MÁSTER INTERUNIVERSITARIO EN SEGURIDAD DE LAS TECNOLOGÍAS DE LA INFORMACIÓN Y LA COMUNICACIÓN (MISTIC)

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

Autor: Enrique Perona Játiva

Director: Antonio José Segovia Henares

Junio, 2015

RESUMEN

Este proyecto plantea la manera de llevar a cabo la implantación de la norma ISO/IEC 27001:2005 en una organización. Esto va a permitir a la misma alinear sus objetivos de negocio y sus directrices de seguridad de acuerdo a los requisitos impuestos por la normativa internacional de referencia.

Se plantean las bases para la implementación de un Sistema de Gestión de Seguridad de la Información (SGSI) en la organización objeto de estudio, desarrollando las fases de contextualización y estudio de la situación actual, desarrollo del esquema documental, análisis de riesgos, propuesta de proyectos y evaluación del nivel de cumplimiento de la norma.

ABSTRACT

The following dissertation shows how you may introduce the law ISO/IEC 27001:2005 into an organization. This might lead in the same way to establish the aims of the business and the guidelines for a security agreement; according to the international regulation.

The bases to implement the Information Security Management System (ISMS) are set out within the subject of study; throughout developing the contextualization and the analysis of the current situation. It also includes the development of the documentary outline, risk analysis and a new project proposal. In order to finish with an evaluation of the rate of rules followed at this level.

Agradecimientos

A todos los profesores que un día despertaron en mi las ganas de saber y profundizar en el mundo de la Seguridad de la Información.

A mi tutor, Antonio, cuya atención y dedicación ha sido crucial para que este trabajo sea un poquito mejor.

A mi familia, que a pesar del esfuerzo que han tenido que realizar para proporcionarme estos estudios no lo dudaron ni un momento.

A mis amigos, que siempre han estado ahí en los momentos en que era necesario desconectar y apartar la cabeza del trabajo.

Dedicatorias

A mi familia, por proporcionarme una inmejorable educación y un buen futuro. Gracias.

ÍNDICE

CAPÍTULO 1. INTRODUCCIÓN 9
1.1 FAMILIA ISO/IEC 27000 10
1.2 OBJETIVOS DEL PROYECTO 11
1.3 METODOLOGÍA Y ESTRUCTURA DE LA MEMORIA 12
CAPÍTULO 2. SITUACIÓN ACTUAL: CONTEXTUALIZACIÓN, OBJETIVOS Y ANÁLISIS DIFERENCIAL 14
2.1 CONTEXTUALIZACIÓN 14
2.1.1 ORGANIZACIÓN SELECCIONADA 14
2.1.2 ALCANCE 15
2.2 OBJETIVOS DEL PLAN DIRECTOR 16
2.3 OBJETIVOS DEL SGSI 17
2.4 ANÁLISIS DIFERENCIAL 17
2.4.1 TABLA ANÁLISIS DIFERENCIAL ISO/IEC 27001:2005 19
2.4.2 TABLA ANÁLISIS DIFERENCIAL ISO/IEC 27002:2005 20
CAPÍTULO 3. SISTEMA DE GESTIÓN DOCUMENTAL 39
3.1 POLÍTICA DE SEGURIDAD 39
3.1.1 INTRODUCCIÓN 39
3.1.2 OBJETIVOS 39
3.1.3 ALCANCE 40
3.1.4 SEGURIDAD FÍSICA 40
3.1.5 PERÍMETRO (COMUNICACIONES Y ACCESO A LA RED INTERNA) 41
3.1.6 HARDWARE (ESTACIONES DE TRABAJO Y SERVIDORES) 43
3.1.7 APLICACIONES Y SOFTWARE 44
3.1.8 CLASIFICACIÓN, ALMACENAMIENTO Y ADMINISTRACIÓN DE LA INFORMACIÓN 48
3.1.9 RESPONSABILIDADES DEL PERSONAL 51
3.1.10 REGISTRO DE AUDITORÍA 52
3.2 PROCEDIMIENTO DE AUDITORÍAS INTERNAS 53
3.2.1 OBJETIVO 53
3.2.2 ALCANCE 53
3.2.3 PLANIFICACIÓN DE AUDITORÍAS 53
3.2.4 REQUISITOS A CUMPLIR POR LOS AUDITORES INTERNOS 54

3.2.5 MODELO DE INFORME DE AUDITORÍA 55
3.3 GESTIÓN DE INDICADORES 58
3.4 PROCEDIMIENTO DE REVISIÓN POR LA DIRECCIÓN 60
3.4.1 INTRODUCCIÓN 60
3.4.2 OBJETIVO 60
3.4.3 ALCANCE 60
3.4.4 ENTRADAS 61
3.4.5 SALIDAS 61
3.4.6 PROCEDIMIENTO 61
3.5 GESTIÓN DE ROLES Y RESPONSABILIDADES 62
3.5.1 COMITÉ DE SEGURIDAD 62
3.5.2 FUNCIONES Y OBLIGACIONES DEL PERSONAL 63
3.6 METODOLOGÍA DE ANÁLISIS DE RIESGOS 66
3.7 DECLARACIÓN DE APLICABILIDAD 69
CAPÍTULO 4. ANÁLISIS DE RIESGOS 89
4.1 IDENTIFICACIÓN, CLASIFICACIÓN Y VALORACIÓN DE LOS ACTIVOS. 89
4.2 IDENTIFICACIÓN DE LAS AMENAZAS 91
4.3 CÁLCULO DEL RIESGO POTENCIAL 96
4.4 APLICACIÓN DE CONTROLES 111
4.5 CÁLCULO DEL RIESGO RESIDUAL 128
CAPÍTULO 5. PROPUESTA DE PROYECTOS 144
5.1 PROYECTO 1: REDEFINICIÓN DE LA POLÍTICA DE SEGURIDAD Y ASPECTOS ORGANIZATIVOS 144
5.2 PROYECTO 2: PROGRAMA DE FORMACIÓN Y SENSIBILIZACIÓN EN SEGURIDAD DE LA INFORMACIÓN 146
5.3 PROYECTO 3: DEFINICIÓN DE POLÍTICA DE CONTROLES CRIPTOGRÁFICOS Y PROCEDIMIENTOS DE CONTROL DE CAMBIOS 148
5.4 PROYECTO 4: MEJORA EN LA GESTIÓN DE INCIDENTES DE SEGURIDAD 150
5.5 PROYECTO 5: ESTABLECIMIENTO DE UN PLAN DE CONTINUIDAD DEL NEGOCIO 151
5.6 RESUMEN DE RESULTADOS 153
CAPÍTULO 6. AUDITORÍA DE CUMPLIMIENTO DE LA ISO/IEC 27002:2005 156

6.1 EVALUACIÓN DE CUMPLIMIENTO 156

6.2 NO CONFORMIDADES, OBSERVACIONES Y OPORTUNIDADES DE MEJORA 161

6.3 RESUMEN DE RESULTADOS 162

CAPÍTULO 7. CONCLUSIONES 165

BIBLIOGRAFÍA 166

ÍNDICE DE FIGURAS

Figura 2-1: Gráfico radial de representación del análisis diferencial respecto a la ISO/IEC 27001:2005 20
Figura 2-2: Gráfico radial de representación del análisis diferencial respecto a la ISO/IEC 27002:2005 38
Figura 4-1: Esquema de análisis de riesgos MAGERIT 89
Figura 5-1: Nivel de cumplimiento antes y después de la realización de los proyectos 154
Figura 6-1: Representación gráfica del nivel de madurez de los controles implantados en la organización 163
Figura 6-2: Representación gráfica del nivel de cumplimiento de los dominios de la norma ISO/IEC 27002:2005 164

