrada en vigor del mismo. El plazo de adecuación vence el 30 de enero de 2014.

La adecuación ordenada al Esquema Nacional de Seguridad requiere el tratamiento de las siguientes cuestiones:

* Preparar y aprobar la política de seguridad, incluyendo la definición de roles y la asignación de responsabilidades. (Véase CCN-STIC 805 Política de seguridad de la información)
* Categorizar los sistemas atendiendo a la valoración de la información manejada y de los servicios prestados.(Véase CCN-STIC 803 Valoración de sistemas en el Esquema Nacional de Seguridad)
* Realizar el análisis de riesgos, incluyendo la valoración de las medidas de seguridad existentes. (Véase Magerit versión 3 y programas de apoyo –Pilar)
* Preparar y aprobar la Declaración de aplicabilidad de las medidas del Anexo II del ENS. (Véase CCN-STIC 804 Medidas e implantación del Esquema Nacional de Seguridad)
* Elaborar un plan de adecuación para la mejora de la seguridad, sobre la base de las insuficiencias detectadas, incluyendo plazos estimados de ejecución. (Véase CCN-STIC 806 Plan de adecuación del Esquema Nacional de Seguridad)
* Implantar operar y monitorizar las medidas de seguridad a través de la gestión continuada de la seguridad correspondiente. (Véase serie CCN-STIC)
* Auditar la seguridad (Véase CCN-STIC 802 Auditoría del Esquema Nacional de Seguridad y CCN-STIC 808 Verificación del cumplimiento de las medidas en el Esquema Nacional de Seguridad).
* Informar sobre el estado de la seguridad (Véase CCN-STIC Métricas e Indicadores en el Esquema Nacional de Seguridad y CCN-STIC Informe del Estado de Seguridad.

### Introducción a la documentación CCN-STIC

Febrero de 2010 - El uso masivo de las tecnologías de la información y las telecomunicaciones (TIC), en todos los ámbitos de la sociedad, ha creado un nuevo espacio, el ciberespacio, donde se producirán conflictos y agresiones, y donde existen ciberamenazas que atentarán contra la seguridad nacional, el estado de derecho, la prosperidad económica, el estado de bienestar y el normal funcionamiento de la sociedad de las administraciones públicas.

La ley 11/2002, de 6 de mayo, reguladora del Centro Nacional de Inteligencia, encomienda al Centro Nacional de Inteligencia el ejercicio de las funciones relativas a la seguridad de las tecnologías de la información en su artículo 4.e) y de protección de la información clasificada en su artículo 4.f) a la vez que se confiere a su Secretario de Estado Director la responsabilidad de dirigir al Centro Criptológico Nacional en su artículo 9.2f)

Partiendo del conocimiento y la experiencia del CNI sobre amenazas y vulnerabilidades en la materia de riesgos emergentes, el Centro realiza, a través de su Centro Criptológico Nacional, regulado por el Real Decreto 421/2004, de 12 de marzo, diversas actividades directamente relacionadas con la seguridad de las TIC, orientada a la formación de personal experto, a la aplicación de políticas y procedimientos de seguridad, y al empleo de tecnologías de seguridad adecuadas.

Una de las funciones más destacables del Centro Criptológico Nacional es la de elaborar y difundir normas, instrucciones, guías y recomendaciones para garantizar la seguridad de los sistemas de las tecnologías de la información y las comunicaciones de la Administración, materializada en la existencia de la serie de documentos CCN-STIC.

Disponer de un marco de referencia que establezca las condiciones necesarias de confianza en el uso de los medios electrónicos es, además uno de los principios que establece la ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los servicios públicos en su artículo sobre el Esquema Nacional de Seguridad (ENS).

Precisamente el Real Decreto 3/2010, de 8 de enero, de desarrollo del Esquema Nacional de Seguridad fija los principios básicos y requisitos mínimos así como las medidas de protección para implantar en los sistemas de la Administración, y promueva la elaboración y difusión de guías de seguridad de las tecnologías de la información y las comunicaciones por parte de CCN para facilitar un mejor cumplimiento de dichos requisitos mínimos.

En definitiva, la serie de documentos CCN-STIC se elabora para dar cumplimiento a los cometidos del Centro Criptológico Nacional y a los reflejado en el Esquema Nacional de Seguridad, conscientes de la importancia que tiene el establecimiento de un marco de referencia en esta materia que sirva de apoyo para que el personal de la Administración lleve a cabo su difícil, y en ocasiones, ingrata tarea de proporcionar seguridad a los sistemas de las TIC bajo su responsabilidad.

# Plan director de Seguridad.

LAMUTUA encaminada en un trabajo de estandarización y Modelo **EFQM** de Excelencia ha decidido llevar a cabo la elaboración de un Plan Director de Seguridad que marque las directrices generales de la compañía en el ámbito de la seguridad.

