Máster Interuniversitario en Seguridad de las TIC (MISTIC)

UOC *7 de junio de 2013*

Memoria

Elaboración de un Plan de Implementación de la ISO/IEC 27001:2005

Alumno:
Enrique Pedro Marín Escuer

Director:
Antonio José Segovia Henares

Resumen

Tenemos que entender 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.

Esta actividad integral debe verse soportada por normas internacionalmente reconocidas como la ISO 27001:2005, que dará soporte, confiabilidad y trazará un plan de mejora continua de la seguridad.

Este trabajo de fin de Master Interuniversitario en Seguridad de las TIC, trata de elaborar un Plan de Implementación de la ISO/IEC 27001:2005, en una empresa del sector de las Mutuas de Accidentes de Trabajo de la Seguridad Social.

Comenzaremos identificando la situación actual referente a la seguridad de la empresa, confrontándola con la norma ISO 27001, para ir elaborando la documentación necesaria que dará soporte a nuestro Sistema de Gestión de Seguridad de la Información destacando dentro de esta documentación la Política de Seguridad.

Desarrollaremos el Análisis de Riesgos, que será la piedra angular del proyecto ya que conocer el riesgo al que están sometidos los elementos de trabajo es, simplemente, imprescindible para poder gestionarlos.

Una vez conocidos los riesgos, procederemos a gestionarlos, elaborando proyectos de gestión de riesgos que nos permitan mejorar la seguridad de una forma eficiente, sin dejar lugar a la improvisación ni al derroche de recursos.

Summary

We need to understand security as an integral activity in specific actions that do not fit or cyclical treatments, because the weakness of a system is determined by its most fragile and often, this point is the coordination between individual measures adequate but poorly assembled.

This activity should be supported by comprehensive internationally recognized standards such as ISO 27001:2005, which will support, reliability and outline a plan of continuous safety improvement.

This work order Interuniversity Master in ICT security, try to develop a Plan of Implementation of the ISO / IEC 27001:2005, a company in the sector of the Mutual Workers' Compensation Social Security.

Begin by identifying the current situation concerning the safety of the company, comparing it to ISO 27001, to be preparing the necessary documentation that will support our Safety Management System of Information within this documentation highlighting the Security Policy.

Risk Analysis will develop, which will be the cornerstone of the project and to know the risk they are subjected work items is simply essential to manage them.

Once known proceed to manage risks, developing risk management projects, that allow us to improve the security of an efficient way, without leaving room for improvisation or the waste of resources.

Introducción

El punto de partida es una empresa y su necesidad de cubrir con garantías los aspectos relativos a la seguridad de la información. En concreto se trata de una Mutua de Accidentes de Trabajo de la Seguridad Social y su objetivo no es tan solo cubrir los aspectos relativos a la seguridad, sino además hacerlo dentro de un marco de excelencia empresarial.

Para ello debemos entender la seguridad tal y como la he descrito en el resumen anterior y como la define el Esquema Nacional de Seguridad, 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.

Por todo esto necesitamos elaborar un Sistema de Gestión de Seguridad de la Información que se soporte en una metodología contrastada que cubra las expectativas de la empresa.

La metodología que aporta este proyecto es la ISO/IEC 27001:2005. Se trata de 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.

Los objetivos a cubrir con la implantación de la ISO/IEC 27001:2005 son los siguientes:

- Enmarcar la Seguridad dentro de la cultura y gestión de la organización.
- Garantizar la confidencialidad, disponibilidad e integración de la información de la organización. De esta manera ésta puede cumplir sus objetivos, tanto de negocio como contractual y legal.
- Establecer una metodología de la gestión de la información que sea clara y eficiente.
- Que los usuarios accedan a la información de manera segura y con total confianza.
- Reduce el riesgo de uso malicioso de la información.
- Exige el establecimiento de unos objetivos de seguridad medibles y un criterio de mejora continua para ellos (Ciclo de Deming-PDCA)
- Los riesgos son controlados constantemente.
- Garantiza el cumplimiento de las leyes en materia de gestión de la información.
- Conciencia a la organización sobre la importancia de la seguridad.