ÍNDICE DE TABLAS

Tabla 2-1: Niveles de madurez de la escala CMM 19
Tabla 2-2: Tabla de análisis diferencial respecto a la norma ISO/IEC 27001:2005 20
Tabla 2-3: Tabla de análisis diferencial respecto a la norma ISO/IEC 27002:2005 37
Tabla 3-1: Tabla de indicadores para medición de la eficacia de los controles implantados..... 59
Tabla 3-2: Tabla de indicadores para medición de los objetivos del SGSI 60
Tabla 3-3: Tabla de valoración de activos 67
Tabla 3-4: Escala de probabilidad de ocurrencia de las amenazas 67
Tabla 3-5: Escala de cuantificación del impacto..... 68
Tabla 3-6: Declaración de aplicabilidad 88
Tabla 4-1: Inventario de activos de la organización 91
Tabla 4-2: Catálogo de amenazas 93
Tabla 4-3: Relación entre activos y amenazas 96
Tabla 4-4: Valores de riesgo potencial para los activos de la organización 111
Tabla 4-5: Aplicación de controles 128
Tabla 4-6: Valores de riesgo residual para los activos de la organización 143
Tabla 5-1: Relación entre implantación de proyectos y reducción del impacto . 154
Tabla 5-2: Distribución temporal de los proyectos 155
Tabla 6-1: Nivel de implantación de los controles de la norma ISO/IEC 27002:2005 161
Tabla 6-2: No conformidades (NC), observaciones (OBS) y oportunidades de mejora (OM) identificadas en la organización 162
Tabla 6-3: Número de controles por nivel de madurez..... 163
Tabla 6-4: Nivel de cumplimiento de los dominios de la norma ISO/IEC 27002:2005 163

CAPÍTULO 1.INTRODUCCIÓN

En esta era de Sociedad de la Información en la que nos encontramos, lo más valioso que cualquier empresa u organización posee es eso, información. Ésta será el activo más importante que tenga en su haber, y por consecuente, todo lo que la rodea. Decimos esto porque la información no es algo físico o tangible que podamos gestionar "por sí solo", sino que necesitará de otros activos para poder manejarla: equipos informáticos, soportes de almacenamiento, sistemas de comunicación, etc. Estos activos de los que va a depender la información, se van a convertir en igual o más importantes para la organización.

Pero estos activos se pueden ver, en cuanto a seguridad se refiere, comprometidos diariamente por una serie de factores internos o externos a la organización y estará en peligro la integridad, confidencialidad y disponibilidad de los mismos. Podemos decir que los activos de una organización poseen un riesgo constante, y si tan importantes son para nosotros estos activos, no podemos ignorarlo. Por ello, hoy en día, las organizaciones tienen que valorar otro nuevo tipo de riesgo: los riesgos tecnológicos o riesgos relacionados con las Tecnologías de la Información (TI).

Los riesgos de TI siempre existen, sean o no detectados o reconocidos por la organización. Estos riesgos son un componente del universo de riesgos a los que está sometida una organización. En este compendio de riesgos encontramos riesgos estratégicos, riesgos ambientales, riesgos de mercado, riesgos de crédito, riesgos operativos, etc. Decimos que los riesgos de TI son un componente de los demás riesgos porque suelen tener una estrecha relación con la mayoría de ellos. Por ejemplo, si consideramos el riesgo de crédito en una organización del sector financiero, una política pobre en cuanto a seguridad de la información se refiere, puede conducir a menores calificaciones de crédito [1].

Dado este nuevo contexto en el que nos encontramos en la actualidad, la mayoría de organizaciones, grandes o pequeñas, pertenecientes al sector público o al sector privado, están tomando conciencia de la importancia de asegurar sus activos de información. Para este objetivo se concibieron la familia de normas ISO/IEC 27000, un conjunto de normas y estándares que proporcionan un marco de gestión de la seguridad de la información aplicable a cualquier compañía.

Dentro de esta familia de normas, adquieren especial relevancia en el presente trabajo las normas ISO/IEC 27001 [2] e ISO/IEC 27002 [3]. La norma ISO/IEC 27001 agrupa los requerimientos de implantación de un Sistema de Gestión de la Seguridad de la Información (SGSI), mientras que la norma ISO/IEC 27002 comprende una guía de buenas prácticas para la gestión de la seguridad de la información, la cual describe los objetivos de control y controles recomendables.

La certificación en estas normas darán a clientes y proveedores de la organización una confianza añadida, ya que será la prueba de que se lleva a cabo una correcta gestión de la seguridad de la información. Además, proporcionará a la organización un sello diferenciador frente a la competencia, algo que posiblemente le reportará mayores beneficios, demostrando que realizar mejoras en seguridad de la información debe verse como una inversión, y no como un coste.

1.1 FAMILIA ISO/IEC 27000

En una clara demostración de la importancia que la seguridad de la información tiene para el éxito de las organizaciones, la ISO (International Organization for Standardization) y la IEC (International Electrotechnical Comision) han elaborado conjuntamente todo tipo de normas, estándares, guías e informes técnicos relacionados con las TIC y, más particularmente, con las técnicas de seguridad [4].

ISO/IEC ha reservado la familia de normas ISO 27000 para tratar distintos aspectos de esta temática, del mismo modo que se ha realizado con la calidad y la familia ISO 9000, o la gestión medioambiental con la ISO 14000. El trabajo sobre la familia ISO 27000 es coordinado por un subcomité (el subcomité 27, dentro del JTC1: Joint Technical Committee 1) que se organiza en base a grupos de trabajo dedicados a distintas temáticas: sistemas de gestión de la seguridad de la información, criptografía y mecanismos de seguridad, criterios de evaluación de la seguridad, servicios y controles de seguridad, gestión de identidades y tecnologías relacionadas con la privacidad, etc [4].

Las normas que componen la familia ISO/IEC 27000, son las que se describen a continuación [4]:

- **ISO/IEC 27000.** Proporciona una introducción y visión de conjunto de todo el marco ISO 27000 y facilita un glosario común.
- **ISO/IEC 27001:2005.** Es la norma que recoge los requerimientos para la implantación de un sistema de gestión de la seguridad de la información (ha sido trasladada al marco español en el 2007). La implantación de un SGSI según esta norma puede certificarse.
- **ISO/IEC 27002:2005.** Se trata del código de buenas prácticas para la gestión de la seguridad de la información, y recoge un completo y amplio catálogo de controles y buenas prácticas en la materia. Es el conjunto de controles que la norma ISO/IEC 27001 toma como referencia a la hora de seleccionar controles de seguridad.
- **ISO/IEC 27003:2010.** Facilita una guía para implementar un SGSI según la norma ISO/IEC 27001.
- **ISO/IEC 27004:2009.** Facilita una guía y sugiere mecanismos para medir la eficiencia de un SGSI.

- **ISO/IEC 27005:2008.** Facilita una guía para la gestión de los riesgos de seguridad de la información, y proporciona un marco para realizar un análisis de riesgos. Está inspirada en el ISO/IEC Technical Report 13335-3.
- **ISO/IEC 27006:2007.** Es la norma que recoge los requisitos de las entidades de certificación acreditadas para certificar SGSI según la norma ISO/IEC 27001.
- **ISO/IEC 27007:2011.** Proporciona una guía para la auditoría de SGSI (ampliamente basada en la ISO 19011).
- **ISO/IEC 27008:2011.** Proporciona una guía para la auditoría de los controles de seguridad.

La norma ISO/IEC 27001:2005 fue aprobada en octubre del 2005, pero no es la primera en su especialidad. La organización británica de estandarización BSI (British Standard Institute) creó la norma BS-7799 ya en 1995, que contenía una primera versión del catálogo de buenas prácticas para la seguridad de la información. Esta misma organización creó posteriormente, en 1999, la norma BS-7799-2, con los requerimientos para un sistema de gestión de la seguridad de la información que escogiera sus controles de la BS-7799. Ambas normas fueron la base para la creación de las normas ISO/IEC 27002:2005 e ISO/IEC 27001:2005, respectivamente. La norma ISO/IEC 27002:2005 fue inicialmente la ISO/IEC 17799:2000, que fue revisada en el 2005 y dio lugar a la ISO/IEC 17799:2005. En el 2007, esta norma sufrió un cambio de denominación, dando lugar al nombre actual: ISO/IEC 27002:2005. Sin embargo, al tratarse únicamente de un cambio de denominación, no se ha modificado el año de aprobación (2005) [4].