Los objetivos a cumplir son los siguientes:

* Cumplimiento legal de las normativas referentes a seguridad en especial **LOPD**.
* Aseguramiento de la información y capacitación para dar un servicio eficiente y seguro a los mutualistas.
* Estandarización de normas de seguridad con la finalidad de ofrecer una imagen competitiva y evaluable del nivel de confianza.
* Identificación de **riesgos**.
	+ Este punto en sí mismo se considera desde la dirección de la empresa fundamental de cara a afrontar los próximos proyectos.
* Asegurar el cumplimiento en las auditorias llevadas a cabo por parte de la Seguridad Social.
* Prepararnos para acometer a corto plazo la certificación en la **ISO/IEC 27001:2005** y a medio plazo homologarnos dentro del esquema nacional de seguridad de cara a garantizar nuestra relación con las administraciones públicas y ciudadanos. Para cumplir este objetivo lo dividimos en tres fases en base a su alcance.
	+ Fase 1: Implantación de **ISO/IEC 27001:2005** en sistemas críticos definidos por TIC y acordados con Dirección General.
	+ Certificación de Fase 1.
	+ Fase 2: Implantación de **ISO/IEC 27001:2005** en resto de procesos TIC y procesos de negocio afectados por procesos TIC.
	+ Certificación Fase 2.
	+ Implantación esquema nacional seguridad.

Los medios asignados para cumplir dichos objetivos son los siguientes:

* Creación el **Comité de Seguridad** cuya principal responsabilidad será alcanzar las metas propuestas y cuyas responsabilidades y funciones quedan fijadas en el documento “Responsabilidades y funciones del Comité Seguridad”.
* Designación del nuevo puesto de trabajo**. Responsable de Seguridad de la Información**.
* Asignación anual de una partida presupuestaria al **SGSI**.
* Compromiso firme de la **Dirección General** con el **SGSI**.

# Análisis Diferencial

Vamos a enfrentar la situación actual de LAMUTUA frente a las principales cláusulas de seguridad de la norma 27001. Así mismo vamos a marcar en base a los **Dominios** de la **ISO 27002** los **Objetivos de control** que no están implantados sin tener en cuenta **el alcance** objeto de certificación.

* **Evaluación y tratamiento del riesgo**.
	+ No dispone de una gestión de inventario apropiada para la gestión del riesgo ni tampoco de una gestión de riesgo ni política aproximada.
		- 4.- Incumple X
* **Política de seguridad**.
	+ No dispone de una política de seguridad específica y detallada más allá de algunas matizaciones en el documento de bienvenida de los empleados.
		- 5 .1 Política de seguridad de la información. Incumple. X
* **Aspectos organizativos de la seguridad**.
	+ Existe un departamento específico de LOPD dependiente del área jurídica de la organización que se encarga de las principales tareas de cumplimiento legal. No existe la figura de responsable de seguridad en la organización si bien las funciones son asumidas por el personal de TIC sin una asignación de roles específicos.
		- 6.1 Organización interna. Parcialmente. **P**
		- 6.2 Terceros. Parcialmente. **P**
* **Gestión de activos**.
	+ No existe un plan de gestión de activos.
		- 7.1 Responsabilidad sobre los activos. Incumple. X
		- 7.2 Clasificación de la información. Incumple. X
* **Seguridad en recursos humanos**.
	+ Hay cierto grado de concienciación respecto a la problemática de seguridad pero no es determinante ni asumida por el departamento de Recursos Humanos.
		- 8.1 Antes del empleo. Incumple. X
		- 8.2 Durante el empleo. Parcialmente. **P**
		- 8.3 Cese del empleo o cambio de puesto de trabajo. Parcialmente. **P**
* **Seguridad física y ambiental**.
	+ Se toman gran cantidad de medidas en ambos aspectos.
		- 9.1 Áreas seguras. Cumple. **√**
		- 9.2 Seguridad de los equipos. Cumple. **√**
* **Gestión de comunicaciones y operaciones**.
	+ Existe un área específica dotada de medios personales y técnicos para tal fin.
		- 10.1 Responsabilidades y procedimientos de operación. Cumple. **√**
		- 10.2 Gestión de la provisión de servicios por terceros. Parcialmente. **P**
		- 10.3 Planificación y aceptación del sistema. Parcialmente. **P**
		- 10.4 Protección contra el código malicioso y descargable. Cumple. **√**
		- 10.5 Copias de seguridad. Cumple. **√**
		- 10.6 Gestión de la seguridad de las redes. Cumple. **√**
		- 10.7 Manipulación de los soportes. Parcialmente. **P**
		- 10.8 Intercambio de información. Incumple. X
		- 10.9 Servicios de comercio electrónico. No aplica.
		- 10.10 Supervisión. Cumple. **√**
* **Control de accesos**.
	+ Existe una política de control de acceso y unos roles definidos en la organización si bien no existen controles de seguimiento.
		- 11.1 Requisitos de negocio para el control de acceso. Cumple. **√**
		- 11.2 Gestión de acceso de usuario. Cumple. **√**
		- 11.3 Responsabilidades de usuario. Cumple. **√**
		- 11.4 Control de acceso a la red. Cumple **√**
		- 11.5 Control de acceso al sistema operativo. Cumple. **√**
		- 11.6 Control de acceso a las aplicaciones y la información. Cumple. **√**
		- 11.7 Ordenadores portátiles y teletrabajo. Parcialmente. **P**
* **Adquisición desarrollo y mantenimiento de sistemas de información**.
	+ Las medidas de seguridad no son un factor clave en las decisiones de adquisición si bien se exigen unas medidas mínimas excluyentes en este sentido.
		- 12.1 Requisitos de seguridad de los sistemas de información. Parcialmente. **P**
		- 12.2 Tratamiento correcto de las aplicaciones. Incumple. X
		- 12.3 Controles criptográficos. Parcialmente. **P**
		- 12.4 Seguridad de los archivos de sistema. Cumple. **√**
		- 12.5 Seguridad en los procesos de desarrollo y soporte. Parcialmente. **P**
* **Gestión de incidentes de la seguridad de información**.
	+ No existe una política relativa a los incidentes de seguridad. Hay relación con terceros para las acciones legales derivadas de estos incidentes si bien no existe un protocolo de actuación.
		- 13.1 Notificación de eventos y puntos débiles de la seguridad de la información. Incumple X
		- 13.2 Gestión de incidentes y mejoras de la seguridad de la información. Incumple X
* **Gestión de continuidad de negocio**.
	+ Hay un CPD de respaldo y una gestión de Disaster&Recovery si bien no se basa en ninguna política definida de actuación
		- 14.1 Aspectos de la seguridad de la información en la gestión de continuidad de negocio. Parcialmente. **P**
* **Cumplimiento legal.**
	+ Hay un departamento de LOPD que se encarga de llevar el cumplimiento a tal fin. No se toman medidas en otras normativas como puede ser el Esquema Nacional de Seguridad lo cual si bien puede ser requerido debido a la relación con las administraciones públicas sería de gran valor.
		- 15.1 Cumplimiento de los requisitos legales. Cumple. **√**
		- 15.2 Cumplimiento de las políticas de normas de seguridad y cumplimiento técnico. Incumple X
		- 15.3 Consideraciones sobre las auditorias de los sistemas de información. Incumple. X