Una de las claves fundamentales en la implantación de la ISO/IEC 27001:2005 es el análisis de riesgos. Este análisis de riesgos debe de hacerse de una forma metódica y estandarizada que permita ser evaluada y reproducida y cuyo resultado sea cuantificable.

La metodología empleada para el análisis de riesgos será Magerit en su versión 3. 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.

El resultado de utilizar esta metodología nos asegura que el resultado será confiable y preciso sin dejar lugar a la improvisación ni las interpretaciones y ello nos permitirá calcular los riesgos a los que están expuestos los activos de nuestra compañía.

Un correcto análisis de riesgos nos permitirá una eficiente gestión de los mismos.

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

Está gestión de riesgos se reflejara en proyectos que permitirán mejorar la seguridad de la compañía y reducir de este modo el riesgo al que están expuestos nuestros activos.

Por lo tanto conoceremos nuestros activos y los riesgos a los que están sometidos y podremos actuar en consecuencia.

Esta metodología solo es eficaz si se mantiene en el tiempo y se audita su estado de forma continua tal y como marca el ciclo de Deming.

Por lo tanto finalmente someteremos nuestra implantación a una auditoria de cumplimiento frente a la norma. 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 de seguridad.

Para realizar dicha medición nos basaremos en el Modelo de Madurez de la Capacidad (CMM).

El resultado nos dará una visión del cumplimiento de la norma y lo que es más importante, nos identificará aquellos puntos en los que la incumplimos.

ISO 27001:2005

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.

LAMUTUA

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.

TIC

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 50 trabajadores, un CPD principal sito en Ciudad Real y 1 CPD de respaldo con funcionalidad Disaster&Recovery ubicado en Barcelona.

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.

Un análisis inicial de seguridad sobre los principales controles de seguridad de los diferentes dominios de seguridad que establece la norma arroja como resultado que:

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

Documentos ISO 27001.

La norma ISO 27001 requiere los siguientes documentos:

- Alcance del SGSI
- Política del SGSI
- Procedimiento de auditorías internas
- Gestión de indicadores
- Gestión de roles y responsabilidades de seguridad
- Procedimiento de revisión por dirección
- Metodología de evaluación de riesgos
- Análisis de riesgos
- Declaración de aplicabilidad
- Gestión de riesgos.

Todos estos documentos son fundamentales y requeridos para la implantación de la ISO 27001 y quedan recogidos en el proyecto.

Alcance / Declaración de aplicabilidad

Podemos resumir el alcance definido por LAMUTUA de la siguiente manera:

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

En base a esta definición se definen cuáles de los 130 controles propuestos por la ISO 27001 son de aplicación y cuales quedan excluidos de forma motivada.

Como resumen podemos decir que LAMUTUA ha seleccionado 99 controles para ser aplicados quedando excluidos un total de 31.

Política SGSI

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.

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.**

Gestión de indicadores

Se desarrollan un total de 13 indicadores que tratan de medir la eficiencia de los controles implantados en los diferentes dominios de seguridad.

Gestión de roles y responsabilidades de seguridad

Se determina la creación de un Comité de seguridad formado por responsables de las diferentes áreas de la empresa.

Se decide crear la figura de Responsable de seguridad y dotarle de funciones específicas dentro de la empresa siendo el máximo responsable en el área de seguridad y cuya principal misión es la elaboración y mantenimiento del SGSI.

Procedimiento de revisión por dirección

El principal objetivo es involucrar a la Dirección General de LAMUTUA en el proceso de seguridad y que se la Dirección General la que tome las decisiones utilizando para ello una metodología concreta definida por la ISO 27001.

Análisis de riesgos

Se tratará en más profundidad a continuación.

Gestión de riesgos.

Se tratará en más profundidad a continuación.