1.2 OBJETIVOS DEL PROYECTO

El objetivo del presente trabajo consiste en elaborar un Plan de Implementación de la ISO/IEC 27001:2005 para una organización, que le permita alinear sus objetivos y principios de seguridad a la normativa internacional de referencia. Mediante dicho plan, se sentarán las bases del proceso de mejora continua en materia de seguridad de la información, permitiendo a la organización conocer el estado de la misma y plantear las acciones necesarias para minimizar el impacto de los riesgos potenciales. De este modo, se establecerán las bases para la implementación de un SGSI adecuado a la normativa en la organización.

De una forma más específica, y a nivel de realización del trabajo, los objetivos o hitos del proyecto son los siguientes:

- Llevar a cabo una documentación normativa sobre las mejores prácticas en seguridad de la información.

- Definir de forma clara la situación actual y los objetivos del SGSI.
- Realizar un Análisis de Riesgos en la organización:
    - Identificar y valorar los activos corporativos como punto de partida del análisis.
    - Identificar amenazas, evaluarlas y clasificarlas.
- Realizar una evaluación del nivel de cumplimiento de la ISO/IEC 27002:2005 en la organización.
- Proponer proyectos de cara a conseguir una adecuada gestión de la seguridad en la organización.
- Establecer un Esquema Documental.

Como entregables del proyecto, se presentarán básicamente los productos que se especifican a continuación:

- Informe del Análisis Diferencial.
- Esquema Documental ISO/IEC 27001.
- Análisis de Riesgos.
- Plan de Proyectos.
- Auditoría de Cumplimiento.
- Presentación de resultados.

1.3 METODOLOGÍA Y ESTRUCTURA DE LA MEMORIA

A nivel metodológico, se abordará el proyecto mediante una aproximación por fases. A continuación se comenta brevemente las acciones llevadas a cabo en cada una de las fases, para proporcionar al lector una visión global sobre el proyecto:

Fase 1: Situación actual: Contextualización, objetivos y análisis diferencial. En esta primera fase, se seleccionará y describirá la empresa que será objeto de estudio, se definirá el alcance y los objetivos del Plan Director de Seguridad y se llevará a cabo el Análisis Diferencial respecto a las normas ISO/IEC 27001:2005 [2] e ISO/IEC 27002:2005 [3].

Fase 2: Sistema de Gestión Documental. En esta fase, se desarrollará toda la documentación pertinente, necesaria para dotar al SGSI de un cuerpo documental para el cumplimiento normativo. Los documentos a desarrollar vienen establecidos en la propia norma ISO/IEC 27001:2005, y son los siguientes: Política de Seguridad, Procedimiento de Auditorías Internas, Gestión de Indicadores, Procedimiento de Revisión por la Dirección, Gestión de Roles y Responsabilidades, Metodología de Análisis de Riesgos y Declaración de Aplicabilidad.

Fase 3: Análisis de Riesgos. El objetivo de esta fase radica en la realización del análisis de riesgos de la organización, el cual será la piedra angular del proyecto y en el que se basarán la mayoría de decisiones tomadas. Para llevar a cabo este análisis, en primer lugar se deben inventariar todos los activos de la organización que tienen relevancia en cuanto a seguridad de la información se refiere. A continuación, es necesario identificar las amenazas que pueden afectar a estos activos, para después poder calcular los valores de riesgo potencial y riesgo residual de dichos activos.

Fase 4: Propuesta de Proyectos. En esta fase se plantearán los proyectos que ayudarán a mejorar el estado de la seguridad de la organización. La descripción de dichos proyectos debe ayudar a mitigar el riesgo actual y contribuir a evolucionar el cumplimiento de la norma ISO/IEC 27002 hasta un nivel adecuado, tal y como se puede observar en los resultados aportados al final del capítulo.

Fase 5: Auditoría de Cumplimiento de la ISO/IEC 27002:2005. En esta fase se evaluará el nivel de cumplimiento de la organización con respecto a los controles de la norma ISO/IEC 27002:2005, una vez llevada a cabo la gestión de riesgos. Además, se identificarán posibles no conformidades, observaciones y oportunidades de mejora en la organización.

Fase 6: Presentación de resultados y entrega de informes. En esta última fase, tras la consecución de todas las fases anteriores, se recopilará toda la información y se analizarán los resultados obtenidos, para posteriormente, elaborar toda la documentación necesaria que se entregará a la Dirección de la organización. Esta documentación estará compuesta de un Resumen Ejecutivo, una Memoria descriptiva del proceso llevado a cabo (el presente documento) y una presentación a la Dirección.

CAPÍTULO 2.SITUACIÓN ACTUAL: CONTEXTUALIZACIÓN, OBJETIVOS Y ANÁLISIS DIFERENCIAL

2.1 CONTEXTUALIZACIÓN

Este apartado tiene dos objetivos. En primer lugar, se hará una descripción de la organización seleccionada para llevar a cabo el proyecto, comentando algunos aspectos relevantes tales como su entorno de actividad, tamaño, estado inicial de la seguridad, etc.

En segundo lugar, se concretará el alcance del proyecto, para acotar los aspectos que serán tratados y definir las consideraciones pertinentes.

2.1.1 ORGANIZACIÓN SELECCIONADA

Para el desarrollo de las diferentes fases del proyecto se utilizará la organización ficticia descrita a continuación:

La organización en cuestión es una pequeña entidad bancaria, que desea implementar su Sistema de Gestión de Seguridad de la Información (SGSI) de acuerdo a la norma ISO/IEC 27001 [2]. Dicha entidad se trata de una entidad a nivel provincial y consta de una sede central, localizada en la capital, y cinco sucursales repartidas entre las cinco localidades más pobladas de la provincia.

En cuanto a recursos humanos la organización cuenta con un director general, los directores de sucursal y los empleados de las distintas sucursales. Además, la entidad cuenta con un Departamento de Tecnologías de la Información (TI), compuesto por un jefe de departamento, tres responsables de seguridad y seis técnicos/desarrolladores. Cada responsable de seguridad tiene asignada una zona, debido a la segregación de la organización en diferentes ubicaciones. El responsable de seguridad 1 tiene asignada la zona 1, que comprende la sede central y la sucursal 1. El responsable de seguridad 2 tiene asignada la zona 2, que comprende las sucursales 2 y 3. El responsable de seguridad 3 tiene asignada la zona 3, que comprende las sucursales 4 y 5. El servicio de seguridad y videovigilancia está externalizado.

La infraestructura tecnológica de la entidad consta mayormente de un servidor central ubicado en la sede principal y utilizado por los diversos empleados de las

sucursales para realizar todas las operaciones propias de la actividad bancaria, un servidor destinado a las actividades del servicio de banca online que la entidad ofrece a sus clientes, los distintos terminales utilizados por los empleados y directores, y por supuesto, toda la infraestructura de red empleada para las comunicaciones entre terminales y servidores de la entidad. El CPD propiamente dicho se encontrará en la sede principal de la organización.

Debido, entre otras cosas, a que la entidad bancaria es de relativamente reciente creación, tiene un tamaño y alcance pequeños (nivel provincial), y su presupuesto no es muy elevado, podríamos decir que el nivel de madurez en cuanto a seguridad de la información en la organización estará situado entre "Inicial" y "Repetible", respecto a la escala CMM [5]. Se tienen documentados e implementados algunos procedimientos (plan de seguridad, plan de contingencia, etc.), pero éstos tienen aún mucho margen de mejora. Por ello, y dado que la organización es consciente del grado de criticidad del servicio que ofrecen, desean realizar un proceso de mejora dentro de su SGSI.