## Resumen de cumplimiento

A modo de resumen como visión general del estado de la seguridad podemos presentar los siguientes datos acerca de los Objetivos de control reflejados en la ISO 27002.

Incumple: 11 Parcialmente: 12 Cumple: 15 No aplica: 1

# Alcance

Siguiendo las instrucciones definidas en el **Plan Director de Seguridad** de LAMUTUA el departamento TIC, de acuerdo con Dirección General, ha seleccionado los sistemas críticos que deberán ser cubiertos en esta Fase 1.

Desde dirección se ha decidido que es crítico para la empresa velar por la seguridad de los datos y la gestión de los mismos, por lo tanto el alcance será:

**Los sistemas de información que dan soporte a la administración y acceso de los datos de las BBDD consideradas críticas en la organización.**

Aquí se contemplan dichos sistemas y los procesos en los que son críticos:

* **Administración de los servidores y servicios de BBDD que contienen las BBDD críticas.**
	+ Administración y operaciones CPD
	+ Administración y operaciones Servidores
	+ Securización servidores.
* **Administración de los servidores y servicios de aplicaciones que acceden a estos datos.**
	+ Administración y operaciones CPD
	+ Administración y operaciones Servidores
	+ Securización servidores.
	+ Backup y Continuidad Negocio Datos y servicios.
* **Gestión de accesos.**
	+ Solicitud y gestión de cuentas de usuario.
* **Securización telecomunicaciones.**
	+ Securización accesos Servidores y servicios.
* **Gestión de logs que permitan investigar incidentes.**
	+ Administración y operación de Servidores.
	+ Securización servidores.

# Declaración de Política de seguridad

LAMUTUA y el Comité de dirección General somos conscientes de la importancia que tiene la seguridad de los sistemas de información de ahora en adelante SGSI para poder alcanzar los objetivos de nuestra empresa, ser eficientes y poder proyectar una imagen competitiva ante nuestros clientes y colaboradores.

Entre los objetivos principales que debemos alcanzar están:

* **El cumplimiento normativo**, con especial incidencia en LOPD asegurando los derechos ARCO de nuestros clientes.
* **Aseguramiento de la información** y capacitación para dar un servicio adecuado eficiente y seguro a los mutualistas.
* **Estandarización de normas de seguridad** con la finalidad de ofrecer una imagen competitiva ante nuestros clientes y colaboradores.

Todos los trabajadores de LAMUTUA debemos colaborar en la consecución de estos objetivos y para ello desde el Comité de Dirección General queremos mostrar nuestro compromiso firme con la seguridad de los sistemas de información, ofreciendo nuestro apoyo al nuevo Responsable de Seguridad y solicitando vuestra más estrecha colaboración y desempeño en las tareas que por su parte sean requeridas.