Análisis de Riesgos

El análisis de riesgos lo hemos dividido en las siguientes fases:

- Valoración de activos
    - Valoración propia
    - Valoración acumulada

- Dimensiones
    - Factor de los activos en cada dimensión
    - Valor de los activos en cada dimensión

- Valoración de amenazas

- Salvaguardas

- Estimación del riesgo
    - Riesgo residual con salvaguardas actuales
    - Riesgo residual con salvaguardas potenciales
    - Resumen simplificado

La metodología utilizada para el cálculo de cada proceso es Magerit en su versión 3.

Valoración de activos

Valores propios y valores acumulados

Activo	Valor propio	Valor acumulado
Administración y Operación Servidores	10000	165000
Administración y Gestión aplicaciones.	10000	35000
Administración y Operación BBDD	25000	100000
Administración Telecomunicaciones	50000	205000
Administración Servicio A.D. / DNS	10000	45000
Gestión operaciones /CPD	10000	165000
Servicio Gestión de accesos.	10000	10000
Servicio de Aplicaciones.	25000	25000
Servicio Gestión de puesto de trabajo.	10000	10000
Servicio de BackUp	50000	50000
Servicio de BBDD	50000	50000
Servicio de Telecomunicaciones	10000	10000
O.S. + S.G. - Servidores A.D./DNS	5000	35000
O.S. + S.G. – Servidor Backup	5000	105000
O.S. + S.G. – Clúster B.B.D.D.	5000	80000
O.S. + S.G. – Clúster Aplicaciones	5000	30000
O.S. + S.G. – Firewall Switches	10000	165000
Servidores Directorio Activo / DNS	10000	45000
Servidor BackUP	5000	105000
Servidores Clúster BBDD	10000	85000
Servidores Clúster Aplicaciones	10000	35000
Puestos de trabajo	1000	11000
Switch Central	100000	255000
Firewall	25000	180000
Router	5000	15000
Switches LAN / Macrolan	5000	51000
SAN de Almacenamiento	50000	125000
Sistema de alimentación eléctrica	10000	380000
CPD	100000	460000
Administrador de Sistemas	90000	130000
Administrador de aplicaciones DBA / DBSA	120000	160000
Responsable telecomunicaciones	120000	180000
Responsable de operaciones	90000	136000

Dimensiones

Factor de activos en cada dimensión

Activo	Confidencialidad	Integridad	Autenticidad	Trazabilidad	Disponibilidad
Administración y Operación Servidores	7	4	0	8	2
Administración y Gestión aplicaciones.	7	6	0	8	2
Administración y Operación BBDD	7	8	0	8	2
Administración Telecomunicaciones /	8	3	0	8	2
Administración Servicio A.D.	7	3	0	8	2
Gestión operaciones /CPD	7	7	0	8	2
Servicio Gestión de accesos.	2	7	7	6	9
Servicio de Aplicaciones.	2	5	7	6	9
Servicio Gestión de puesto de trabajo.	2	2	5	4	9
Servicio de BackUp	2	5	4	4	9
Servicio de BBDD	3	8	7	6	9
Servicio de Telecomunicaciones	3	3	4	6	9
O.S. + S.G. - Servidores A.D./DNS	0	8	8	3	9
O.S. + S.G. – Servidor Backup	0	5	8	3	9
O.S. + S.G. – Clúster B.B.D.D.	0	9	9	3	9
O.S. + S.G. – Clúster Aplicaciones	0	7	7	3	9
O.S. + S.G. – Firewall Switches	0	8	8	3	9
Servidores Directorio Activo / DNS	0	2	4	2	9
Servidor BackUP	0	2	3	2	9
Servidores Clúster BBDD	0	2	5	2	9
Servidores Clúster Aplicaciones	0	2	5	2	9
Puestos de trabajo	0	2	2	2	5
Switch Central	0	2	5	2	9
Firewall	0	4	7	2	9
Router	0	1	5	2	5
Switches LAN / Macrolan	0	1	2	2	5
SAN de Almacenamiento	0	8	8	7	9
Sistema de alimentación eléctrica	0	8	8	5	9
CPD	0	8	8	5	9
Administrador de Sistemas	0	5	8	0	2
Administrador de aplicaciones DBA / DBSA	0	5	8	0	2
Responsable telecomunicaciones	0	5	8	0	2
Responsable de operaciones	0	5	8	0	2