2.1.2 ALCANCE

Para empezar, es importante destacar que este trabajo tiene fines puramente académicos, con las limitaciones y requisitos que ello puede conllevar. Además, como se ha dicho anteriormente, la organización tomada como ejemplo es ficticia y cualquier semejanza que pueda darse con una entidad bancaria real será fruto de la casualidad o de las similitudes propias que existen entre organizaciones de este tipo.

Este proyecto tiene como fin analizar el grado de madurez del SGSI implantado en la organización, y proponer mejoras para su adecuación a la norma ISO/IEC 27001:2005 [2]. Para ello será necesario inventariar los activos de la organización, pero no todos, sino aquellos que tengan una cierta relevancia dentro de los procesos de negocio de la misma. Estos procesos de negocio se refieren básicamente a las actividades de banca tradicional gestionadas por los empleados de la organización y al servicio de banca online. Dichos procesos serán los que centrarán la atención de los objetivos de este proyecto.

De una forma más específica, la finalidad de este plan de implantación es adecuar a la norma de referencia todos los procesos organizativos y técnicos que intervienen de una u otra forma en el tratamiento de la información. Por una parte, serán objeto de estudio los procedimientos llevados a cabo por el personal interno (o externo si se da el caso) de la organización, corroborando que cumplen con la política de seguridad definida y que ésta es conocida por todos ellos. Se revisarán los procedimientos de intercambio de información entre el personal de las distintas localizaciones. Además, se evaluará el compromiso de la Dirección con la seguridad de la información. En definitiva, el alcance de este proyecto abarca todos los sistemas de información que dan soporte a los procesos, servicios y actividades de negocio mencionados y que son

llevados a cabo y ofrecidos por la organización, de acuerdo a la declaración de aplicabilidad vigente.

Por otra parte, se auditarán todos los activos informáticos de la organización, ya que todos intervienen de una manera u otra en los procesos de negocio mencionados: servidores, terminales de usuarios, comunicaciones, software utilizado, bases de datos, métodos de autenticación del personal en el sistema, métodos de autenticación y técnicas criptográficas utilizadas en el servicio de banca online ofrecido, etc.

Por último, y dado que la organización utilizada para el ejemplo es ficticia, en los documentos que componen este proyecto solamente se proporcionarán los datos de la organización estrictamente necesarios para el cumplimiento de los objetivos de este trabajo.

2.2 OBJETIVOS DEL PLAN DIRECTOR

El Plan Director de Seguridad tiene como objetivo general definir y priorizar un conjunto de proyectos en materia de seguridad de la información dirigidos a reducir los riesgos a los que está expuesta la organización hasta unos niveles aceptables, a partir de un análisis de la situación inicial [6]. En la organización que nos ocupa, los objetivos del Plan Director son, de una manera más específica, los siguientes:

- Analizar el estado actual de seguridad de la organización con respecto a la normativa de referencia (ISO/IEC 27001:2005 [2] e ISO/IEC 27002:2005 [3]).
- Definir y planificar los proyectos a realizar a corto, medio y largo plazo, teniendo en cuenta la diferencia existente entre el nivel de seguridad actual y el nivel de seguridad objetivo.
- Ofrecer unos niveles de seguridad a los sistemas de información de la organización que sean coherentes con el grado de criticidad de los servicios que ofrecen.
- Identificar los riesgos que poseen los activos de la organización e implementar salvaguardas que reduzcan dichos riesgos hasta niveles aceptables.
- Establecer las medidas de seguridad oportunas para cumplir con los requerimientos legales que atañen a los servicios ofrecidos por la organización.
- Establecer y formalizar procedimientos de gestión de la seguridad.
- Crear y fomentar una cultura de la seguridad de la información a todos los niveles de la organización.

2.3 OBJETIVOS DEL SGSI

Por otra parte, los objetivos que pretende alcanzar la organización con la implantación de un Sistema de Gestión de Seguridad de la Información son los siguientes:

- Identificar amenazas, vulnerabilidades e impactos en las actividades de negocio de la organización.
- Llevar a cabo una mejora continua en la gestión de la seguridad de la información.
- Reducir costes vinculados a la materialización de incidentes de seguridad.
- Incrementar el nivel de confianza de los clientes de la organización.
- Aumentar el valor comercial y mejorar la imagen de la organización.
- Cumplir con la legislación vigente en materia de protección de datos de carácter personal, servicios de la sociedad de la información, comercio electrónico, y en general, con toda aquella relacionada con la seguridad de la información.

2.4 ANÁLISIS DIFERENCIAL

A pesar de haberse definido el alcance, se considera necesario definir un alcance más acertado con la realidad o estado actual de la organización, por tanto, se hace necesario verificar el estado actual de la seguridad, y una de las mejores formas de hacerlo es mediante la realización de un análisis diferencial, también denominado análisis de brechas o *GAP Analysis* [7].

El análisis diferencial se realizará con respecto a las normas ISO/IEC 27001:2005 [2] e ISO/IEC 27002:2005 [3]. El análisis diferencial permite conocer de primera mano, el estado general de la empresa en torno a la seguridad de la información, permitiendo una definición más precisa del alcance [7].

En la organización que nos ocupa, podríamos decir que el nivel de implantación de la norma ISO/IEC 27001:2005 [2] en su SGSI es inmaduro o nulo con respecto al modelo PDCA (*Plan-Do-Check-Act*) [8]. Muchos apartados de la norma no se encontrarán implantados en el SGSI de la organización, por ello, está lejos de cumplir con la misma. Esto se debe a que existe alguna documentación y algunos procedimientos definidos, pero éstos son muy pobres, poco coherentes y no son conocidos por la mayoría de miembros de la organización. Además, la organización no cuenta con ningún otro Sistema de Gestión implantado (calidad, medioambiental, etc.), lo cual contribuye a ese bajo nivel de implantación. También influye en este bajo nivel de madurez, la reciente creación de la organización. A continuación, se cita el estado actual de la organización con respecto a algunos aspectos clave de la norma:

- Existe documentación que define el alcance, los límites y los objetivos del SGSI pero ésta no está aprobada por la Dirección. La documentación es gestionada en su totalidad por el Departamento de TI.
- La organización no tiene adoptada una metodología de evaluación de riegos adecuada para el SGSI. Se identifican algunos de los riesgos más comunes, pero no se analizan y valoran correctamente y, por tanto, no se aplican los controles adecuados.
- El plan de tratamiento de riesgos no identifica las acciones de la Dirección, y no existe una asignación adecuada de prioridades y responsabilidades para gestionar los riesgos de seguridad de la información.
- Se ejecutan procedimientos de supervisión y revisión del SGSI, pero éstos no se realizan con una periodicidad establecida ni son controlados por la Dirección. Se realizan algunas auditorías internas muy pobres del SGSI, pero sin ninguna planificación consensuada.
- Las tareas de mantenimiento y mejora llevadas a cabo en el SGSI son muy básicas y no siguen un procedimiento planificado y metódico, aplicando mejoras identificadas en etapas anteriores o comunicando los cambios a las partes interesadas.
- No hay un procedimiento documentado para llevar a cabo el control documental de los documentos del SGSI. Éste es gestionado por el Departamento de TI, y presenta deficiencias en el control de cambios y en la identificación de los mismos.
- La Dirección, hasta ahora, no era consciente de la importancia de que la organización implementara un SGSI acorde a los estándares internacionales, por ello, el compromiso por su parte era casi nulo, no se proveían los recursos necesarios para establecer, implementar, operar, supervisar, revisar, mantener y mejorar el SGSI, y no existía concienciación, formación y capacitación entre el personal con responsabilidades definidas en el mismo, a excepción del personal del Departamento de TI.