Para tal fin se ha desarrollado una normativa de obligado cumplimiento “**Documento: Política de seguridad**” y se van a desarrollar una serie de acciones formativas continuadas al respecto, cuya programación podréis consultar y acordar con vuestros responsables.

*Desde la Dirección General queremos animaros a todos a continuar trabajando cada día para conseguir llevar a esta nuestra empresa al máximo nivel de excelencia empresarial que todos deseamos.*

Documentos asociados:

**Política de seguridad.docx**

# Procedimiento de auditorías internas.

Desde Dirección se aprueba la ejecución periódica de dos tipos de auditorías con finalidades distintas y complementarias.

* **Auditoría de comprobación de la idoneidad del SGSI respecto la ISO 27001**
* **Auditoría de Hacking ético.**

Con la finalidad de comprobar la idoneidad del SGSI regularmente establecemos un plan de Auditorías Internas que comenzará a ejecutarse una vez obtenida la certificación de la norma ISO 27001. Este plan de auditorías nos ayudará a mantener el estado de certificación y poder crecer en los aspectos relativos al SGSI.

Para comprobar el estado de seguridad y la validez de los controles y medidas tomadas así como adecuar los sistemas de seguridad a las nuevas amenazas se decide ejecutar un plan de auditorías de hacking ético bajo la dirección del departamento TIC

La ejecución de las auditorías internas se hará en base al documento “**Procedimiento de auditorías internas**”.

El resultado de estas auditorías se pondrá en conocimiento de Dirección General y serán determinantes en las decisiones y proyectos a seguir.

Documentos asociados:

**Procedimiento de auditorías internas.docx**

# Gestión de indicadores.

Para que el sistema se mantenga vivo y actualizado, es necesario evaluar su eficacia de forma continuada. Para ello, se deben establecer indicadores que permitan controlar el funcionamiento de las medidas de seguridad de la información implantadas, así como su eficacia y eficiencia, y definir los mecanismos y la periodicidad de medida de dichos indicadores.

La efectividad del SGSI está proporcionalmente relacionada con la efectividad de los controles implantados.

Para disponer de información sobre la eficacia de los controles, es imprescindible implantar indicadores que nos proporcionen dicha información. Los indicadores seleccionados y su procedimiento de ejecución se encuentran detallados en el documento “**Gestión de indicadores”**.

El resultado de estos indicadores será un factor clave para revisar la implantación de los controles y su revisión y seguimiento será una tarea clave.

Documentos asociados:

**Gestion de indicadores.docx**

# Gestión de roles y responsabilidades de seguridad

La asignación de responsabilidades sobre seguridad de la información debe hacerse en concordancia con la información de la política de seguridad.

Las responsabilidades para la protección de activos individuales y para llevar a cabo procesos de seguridad específicos deben ser claramente identificadas por los responsables departamentales y los responsables de procesos. Esta asignación, debería completarse, dónde sea necesario, con una guía más detallada para ubicaciones, sistemas o servicios específicos.

Los propietarios de los activos de información pueden delegar sus responsabilidades de seguridad en terceros a título individual o en proveedores de servicios. Sin embargo, el propietario sigue manteniendo la responsabilidad última sobre la seguridad del activo y está capacitado para determinar que cualquier responsabilidad delegada se ha cumplido correctamente.

La Dirección de LAMUTUA decide crear una estructura jerárquica de roles de seguridad para que sean estos los encargados de asignar las responsabilidades de seguridad sobre los activos y procesos de la organización.

Esta definición de roles se define en el documento: “**Gestión de roles y responsabilidades de seguridad”** y es de obligado conocimiento para todos los trabajadores conocer los responsables y responsabilidades que tenemos sobre los activos que utilizamos en el desempeño de nuestro trabajo.

Documentos asociados:

**Gestión de roles y responsabilidades de seguridad**

# Procedimiento revisión por dirección.

En base al firme compromiso mostrado por parte del comité de Dirección General el seguimiento del SGSI pasa a formar parte de la agenda ordinaria de las reuniones del Comité.

Las decisiones tomadas por parte de la Dirección General en este sentido quedarán recogidas en acta y serán de obligado cumplimiento por parte de la compañía.

De forma extraordinaria a la agenda ordinaria se establece una revisión anual la primera semana del mes de mayo del estado del SGSI que deberá seguir el procedimiento que a continuación se detalla en el documento “**Revisión por dirección”.**

Documentos asociados:

**Revision por dirección.docx**

# Declaración de aplicabilidad.

En cumplimiento de la normativa marcada por la ISO 27001 y atendiendo al alcance definido por LAMUTUA el Comité de Seguridad ha elaborado el documento de “**Declaración de aplicabilidad**” que incluye todos los controles de Seguridad establecidos en la Organización, con el detalle de su aplicabilidad.