Valor de activos en cada dimensión

Activo	Confidencialidad	Integridad	Autenticidad	Trazabilidad	Disponibilidad
Administración y Operación Servidores	11550	6600			660
Administración y Gestión aplicaciones.	2450	2100			140
Administración y Operación BBDD	7000	8000			400
Administración Telecomunicaciones	16400	6150			820
Administración Servicio A.D. / DNS	3150	1350			180
Gestión operaciones /CPD	11550	11550			660
Servicio Gestión de accesos.	20	7000		6000	900
Servicio de Aplicaciones.	50	12500		15000	2250
Servicio Gestión de puesto de trabajo.	20	2000		4000	900
Servicio de BackUp	100	25000		20000	4500
Servicio de BBDD	150	40000		30000	4500
Servicio de Telecomunicaciones	30	3000		6000	900
O.S. + S.G. - Servidores A.D./DNS		28000	2800		31500
O.S. + S.G. – Servidor Backup		52500	8400		94500
O.S. + S.G. – Clúster B.B.D.D.		72000	7200		72000
O.S. + S.G. – Clúster Aplicaciones		21000	2100		27000
O.S. + S.G. – Firewall Switches		132000	13200		148500
Servidores Directorio Activo / DNS		900			20250
Servidor BackUP		2100			47250
Servidores Clúster BBDD		1700			38250
Servidores Clúster Aplicaciones		700			15750
Puestos de trabajo		220			2750
Switch Central		5100	12750		229500
Firewall		7200	12600		162000
Router		150	750		7500
Switches LAN / Macrolan		510	1020		25500
SAN de Almacenamiento		10000			56250
Sistema de alimentación eléctrica		608			3420
CPD		736			4140
Administrador de Sistemas		6500			2600
Administrador de aplicaciones DBA		8000			3200
Responsable telecomunicaciones		9000			3600
Responsable de operaciones		6800			2720

Valoración de amenazas

Agrupamos los valores máximos de las amenazas y obtenemos la tabla resumen con el siguiente resultado:

	Conf.	Int.	Aut.	Traza.	Disp.
[D] datos / información	1	1	1		0,2
[S] servicios	0,1	10		10	1
[SW] aplicaciones (software)	10	10	1		10
[HW] equipos informáticos (hardware)	1	1			5
[COM] redes de comunicaciones	2	1	1		10
[Media] soportes de información	1	1			5
[L] instalaciones	0,02	0,02			0,1
[P] personal interno	1	1			1

Esta es la tabla de valores de factorización que aplicaremos sobre los activos pertenecientes a cada dimensión.

Salvaguardas

Se adjunta hoja de cálculo con el cálculo de las amenazas en base a las amenazas estándar propuestas por Magerit.

Estimación del riesgo

Riesgo residual con salvaguardas actuales

Calculo de riesgos cobre valores acumulados **Calculo con salvaguardas actuales**