Por otro lado, se realiza el análisis diferencial con respecto a la norma ISO/IEC 27002:2005 [3]. Este análisis va a permitir obtener el estado actual de la organización frente a los controles de seguridad especificados en la norma. Para ello, se va a plantear una tabla donde aparecerán los dominios, objetivos de control y controles de la norma junto con el estado actual de implantación de los mismos en la organización. Para determinar el nivel de madurez de cada uno de los controles se utilizará la escala CMM (Tabla 2-1) especificada a continuación [5]:

Valor	Nombre	Descripción	Efectividad
0	Inexistente	No hay evidencia de esta norma o práctica en la organización.	0%
1	Inicial	La organización tiene prácticas hechas a medida pero inconsistentes.	10%
2	Repetible	La organización cuenta con un enfoque global y coherente, pero no documentado.	50%

3	Definido	La organización tiene un enfoque detallado y documentado, pero no medido.	90%
4	Gestionado	La organización mide periódicamente su cumplimiento y hace mejoras regulares del proceso.	95%
5	Optimizado	La organización ha refinado su conformidad al nivel de las mejores prácticas.	100%

Tabla 2-1: Niveles de madurez de la escala CMM

Una vez realizado este análisis diferencial, se mostrarán los resultados arrojados para el mismo por la herramienta *Data Security Maturity Model*, desarrollada en Excel, y que permite obtener de forma numérica el nivel de madurez de la organización respecto de la norma, en base al nivel de cada uno de los controles especificados en ella.

2.4.1 TABLA ANÁLISIS DIFERENCIAL ISO/IEC 27001:2005

En la Tabla 2-2 se recoge el análisis diferencial respecto a la norma ISO/IEC 27001:2005 [2] de una forma más específica, pudiendo observar el nivel de cumplimiento en la organización de cada uno de los apartados de la norma.

Para la evaluación de dichos apartados, se utilizará la escala CMM reflejada en la Tabla 2-1, y al final de dicha evaluación, se mostrarán los resultados mediante un gráfico radial.

4	**SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN**	**2 - Repetible**
4.1	**REQUISITOS GENERALES**	**2 - Repetible**
4.2	**CREACIÓN Y GESTIÓN DEL SGSI**	**2 - Repetible**
4.2.1	Creación del SGSI	2 - Repetible
4.2.2	Implementación y operación del SGSI	2 - Repetible
4.2.3	Supervisión y revisión del SGSI	2 - Repetible
4.2.4	Mantenimiento y mejora del SGSI	2 - Repetible
4.3	**REQUISITOS DE LA DOCUMENTACIÓN**	**2 - Repetible**
4.3.1	Generalidades	2 - Repetible
4.3.2	Control de documentos	2 - Repetible
4.3.3	Control de registros	2 - Repetible
5	**RESPONSABILIDAD DE LA DIRECCIÓN**	**1 - Inicial**
5.1	**COMPROMISO DE LA DIRECCIÓN**	**1 - Inicial**
5.2	**GESTIÓN DE LOS RECURSOS**	**1 - Inicial**
5.2.1	Provisión de los recursos	2 - Repetible
5.2.2	Concienciación, formación y capacitación	1 - Inicial
6	**AUDITORÍAS INTERNAS DEL SGSI**	**2 - Repetible**
7	**REVISIÓN DEL SGSI POR LA DIRECCIÓN**	**1 - Inicial**
7.1	**GENERALIDADES**	**1 - Inicial**
7.2	**DATOS INICIALES DE LA REVISIÓN**	**1 - Inicial**
7.3	**RESULTADOS DE LA REVISIÓN**	**1 - Inicial**
8	**MEJORA DEL SGSI**	**2 - Repetible**
8.1	**MEJORA CONTINUA**	**2 - Repetible**
8.2	**ACCIÓN CORRECTIVA**	**2 - Repetible**

8.3	**ACCIÓN PREVENTIVA**	**2 - Repetible**

Tabla 2-2: Tabla de análisis diferencial respecto a la norma ISO/IEC 27001:2005

Resumen de resultados

La Figura 2-1 muestra un gráfico radial que representa el estado actual de la organización respecto a los apartados de la norma, el estado objetivo que se pretende alcanzar a corto-medio plazo y el estado óptimo. Como podemos observar, el SGSI de la organización presenta un estado muy inmaduro con respecto a la normativa de referencia. Uno de los aspectos más preocupantes que se aprecian es el bajo compromiso de la Dirección con las labores de implantación, mantenimiento y mejora del SGSI, algo crucial en el buen funcionamiento del mismo.

En cuanto a los demás apartados, también presentan graves deficiencias que deben subsanarse y mejorarse, sobre todo teniendo en cuenta la criticidad del negocio en cuestión. Por ello, se hace tan importante la implantación de un SGSI acorde a la normativa de referencia y por consecuente la elaboración de este Plan Director.

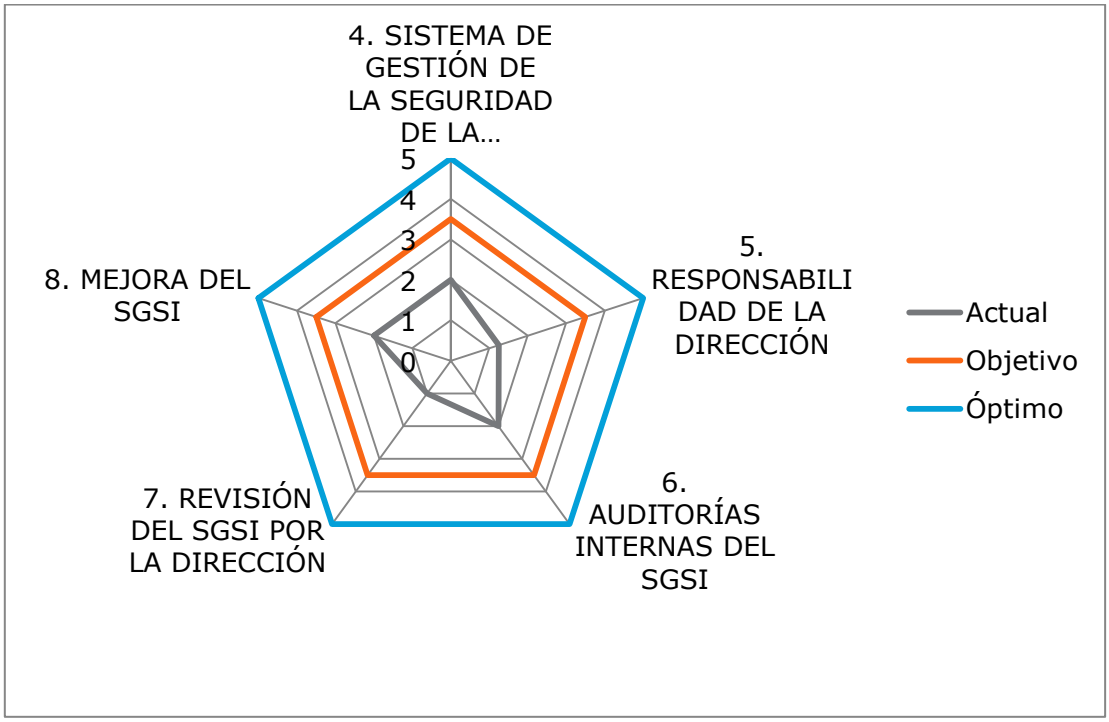

Figura 2-1: Gráfico radial de representación del análisis diferencial respecto a la ISO/IEC 27001:2005

2.4.2 TABLA ANÁLISIS DIFERENCIAL ISO/IEC 27002:2005

En la Tabla 2-3 se recoge el análisis diferencial respecto a la norma ISO/IEC 27002:2005 [3] tal y como se ha comentado anteriormente.