En este documento se definen que controles deberán ser aplicados y cuales quedan excluidos. Aquellos controles que queden excluidos serán de forma motivada y aplica solo a la FASE 1 determinada por Dirección General.

Documentos asociados:

**Declaracion de aplicabilidad.docx**

# Metodología de análisis de riesgos.

La gestión de los riesgos es una piedra angular en las guías de buen gobierno [ISO 38500], público o privado, donde se considera un principio fundamental que las decisiones de gobierno se fundamenten en el conocimiento de los riesgos que implican.

Para realizar el análisis de riesgos nos hemos basado en el modelo MAGERIT.

Esta norma establece los principios para el uso eficaz, eficiente y aceptable de las tecnologías de la información. Garantizando que sus organizaciones siguen estos principios ayudará a los directores a equilibrar riesgos y oportunidades derivados del uso de las TI

En pocas palabras, **la gestión de los riesgos es nuclear al gobierno de las organizaciones**.

Los riesgos que tienen su origen en el uso de tecnologías de la información deben trasladarse a los órganos de gobierno y contextualizarse en la misión de la organización.

MAGERIT es la metodología de análisis y gestión de riesgos elaborada por el Consejo Superior de Administración Electrónica, como respuesta a la percepción de que la Administración, y, en general, toda la sociedad, dependen de forma creciente de las tecnologías de la información para el cumplimiento de su misión.

MAGERIT interesa a todos aquellos que trabajan con información digital y sistemas informáticos para tratarla. Si dicha información, o los servicios que se prestan gracias a ella, son valiosos, MAGERIT les permitirá saber cuánto valor está en juego y les ayudará a protegerlo.

Conocer el riesgo al que están sometidos los elementos de trabajo es, simplemente, imprescindible para poder gestionarlos.

Con MAGERIT se persigue una aproximación metódica que no deje lugar a la improvisación, ni dependa de la arbitrariedad del analista.

El análisis de riesgos ejecutado podemos encontrarlo en el documento “**Análisis de riesgos”**

Documentos asociados:

**Analisis de riesgos.docx**

# Gestión del riesgo / Propuestas de proyectos

Tras este análisis se procederá a estudiar los resultados y proponer los Proyectos de Gestión de Riesgos. Estos proyectos se indican en el documento “**Propuestas de proyectos”.**

A raíz de los resultados obtenidos en el análisis de riesgos LAMUTA se plantea la necesidad de hacer un plan de mitigación de riesgos.

Este plan de mitigación de riegos que se basa en los resultados obtenidos en el análisis debe basarse en cifras reales y que estén aseguradas en el tiempo, en concreto nos tenemos que asegurar que las salvaguardas que LAMUTUA tiene desplegadas cumplan su función y a ser posible mejoren en eficiencia.

Pese a las salvaguardas desplegadas, el resultado de análisis de riesgos nos muestra que hay valores de análisis de riesgos que deben ser mitigados de inmediato con la aplicación de nuevas salvaguardas de imprescindible aplicación y cuya efectividad potencial ya se ha calculado y aprobado.

Ambos proyectos deben cumplir el ciclo de Deming para poder integrarlos dentro del SGSI.

Con la finalidad de cumplir estos requerimientos LAMUTUA ha desarrollado dos proyectos:

**1.- Normalización, optimización y aseguramiento de salvaguardas actuales.**

**2.- Implantación de salvaguardas imprescindibles**.

Documentos asociados:

**Propuestas de proyectos.docx**

# Auditoria de cumplimiento.

El objetivo de esta auditoría de cumplimiento es evaluar la madurez de la seguridad en lo que respecta a los diferentes dominios de control y los controles planteados por la ISO/IEC 27002:2005.

El estudio debe realizar una revisión de los controles planteados por la norma para cumplir con los diferentes objetivos de control para cada uno de los dominios.

Esta estimación la realizaremos según el Modelo de Madurez de la Capacidad (CMM).

El proceso de auditoría de cumplimiento lo hemos dividido en tres fases:

* **Auditoría documental.**
* **Auditoría in situ.**
* **Resultados de auditoría.**

El proceso de ejecución y los resultados se recogen en el documento “**Auditoría de cumplimiento**”

Documentos asociados:

**Auditoria de cumplimiento.docx**

# Glosario

|  |  |
| --- | --- |
| **Aceptación del riesgo**  | Decisión informada a favor de tomar un riesgo. [UNE-ISO Guía 73:2010] |
| **Acreditación**  | Acción de facultar a un sistema o red de información para que procese datos sensibles, determinando el grado en el que el diseño y la materialización de dicho sistema cumplen los requerimientos de seguridad técnica preestablecidos. [CESID:1997] Accreditation: Formal declaration by the responsible management approving the operation of an automated system in a particular security mode using a particular set of safeguards. |
| **Activo**  | Componente o funcionalidad de un sistema de información susceptible de ser atacado deliberada o accidentalmente con consecuencias para la organización. Incluye: información, datos, servicios, aplicaciones (software), equipos (hardware), comunicaciones, recursos administrativos, recursos físicos y recursos humanos. [UNE 71504:2008] Recursos del sistema de información o relacionados con éste, necesarios para que la Organización funcione correctamente y alcance los objetivos propuestos por su dirección. [Magerit: 2006] Recursos del sistema de información o relacionados con éste, necesarios para que la Organización funcione correctamente y alcance los objetivos propuestos por su dirección. [Magerit:1997] Bienes: En la teoría de los valores, la realidad que posee un valor positivo y por ello es estimable. [DRAE] |
| **Amenaza**  | Causa potencial de un incidente que puede causar daños a un sistema de información o a una organización. [UNE 71504:2008] |
| **Amenaza**  | Causa potencial de un incidente que puede causar daños a un sistema de información o a una organización. [UNE 71504:2008] Eventos que pueden desencadenar un incidente en la Organización, produciendo daños materiales o pérdidas inmateriales en sus activos. [Mage-rit:2006] Eventos que pueden desencadenar un incidente en la Organización, produciendo daños materiales o pérdidas inmateriales en sus activos. [Magerit:1997] |
| **Amenaza:**  | Causa potencial de un incidente no deseado que puede resultar en daño al sistema u organización. [ISO/IEC 13335-1:2004] |
| **Análisis de impacto**  | Estudio de las consecuencias que tendría una parada de X tiempo sobre la Organización. |
| **Análisis de riesgos**  | Proceso sistemático para estimar la magnitud de los riesgos a que está expuesta una Organización. |
| **Análisis de riesgos**  | Proceso sistemático para estimar la magnitud de los riesgos a que está expuesta una Organización. Análisis del riesgo – Proceso que permite comprender la naturaleza del riesgo y determinar el nivel de riesgo. [UNE-ISO Guía 73:2010] Identificación de las amenazas que acechan a los distintos componentes pertenecientes o relacionados con el sistema de información (conocidos como ‘activos’); para determinar la vulnerabilidad del sistema ante esas amenazas y para estimar el impacto o grado de perjuicio que una seguridad insuficiente puede tener para la organización, obteniendo cierto cono-cimiento del riesgo que se corre. [Magerit:1997] |
| **Ataque**  | Intento de destruir, exponer, alterar o inhabilitar un sistema de información o la información que el sistema maneja, o violar alguna política de seguridad de alguna otra manera. [ISO/IEC 18043:2006] Cualquier acción deliberada encaminada a violar los mecanismos de seguridad de un sistema de información. [CESID:1997] |
| **Auditoría de seguridad**  | Estudio y examen independiente del historial y actividades de un sistema de información, con la finalidad de comprobar la idoneidad de los controles del sistema, asegurar su conformidad con la estructura de seguridad y procedimientos operativos establecidos, a fin de detectar brechas en la seguridad y recomendar cambios en los procedimientos, controles y estructuras de seguridad. |
| **Autenticidad**  | Propiedad o característica consistente en que una entidad es quien dice ser o bien que garantiza la fuente de la que proceden los datos. [UNE 71504:2008] Aseguramiento de la identidad u origen. [Magerit:2006] |
| **Certificación**  | Confirmación del resultado de una evaluación, y que los criterios de evaluación utilizados fueron correctamente aplicados. |
| **Confidencialidad**  | Propiedad o característica consistente en que la información ni se pone a disposición ni se revela a individuos, entidades o procesos no autorizados. |
| **Contra medida**  | Véase salvaguarda. |
| **Control** | Herramienta de la gestión del riesgo, incluidas políticas, pautas, estructuras organizacionales, que pueden ser de naturaleza administrativa, técnica, gerencial o legal. |
| **Declaración de aplicabilidad**  | Documento formal en el que, para un conjunto de salvaguardas, se indica sin son de aplicación en el sistema de información bajo estudio o si, por el contrario, carecen de sentido. |
| **Degradación**  | Pérdida de valor de un activo como consecuencia de la materialización de una amenaza. |
| **Dimensión de seguridad**  | Un aspecto, diferenciado de otros posibles aspectos, respecto del que se puede medir el valor de un activo en el sentido del perjuicio que causaría su pérdida de valor. |