Activo	C	I	A	T	D
Administración y Operación Servidores	10972,5		132		
Administración y Gestión aplicaciones.	2327,5		28		
Administración y Operación BBDD	6650		80		
Administración Telecomunicaciones / Firewall / VPN	15580		164		
Administración Servicio A.D. / DNS	2992,5		36		
Gestión operaciones /CPD	10972,5		132		
Servicio Gestión de accesos.					
Servicio de Aplicaciones.					
Servicio Gestión de puesto de trabajo.					
Servicio de BackUp					
Servicio de BBDD					
Servicio de Telecomunicaciones					
O.S. + S.G. - Servidores A.D./DNS		17500	315000		34,375
O.S. + S.G. – Servidor Backup		52500	945000		34,375
O.S. + S.G. – Clúster B.B.D.D.		45000	720000		34,375
O.S. + S.G. – Clúster Aplicaciones		13125	270000		34,375
O.S. + S.G. – Firewall Switches		82500	1485000		34,375
Servidores Directorio Activo / DNS					
Servidor BackUP					
Servidores Clúster BBDD					
Servidores Clúster Aplicaciones					
Puestos de trabajo					
Switch Central		5578,125	2295000		0,4375
Firewall		5512,5	1620000		0,4375
Router		328,125	75000		0,4375
Switches LAN / Macrolan		446,25	255000		0,4375
SAN de Almacenamiento					
Sistema de alimentación eléctrica					
CPD					
Administrador de Sistemas					
Administrador de aplicaciones DBA / DBSA					
Responsable telecomunicaciones					
Responsable de operaciones					

Riesgo residual con salvaguardas potenciales

Calculo de riesgos cobre valores acumulados	**Calculo con salvaguardas propuestas**				
Activo	C	I	A	T	D
Administración y Operación Servidores	8662,5		33		
Administración y Gestión aplicaciones.	1837,5		7		
Administración y Operación BBDD	5250		20		
Administración Telecomunicaciones	12300		41		
Administración Servicio A.D. / DNS	2362,5		9		
Gestión operaciones /CPD	8662,5		33		
Servicio Gestión de accesos.					
Servicio de Aplicaciones.					
Servicio Gestión de puesto de trabajo.					
Servicio de BackUp					
Servicio de BBDD					
Servicio de Telecomunicaciones					
O.S. + S.G. - Servidores A.D./DNS		12250	59850		27,34375
O.S. + S.G. – Servidor Backup		36750	179550		27,34375
O.S. + S.G. – Clúster B.B.D.D.		31500	136800		27,34375
O.S. + S.G. – Clúster Aplicaciones		9187,5	51300		27,34375
O.S. + S.G. – Firewall Switches		57750	282150		27,34375
Servidores Directorio Activo / DNS					
Servidor BackUP					
Servidores Clúster BBDD					
Servidores Clúster Aplicaciones					
Puestos de trabajo					
Switch Central		5578,125	436050		
Firewall		5512,5	307800		
Router		328,125	14250		
Switches LAN / Macrolan		446,25	48450		
SAN de Almacenamiento					
Sistema de alimentación eléctrica					
CPD					
Administrador de Sistemas					
Administrador de aplicaciones DBA / DBSA					
Responsable telecomunicaciones					
Responsable de operaciones					

Resultados finales simplificados.

Por último aplicamos un factor de división de 10000 y nos quedamos únicamente con un decimal para poder simplificar el resultado, tomar datos comparativos y permitir la toma de decisiones. Esté cuadro comparativo nos muestra claramente los mayores riesgos que tenemos y el efecto potencial de aplicar las salvaguardas.

Activos	**Salvaguardas Reales**					**Salvaguardas Potenciales**				
	C	**I**	**A**	**T**	**D**	**C**	**I**	**A**	**T**	**D**
Administración y Operación Servidores	1,1					0,9				
Administración y Gestión aplicaciones.										
Administración y Operación BBDD	0,7					0,5				
Administración Telecomunicaciones	1,6					1,2				
Administración Servicio A.D. / DNS										
Gestión operaciones /CPD	1,1					0,9				
Servicio Gestión de accesos.										
Servicio de Aplicaciones.										
Servicio Gestión de puesto de trabajo.										
Servicio de BackUp										
Servicio de BBDD										
Servicio de Telecomunicaciones										
O.S. + S.G. - Servidores A.D./DNS		1,8	31,5				1,2	6		
O.S. + S.G. – Servidor Backup		5,3	94,5				3,7	18		
O.S. + S.G. – Clúster B.B.D.D.		4,5	72				3,2	13,7		
O.S. + S.G. – Clúster Aplicaciones		1,3	27				0,9	5,1		
O.S. + S.G. – Firewall Switches		8,3	148,5				5,8	28,2		
Servidores Directorio Activo / DNS										
Servidor BackUP										
Servidores Clúster BBDD										
Servidores Clúster Aplicaciones										
Puestos de trabajo										
Switch Central		0,6	229,5				0,6	43,6		
Firewall		0,6	162				0,6	30,8		
Router			7,5				0	1,4		
Switches LAN / Macrolan			25,5				0	4,8		
SAN de Almacenamiento										
Sistema de alimentación eléctrica										
CPD										
Administrador de Sistemas										
Administrador de aplicaciones DBA / DBSA										