5	**POLÍTICA DE SEGURIDAD**		
5.1	**POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN**		
5.1.1	Documento de política de seguridad de la información	1 - Inicial	Hay alguna política de seguridad documentada, pero no se ocupa de todos los dominios de seguridad pertinentes ni es conocida por todos los empleados y terceros. La organización tiene un enfoque inconsistente hacia su aprobación y revisión.
5.1.2	Revisión de la política de seguridad de la información	1 - Inicial	La política de seguridad no se revisa a intervalos planificados y no es revisada por la Dirección, solo por algunos miembros del personal de TI.
6	**ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN**		
6.1	**ORGANIZACIÓN INTERNA**		
6.1.1	Compromiso de la Dirección con la seguridad de la información	0 - Inexistente	No existe un comité de seguridad designado por parte de la Dirección.
6.1.2	Coordinación de la seguridad de la información	2 - Repetible	Existe un Departamento de TI dentro de la organización con diversos roles, que se reparten las actividades correspondientes a la seguridad, aunque los procedimientos no están documentados.
6.1.3	Asignación de responsabilidades relativas a la seguridad de la información	1 - Inicial	Aunque existe una asignación de las responsabilidades, ésta ni está documentada ni es formal.
6.1.4	Proceso de autorización de recursos para el tratamiento de la información	1 - Inicial	La Dirección solo provee al Departamento de TI de los recursos imprescindibles en materia de seguridad, y ni mucho menos existe un proceso formal y documentado.
6.1.5	Acuerdos de confidencialidad	2 - Repetible	Existen acuerdos de confidencialidad, pero éstos no son revisados de forma periódica.
6.1.6	Contacto con las autoridades	2 - Repetible	Existen procedimientos de prevención de riesgos y accidentes laborales (incendios, inundaciones, robos, etc.). En el caso de la seguridad de la información, por ejemplo, robos, ataques externos, etc. no se establece

			procedimiento formal.
6.1.7	Contacto con grupos de especial interés	1 - Inicial	Se establecen relaciones con proveedores reconocidos en seguridad de la información, pero esta relación es puramente comercial.
6.1.8	Revisión independiente de la seguridad de la información	1 - Inicial	Se realizan auditorías del sistema, pero no existe una política clara que defina la frecuencia y la metodología.
6.2	**TERCEROS**		
6.2.1	Identificación de los riesgos derivados del acceso de terceros	2 - Repetible	Se hacen estudios de proveedores a la hora de seleccionarlos y siempre se trabaja con compañías importantes.
6.2.2	Tratamiento de la seguridad en la relación con los clientes	2 - Repetible	Se revisan los requisitos de seguridad con los clientes y se establecen controles.
6.2.3	Tratamiento de seguridad en los contratos con terceros	3 - Definido	Se realizan contratos siempre que se contrata un servicio a un tercero, pero éstos no siempre incluyen las clausulas de seguridad correspondientes.
7	**GESTIÓN DE ACTIVOS**		
7.1	**RESPONSABILIDAD SOBRE LOS ACTIVOS**		
7.1.1	Inventario de activos	3 - Definido	Existe un inventario detallado de equipos, servidores y otros dispositivos propiedad de la organización. Sin embargo, no existe un inventario de los activos de información.
7.1.2	Propiedad de los activos	3 - Definido	El propietario del activo figura en el inventario de activos de una forma genérica.
7.1.3	Uso aceptable de los activos	3 - Definido	Existen guías de buenas prácticas para el uso correcto de los activos de la organización.
7.2	**CLASIFICACIÓN DE LA INFORMACIÓN**		
7.2.1	Directrices de clasificación	3 - Definido	Se clasifica la información que contiene datos personales de acuerdo a la legislación vigente de LOPD, pero no se clasifican los activos de información que no contienen información de este tipo.
7.2.2	Etiquetado y manipulado de la información	3 - Definido	La información clasificada esta etiquetada y su manipulación es adecuada.
8	**SEGURIDAD LIGADA A LOS RECURSOS HUMANOS**		
8.1	**ANTES DEL EMPLEO**		

8.1.1	Funciones y responsabilidades	4 - Gestionado	Existe documentación acerca de las funciones y responsabilidades de cada uno de los puestos de trabajo de la organización, sin embargo, no se especifican las responsabilidades en materia de seguridad.
8.1.2	Investigación de antecedentes	4 - Gestionado	Se solicitan referencias y se investigan antecedentes antes de contratar a un tercero.
8.1.3	Términos y condiciones de contratación	4 - Gestionado	En todos los contratos con terceros, se firman cláusulas legales, códigos éticos y acuerdos de confidencialidad.
8.2	**DURANTE EL EMPLEO**		
8.2.1	Responsabilidades de la Dirección	1 - Inicial	No se transmite a los empleados una guía de seguridad clara y concisa.
8.2.2	Concienciación, formación y capacitación en seguridad de la información	1 - Inicial	No existe concienciación, formación y capacitación en seguridad de la información entre el personal con responsabilidades en el SGSI, a excepción del personal de TI.
8.2.3	Proceso disciplinario	0 - Inexistente	No existe un proceso disciplinario formal y claro para los empleados que hayan provocado la violación de la seguridad.
8.3	**CESE DEL EMPLEO O CAMBIO DE PUESTO DE TRABAJO**		
8.3.1	Responsabilidad del cese o cambio	4 - Gestionado	Existe un procedimiento documentado respecto a la baja o cambio de puesto del personal.
8.3.2	Devolución de activos	4 - Gestionado	Existe un procedimiento documentado sobre la devolución de los activos de la organización al finalizar su empleo o contrato.
8.3.3	Retirada de los derechos de acceso	4 - Gestionado	Existe un procedimiento documentado y revisado respecto a la retirada de derechos de acceso en el caso de cese o cambio de puesto de trabajo.
9	**SEGURIDAD FÍSICA Y DEL ENTORNO**		
9.1	**ÁREAS SEGURAS**		
9.1.1	Perímetro de seguridad física	5 - Optimizado	Las instalaciones de la organización están protegidas mediante muros, barreras, puertas y otros elementos físicos. No es posible el

			acceso a las instalaciones físicas sin autorización.
9.1.2	Controles físicos de entrada	5 - Optimizado	Las áreas seguras están protegidas mediante puertas blindadas, cuyo apertura solo es posible utilizando una tarjeta de acceso y un código PIN.
9.1.3	Seguridad de oficinas, despachos e instalaciones	4 - Gestionado	Las salas que albergan los servidores, equipamiento de red y otros dispositivos están protegidas mediante puertas con llave y éstas siempre están custodiadas por el personal de TI. Los despachos están provistos de puertas con cerradura, pero en ocasiones permanecen abiertos sin supervisión.
9.1.4	Protección contra las amenazas externas y de origen ambiental	3 - Definido	La organización está provista de los elementos básicos de protección contra amenazas externas: extintores, detectores de humo, etc. Carece de medidas contra otro tipo de amenazas, como inundaciones.
9.1.5	Trabajo en áreas seguras	4 - Gestionado	Las áreas seguras están físicamente cerradas, pero no se supervisa el trabajo en las mismas.
9.1.6	Áreas de acceso público y de carga y descarga	4 - Gestionado	Se restringen los accesos al área de carga y descarga sólo a personal autorizado.
9.2	**SEGURIDAD DE LOS EQUIPOS**		
9.2.1	Emplazamiento y protección de equipos	3 - Definido	Los equipos están emplazados en zonas físicamente seguras, pero su situación y sus condiciones ambientales no siempre son adecuadas para protegerlos ante amenazas externas.
9.2.2	Instalaciones de suministro	3 - Definido	Existen equipos de protección frente a fallos de alimentación (SAIs, diferenciales, etc.) pero sólo en equipos especialmente sensibles (servidores, equipamiento de red), quedando fuera de esta protección algunos equipos de trabajo.
9.2.3	Seguridad del cableado	5 - Optimizado	El cableado eléctrico y de telecomunicaciones está