| **Disponibilidad**  | Aseguramiento de que los usuarios autorizados tienen acceso cuando lo requieran a la información y sus activos asociados. [UNE 71504:2008] Característica que previene contra la denegación no autorizada de acceso a activos del dominio.  |
| **Estado de riesgo**  | Informe: Caracterización de los activos por su riesgo residual; es decir lo que puede pasar tomando en consideración las salvaguardas desplegadas. |
| **Evaluación de salvaguardas**  | Informe: Evaluación de la eficacia de las salvaguardas existentes en relación al riesgo que afrontan. |
| **Evaluación del riesgo**  | Proceso general de análisis y evaluación del riesgo. [ISO/IEC Guide 73:2002] |
| **Evento de seguridad de información:**  | Es una ocurrencia identificada de un sistema, servicio, o red el cual indica una posible brecha de la política de seguridad de información o fallas de las salvaguardias o una situación desconocida que puede ser relevante para la seguridad. [ISO/IEC 18044-1:2004] |
| **Frecuencia**  | Tasa de ocurrencia de una amenaza. Número de sucesos o defectos en una unidad de tiempo definida |
| **Gestión de riesgos**  | Actividades coordinadas para dirigir y controlar una organización en lo relativo al riesgo. [UNE-ISO Guía 73:2010] Selección e implantación de salvaguardas para conocer, prevenir, impedir, reducir o controlar los riesgos identificados. [Magerit:2006] Selección e implantación de las medidas o ‘salvaguardas’ de seguridad adecuadas para conocer, prevenir, impedir, reducir o controlar los riesgos identificados y así reducir al mínimo su potencialidad o sus posibles perjuicios. La gestión de riesgos se basa en los resultados obtenidos en el análisis de los riesgos. [Magerit:1997] |
| **Gestión del riesgo** | Actividades coordinadas para dirigir y controlar una organización considerando el riesgo. |
| **Impacto**  | Consecuencia que sobre un activo tiene la materialización de una amenaza. Consecuencia – Resultado de un suceso que afecta a los objetivos. [UNE-ISO Guía 73:2010] Consecuencia que sobre un activo tiene la materialización de una amenaza. |
| **Impacto residual**  | Impacto remanente en el sistema tras la implantación de las salvaguardas determinadas en el plan de seguridad de la información. |
| **Incidente de seguridad**  | Suceso (inesperado o no deseado) con consecuencias en detrimento de la seguridad del sistema de información. [UNE 71504:2008] Evento con consecuencias en detrimento dela seguridad del sistema de información. |
| **Incidente de seguridad de información** | Es indicado por una o varias series de eventos inesperados y no deseados que tienen una gran probabilidad de comprometer las operaciones de negocios y de amenazar la seguridad de información.  |
| **Informe de insuficiencias**  | Informe: Ausencia o debilidad de las salvaguardas que aparecen como oportunas para reducir el riesgo sobre el sistema. |
| **Instalaciones de proceso de información:** | Sistemas de información, servicio o infraestructura, o locaciones físicas que los almacena. |
| **Integridad**  | Propiedad o característica consistente en que el activo no ha sido alterado de manera no autorizada. [UNE 71504:2008] Característica que previene contra la modificación o destrucción no autorizadas de activos del dominio. [Magerit:1997]  |
| **Mapa de riesgos**  | Informe: Relación de las amenazas a que están expuestos los activos. |
| **Medida de seguridad**  | Véase salvaguarda. |
| **Modelo de valor**  | Informe: Caracterización del valor que representan los activos para la Organización así como de las dependencias entre los diferentes activos. |
| **Pauta:** | Descripción que aclara que es lo que se debe hacer y como se hace, con el fin de alcanzar los objetivos planteados en las políticas. [ISO/IEC 13335-1:2004] |
| **Plan de seguridad**  | Conjunto de proyectos de seguridad que permiten materializar las decisiones de gestión de riesgos. |
| **Política:**  | Dirección general y formal expresada por la gerencia.  |
| **Probabilidad**  | Probabilidad – Posibilidad de que un hecho se produzca. [UNE-ISO Guía 73:2010] NOTA 1 – En la terminología de la gestión del riesgo, la palabra “probabilidad” se utiliza para indicar la posibilidad de que algún hecho se produzca, que esta posibilidad está definida, medida o determinada objetiva o subjetivamente, cualitativa o cuantitativamente, y descrita utilizando términos generales o de forma matemática [tales como una probabilidad o una frecuencia sobre un periodo de tiempo dado]. |
| **Proyecto de seguridad**  | Agrupación de tareas orientadas a tratar el riesgo del sistema. La agrupación se realiza por conveniencia, bien porque se trata de tareas que en singular carecerían de eficacia, bien porque se trata de tareas con un objetivo común, bien porque se trata de tareas que competen a una única unidad de acción. |
| **Riesgo**  | Estimación del grado de exposición a que una amenaza se materialice sobre uno o más activos causando daños o perjuicios a la Organización. Efecto de la incertidumbre sobre la consecución de los objetivos. [UNE-ISO Guía 73:2010] Posibilidad de que se produzca un impacto determinado en un activo, en un dominio o en toda la Organización. [Magerit:1997] |
| **Riesgo acumulado**  | Dícese del calculado tomando en consideración el valor propio de un activo y el valor de los activos que depende de él. Este valor se combina con la degradación causada por una amenaza y la frecuencia estimada de la misma.  |