Responsable telecomunicaciones Responsable de operaciones

Plan de acción de mejora

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.

La ejecución de ambos planes de mejora tendrá una duración estimada de 1 año, su coste económico está valorado en un total de 55000€ y el impacto en la seguridad supone una disminución del riesgo de hasta un 400% para algunos activos y entorno al 50% para el resto.

O.S. + S.G. - Servidores A.D./DNS	1,8	31,5	1,2	6
O.S. + S.G. – Servidor Backup	5,3	94,5	3,7	18
O.S. + S.G. – Clúster B.B.D.D.	4,5	72	3,2	13,7
O.S. + S.G. – Clúster Aplicaciones	1,3	27	0,9	5,1
O.S. + S.G. – Firewall Switches	8,3	148,5	5,8	28,2

Switch Central	0,6	229,5		0,6	43,6
Firewall	0,6	162		0,6	30,8
Router		7,5		0	1,4
Switches LAN / Macrolan		25,5		0	4,8

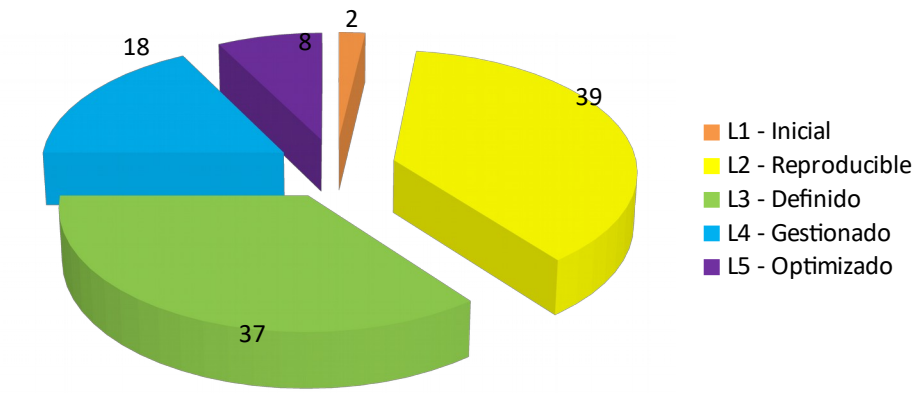
Auditoria de cumplimiento

A continuación mostramos un breve resumen de los resultados obtenidos:

En primer lugar mostramos un resumen de los porcentajes de aplicación organizados por dominios:

5	**POLÍTICA DE SEGURIDAD**	**95**
6	**ASPECTOS ORGANIZATIVOS PARA LA SEGURIDAD**	**83**
7	**CLASIFICACIÓN Y CONTROL DE ACTIVOS**	**72**
8	**SEGURIDAD EN RECURSOS HUMANOS**	**81**
9	**SEGURIDAD FÍSICA Y DEL ENTORNO**	**91**
10	**GESTIÓN DE COMUNICACIONES Y OPERACIONES**	**70**
11	**CONTROL DE ACCESOS**	**70**
12	**ADQUISICION, DESARROLLO Y MANTENIMIENTO DE SISTEMAS**	**67**
13	**GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE INFORMACIÓN**	**83**
15	**CUMPLIMIENTO**	**91**

Resumen de controles sobre un total de 104 controles auditados que están dentro del alcance:


2
8
18
39
37
L1 - Inicial
L2 - Reproducible
L3 - Definido
L4 - Gestionado
L5 - Optimizado