			protegido frente a interceptaciones o daños.
9.2.4	Mantenimiento de los equipos	4 - Gestionado	Los equipos reciben un mantenimiento correcto y éste sólo se lleva a cabo por el personal autorizado. Sin embargo, no se mantienen registros de fallos.
9.2.5	Seguridad de los equipos fuera de las instalaciones	1 - Inicial	No se aplican medidas especiales a los equipos que son utilizados fuera de la organización.
9.2.6	Reutilización o retirada segura de equipos	1 - Inicial	No existe ningún procedimiento documentado respecto a la retirada o reutilización de equipos, y sólo algunos empleados son conscientes de su importancia
9.2.7	Retirada de materiales propiedad de la empresa	1 - Inicial	Se requiere autorización para sacar equipos o otro tipo de activo fuera de la organización, pero ésta no es formal ni se da por escrito. No se establecen limitaciones al tiempo que el activo puede estar fuera de la organización.
10	**GESTIÓN DE COMUNICACIONES Y OPERACIONES**		
10.1	**RESPONSABILIDADES Y PROCEDIMIENTOS DE OPERACIÓN**		
10.1.1	Documentación de los procedimientos de operación	3 - Definido	Existen procedimientos documentados para algunas actividades, tales como procedimientos de copias de respaldo, tratamiento y manipulación de datos personales, etc. Sin embargo, hay falta de documentación para otros procedimientos.
10.1.2	Gestión de cambios	3 - Definido	Se lleva un control de cambios, aunque no es muy exhaustivo y no identifica el área de trabajo ni aplica ninguna clasificación.
10.1.3	Segregación de tareas	4 - Gestionado	Existe segregación de tareas en la medida de lo posible, dado el tamaño de la organización. Existe monitorización y supervisión por la Dirección en actividades críticas.
10.1.4	Separación de los recursos de desarrollo, prueba y operación	3 - Definido	Las áreas de desarrollo y operación están debidamente diferenciadas y se segregan funciones dentro del personal

			de TI. Sin embargo, no existe ninguna política documentada al respecto.
10.2	**GESTIÓN DE LA PROVISIÓN DE SERVICIOS POR TERCEROS**		
10.2.1	Provisión de servicios	3 - Definido	Se comprueban las definiciones, los acuerdos de provisión y los recursos empleados cuando se contrata un servicio a un tercero. No se tienen demasiado en cuenta los controles de seguridad empleados por el tercero y los acuerdos no se revisan periódicamente.
10.2.2	Supervisión y revisión de los servicios prestados por terceros	3 - Definido	Se monitorizan los niveles de servicio prestados por un tercero, pero no se llevan a cabo auditorías de forma periódica.
10.2.3	Gestión del cambio en los servicios prestados por terceros	3 - Definido	Se gestionan los cambios realizados en la provisión de servicios de terceros y se actualizan los procedimientos. Sin embargo, la gestión podría mejorar.
10.3	**PLANIFICACIÓN Y ACEPTACIÓN DEL SISTEMA**		
10.3.1	Gestión de capacidades	4 - Gestionado	Se supervisa y ajusta la utilización de recursos en la organización, y se realizan proyecciones de los requisitos futuros de capacidad. Sin embargo, falta continuidad en el proceso.
10.3.2	Aceptación del sistema	4 - Gestionado	Se realizan pruebas a los sistemas hardware y software antes de ser explotados en la organización. Sin embargo, estas pruebas no se prolongan en el tiempo de manera continua.
10.4	**PROTECCIÓN CONTRA EL CÓDIGO MALICIOSO Y DESCARGABLE**		
10.4.1	Controles contra el código malicioso	4 - Gestionado	Los equipos y servidores tienen instalados antivirus y firewalls y estos son actualizados continuamente. Los firewalls son muy restrictivos en el acceso a Internet. Sin embargo, falta concienciación en seguridad entre los empleados de la organización.
10.4.2	Controles contra el código descargado en el cliente	3 - Definido	Los antivirus y firewalls protegen a los distintos equipos frente a código

			descargable y previenen la ejecución de acciones no autorizadas por parte del mismo. Sin embargo, no existe una política documentada al respecto y solo algunos empleados son conscientes del peligro.
10.5	**COPIAS DE SEGURIDAD**		
10.5.1	Copias de seguridad de la información	4 - Gestionado	Se realizan copias de seguridad de la información y del software periódicamente y se lleva un control del inventario de las mismas. Sin embargo, los procedimientos de copia no están revisados por la Dirección y no se llevan a cabo pruebas de recuperación.
10.6	**GESTIÓN DE LA SEGURIDAD DE LAS REDES**		
10.6.1	Controles de red	5 - Optimizado	La organización cuenta con una red segmentada (dependiendo de la criticidad de los datos y la exposición al exterior) por firewalls y reglas de acceso. Además, cuenta con dispositivos que detectan comportamientos extraños en la red.
10.6.2	Seguridad de los servicios de red	4 - Gestionado	Se identifican las características de seguridad, los niveles de servicio y los requisitos de gestión pero no en todos los servicios de red. No se revisa muy regularmente que los proveedores de servicio cumplan con las medidas acordadas.
10.7	**MANIPULACIÓN DE LOS SOPORTES**		
10.7.1	Gestión de soportes extraíbles	1 - Inicial	Se establecen controles técnicos sobre el uso de memorias extraíbles, pero no sobre otros dispositivos de almacenamiento. No existe un procedimiento formal documentado.
10.7.2	Retirada de soportes	2 - Repetible	Existen prácticas seguras de destrucción de soportes de almacenamiento entre los empleados de la organización, pero no existe ningún procedimiento documentado ni revisado.

10.7.3	Procedimientos de manipulación de la información	3 - Definido	La información se manipula correctamente y existen prácticas que la protegen contra los accesos no autorizados o el uso indebido. Sin embargo, no existe un procedimiento documentado.
10.7.4	Seguridad de la documentación del sistema	3 - Definido	La información está protegida mediante técnicas criptográficas y reglas de acceso.
10.8	**INTERCAMBIO DE INFORMACIÓN**		
10.8.1	Políticas y procedimientos de intercambio de información	4 - Gestionado	Se han establecido políticas y procedimientos para el intercambio de información. Se han establecido acuerdos de confidencialidad pero faltan controles en la comunicación de voz.
10.8.2	Acuerdos de intercambio	3 - Definido	Se establecen acuerdos de intercambio de información entre la organización y terceros, pero éstos no son revisados de forma periódica.
10.8.3	Soportes físicos en tránsito	3 - Definido	La organización tiene una política sobre el transporte de soportes físicos fuera de la misma. Sin embargo, no todos los empleados la conocen y no se revisa con frecuencia.
10.8.4	Mensajería electrónica	4 - Gestionado	La información enviada por mensajería electrónica esta adecuadamente protegida, utilizando mecanismos de firma electrónica y certificados digitales.
10.8.5	Sistemas de información empresariales	4 - Gestionado	La interconexión de los sistemas empresariales está debidamente controlada y su gestión de acceso es correcta. Existe documentación asociada al respecto.
10.9	**SERVICIOS DE COMERCIO ELECTRÓNICO**		
10.9.1	Comercio electrónico	5 - Optimizado	La organización hace uso y ofrece sistemas de comercio electrónico, por ello, cumple con la legislación vigente al respecto (LOPD, LSSI, LFE, etc.). Además, las operaciones de comercio electrónico están protegidas ante actividades fraudulentas, disputas contractuales y