| **Riesgo potencial**  | Riesgos potenciales. Los riesgos del sistema de información en la hipótesis de que no hubiera salvaguardas presentes.  |
| **Riesgo repercutido**  | Dícese del calculado tomando en consideración únicamente el valor propio de un activo. Este valor se combina con la degradación causada por una amenaza y la frecuencia estimada de la misma, medidas ambas sobre activos de los que depende.  |
| **Riesgo residual**  | Riesgo remanente en el sistema después del tratamiento del riesgo. [UNE-ISO Guía 73:2010] Riesgo remanente en el sistema tras la implantación de las salvaguardas determinadas en el plan de seguridad de la información. [Magerit:2006] Riesgo que se da tras la aplicación de salvaguardas dispuestas en un escenario de simulación o en el mundo real.  |
| **Salvaguarda**  | Procedimiento o mecanismo tecnológico que reduce el riesgo. Control: Medida que modifica un riesgo.  |
| **Seguridad**  | La capacidad de las redes o de los sistemas de información de resistir, con un determinado nivel de confianza, los accidentes o acciones ilícitas o malintencionadas que comprometan la disponibilidad, autenticidad, integridad y confidencialidad de los datos almacenados o transmitidos y de los servicios que dichas redes y sistemas ofrecen o hacen accesibles. [  |
| **Seguridad de la información**  | Confianza en que los sistemas de información están libres y exentos de todo peligro o daño inaceptables. [UNE 71504:2008]  |
| **Seguridad de la información** | Preservación de la confidencialidad, integridad y disponibilidad de la información, así mismo, otras propiedades como la autenticidad, no rechazo, contabilidad y confiabilidad también pueden ser consideradas. |
| **Sistema de información**  | Los ordenadores y redes de comunicaciones electrónicas, así como los datos electrónicos almacenados, procesados, recuperados o transmitidos por los mismos para su operación, uso, protección y mantenimiento. Conjunto organizado de recursos para que la información se pueda recoger, almacenar, procesar (tratar), mantener, usar, compartir, distribuir, poner a disposición, presentar o transmitir. [UNE 71504:2008] Conjunto de elementos físicos, lógicos, elementos de comunicación, datos y personal que permiten el almacenamiento, transmisión y proceso de la información. [Magerit:1997]  |
| **Terceros** | Persona que es reconocida por ser independiente de las partes involucradas concerniente al tema en cuestión. [ISO/IEC Guide 73:2002] |
| **Tratamiento del riesgo**  | Proceso de selección e implementación de medidas para modificar el riesgo. [ISO/IEC Guide 73:2002] |
| **Trazabilidad**  | Aseguramiento de que en todo momento se podrá determinar quién hizo qué y en qué momento. [UNE 71504:2008] Propiedad o característica consistente en que las actuaciones de una entidad pueden ser imputadas exclusivamente a dicha entidad. [ISO/IEC 7498-2:1989] Responsabilidad: Cualidad que permite que todas las acciones realizadas sobre un sistema de tecnología de la información sean asociadas de modo inequívoco a un individuo o entidad. [CESID:1997] Accountability: Process of tracing information system activities to a responsible source. [CNSS:2003]  |
| **Valor**  | De un activo. Es una estimación del coste inducido por la materialización de una amenaza. Cualidad que poseen algunas realidades, consideradas bienes, por lo cual son estimables. [DRAE]  |
| **Valor acumulado**  | Considera tanto el valor propio de un activo como el valor de los activos que dependen de él. Bienes de abolengo: Los heredados de los abuelos. [DRAE]  |
| **Valoración del riesgo**  | Proceso de comparación del riesgo estimado contra el criterio del riesgo dado para determinar el significado de este. [ISO/IEC Guide 73:2002] |
| **Vulnerabilidad**  | Defecto o debilidad en el diseño, implementación u operación de un sistema que habilita o facilita la materialización de una amenaza. Propiedades intrínsecas de que algo se produzca como resultado de una sensibilidad a una fuente de riesgo que puede conducir a un suceso con una consecuencia. [UNE-ISO Guía 73:2010]  |

# Bibliografía

**Norma técnica peruana:** EDI. Tecnología de la información. Código de buenas prácticas para la gestión de la seguridad de la información. EDI. Information technology. Code of practice for information security management. (EQV. ISO/IEC 17799:2005 Information technology. 2007-01-16 – (2ª Edición).

**MAGERIT – versión 3.0:** Ministerio de Hacienda y Administraciones Públicas Secretaría General Técnica Subdirección General de Información, Documentación y Publicaciones Centro de Publicaciones

* Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información Libro I – Método.
* Metodología de Análisis y Gestión de Riesgos de los Sistemas de información Libro II - Catálogo de Elementos.
* Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información Libro III - Guía de Técnicas.

**Wikipedia**: [www.wikipedia.es](http://www.wikipedia.es)

**El portal de ISO 27001 en español:** [www.iso27000.es/](http://www.iso27000.es/)

**IS&BCA:** [www.iso27001standard.com](http://www.iso27001standard.com)

**Centro Criptológico Nacional:** [www.ccn.cni.es](http://www.ccn.cni.es)