			revelación de datos, mediante sistemas de encriptación, certificados digitales, etc. Existe una política documentada y revisada al respecto.
10.9.2	Transacciones en línea	5 - Optimizado	Las transacciones en línea se realizan mediante encriptación del canal de comunicación. Se utilizan certificados digitales y firma electrónica en cada una de las partes implicadas. Existe una política formal al respecto.
10.9.3	Información públicamente disponible	4 - Gestionado	La información puesta a disposición pública está protegida ante modificaciones no autorizadas y es revisada.
10.10	**SUPERVISIÓN**		
10.10.1	Registros de auditoría	2 - Repetible	Se generan registros de auditoría en todos los sistemas, pero éstos no incluyen toda la información necesaria. Además, no existe ninguna política documentada al respecto y dichos registros no se mantienen durante un periodo acordado formalmente.
10.10.2	Supervisión del uso del sistema	3 - Definido	Existen procedimientos documentados para supervisar el uso de los sistemas por parte de los usuarios, pero estos no son revisados de forma periódica.
10.10.3	Protección de la información de los registros	4 - Gestionado	Los dispositivos de registro y la información de los registros se protegen de forma adecuada contra manipulaciones y accesos no autorizados, pero no se revisan de forma frecuente.
10.10.4	Registros de administración y operación	2 - Repetible	Se registra cualquier evento del sistema, incluso los realizados por operadores y administradores. Sin embargo, no existe una política documentada ni se revisan dichos registros periódicamente.
10.10.5	Registro de fallos	3 - Definido	Se registran los fallos informados por usuarios o sistemas. Sin embargo, no

			existen reglas claras para el tratamiento de los informes de fallos.
10.10.6	Sincronización del reloj	5 - Optimizado	Los relojes de todos los sistemas están sincronizados utilizando una fuente precisa y acordada de tiempo. Además, la sincronización se revisa periódicamente.
11	**CONTROL DE ACCESO**		
11.1	**REQUISITOS DE NEGOCIO PARA EL CONTROL DE ACCESO**		
11.1.1	Política de control de acceso	4 - Gestionado	Existe una política para el control de acceso basada en los requisitos del negocio y seguridad para el acceso. La política de control de acceso está documentada y revisada.
11.2	**GESTIÓN DE ACCESO DE USUARIO**		
11.2.1	Registros de usuario	5 - Optimizado	La organización dispone de un procedimiento formal de registro y anulación de usuarios para conceder y revocar los derechos de acceso. Este documento se actualiza y revisa con frecuencia.
11.2.2	Gestión de privilegios	4 - Gestionado	La gestión de privilegios es llevada a cabo por el personal de TI. Existe un procedimiento documentado para llevar a cabo dicha gestión.
11.2.3	Gestión de contraseñas de usuario	4 - Gestionado	Se lleva a cabo una gestión correcta de las contraseñas de usuario, asignándoles caducidad y bloqueo y almacenándolas adecuadamente. Existe una política formal sobre la gestión de contraseñas pero no se firman cláusulas de confidencialidad.
11.2.4	Revisión de los derechos de acceso de usuario	0 - Inexistente	No existe ningún proceso formal de revisión de los derechos de acceso.
11.3	**RESPONSABILIDADES DE USUARIO**		
11.3.1	Uso de contraseñas	3 - Definido	La organización provee métodos técnicos para que las contraseñas cumplan con los requisitos básicos de seguridad. Sin embargo, no existe una guía de buenas prácticas en la elección de

			contraseñas para los usuarios.
11.3.2	Equipo de usuario desatendido	3 - Definido	Hay establecidos controles técnicos para el bloqueo de equipos desatendidos. Sin embargo, no existe una guía de buenas prácticas dirigida a los usuarios.
11.3.3	Política de puesto de trabajo despejado y pantalla limpia	1 - Inicial	No existe una política formal de puesto de trabajo despejado y pantalla limpia, solo las técnicas de bloqueo de pantalla.
11.4	**CONTROL DE ACCESO A LA RED**		
11.4.1	Política de uso de los servicios en red	3 - Definido	El uso de los servicios de red está controlado por el personal de TI y sólo se habilita el acceso previa autorización, pero no existe una política formal.
11.4.2	Autenticación de usuario para conexiones externas	4 - Gestionado	Se usan técnicas criptográficas implementadas mediante redes VPN. Existe un procedimiento documentado y revisado sobre conexiones desde el exterior a servidores de la organización.
11.4.3	Identificación de los equipos en las redes	4 - Gestionado	Todos los equipos están identificados dentro de la red.
11.4.4	Diagnóstico remoto y protección de los puertos de configuración	5 - Optimizado	Los puertos de configuración de equipos, servidores y dispositivos de red tienen las medidas de protección físicas y lógicas oportunas.
11.4.5	Segregación de las redes	5 - Optimizado	Existe segregación de redes dentro de la organización, y ésta se hace teniendo en cuenta la criticidad, exposición al exterior y el valor de la información que protegen.
11.4.6	Control de la conexión a la red	4 - Gestionado	Se establecen controles de conexión a la red mediante firewalls y otros dispositivos. Además, se monitorizan los accesos pero no son revisados frecuentemente.
11.4.7	Control de encaminamiento (*routing*) de red	4 - Gestionado	Se implementan controles de encaminamiento de red, direccionando el tráfico a los firewalls y estableciendo en éstos las reglas de acceso.
11.5	**CONTROL DE ACCESO AL SISTEMA OPERATIVO**		
11.5.1	Procedimientos seguros de	4 - Gestionado	Se implementan mecanismos

	inicio de sesión		técnicos de inicio seguro de sesión: bloqueo de contraseña por intentos fallidos, tiempo de espera por bloqueo de cuenta, no mostrar el último usuario bloqueado, etc. Sin embargo, no existe una política formal al respecto.
11.5.2	Identificación y autenticación de usuario	3 - Definido	No todos los usuarios disponen de un identificador único para su uso personal, y se hace uso de identificadores genéricos para los accesos al sistema.
11.5.3	Sistema de gestión de contraseñas	5 - Optimizado	El sistema de gestión de contraseñas es correcto, permite a los usuarios cambiar sus propias contraseñas, fuerza la elección de contraseñas de calidad, fuerza el cambio de contraseñas, etc.
11.5.4	Uso de los recursos del sistema	3 - Definido	Sólo el personal de TI tiene acceso a las utilidades del sistema operativo que pueden comprometer la seguridad. En los equipos existen algunas aplicaciones innecesarias y no existe una política documentada al respecto.
11.5.5	Desconexión automática de sesión	3 - Definido	No se implementan mecanismos de cierre de sesión después de un período de inactividad en los equipos de usuario, aunque sí en el acceso a sistemas remotos.
11.5.6	Limitación del tiempo de conexión	4 - Gestionado	Se implementan medidas de re-autenticación en aplicaciones de alto riesgo (banca online).
11.6	**CONTROL DE ACCESO A LAS APLICACIONES Y A LA INFORMACIÓN**		
11.6.1	Restricción del acceso a la información	4 - Gestionado	Las aplicaciones implementan diferentes vistas dependiendo del perfil del usuario. Existe una política formal al respecto.
11.6.2	Aislamiento de sistemas sensibles	5 - Optimizado	Los sistemas sensibles están aislados y correctamente protegidos bajo los requisitos del negocio y del propietario de los datos.
11.7	**ORDENADORES PORTÁTILES Y TELETRABAJO**		

11.7.1	Ordenadores portátiles y comunicaciones móviles	2 - Repetible	Existen buenas prácticas dentro de la organización respecto al tratamiento de información con ordenadores portátiles y otros dispositivos fuera de la organización. Sin embargo, no existe una política documentada, revisada y aceptada por todos los empleados.
11.7.2	Teletrabajo	1 - Inicial	No existe una política formal al respecto, solamente una serie de recomendaciones generales.
12	**ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN**		
12.1	**REQUISITOS DE SEGURIDAD DE LOS SISTEMAS DE INFORMACIÓN**		
12.1.1	Análisis y especificación de los requisitos de seguridad	3 - Definido	En el análisis y especificaciones de los nuevos productos se suelen evaluar las características y controles de seguridad aunque no siempre. No se realizan evaluaciones de riesgos.
12.2	**TRATAMIENTO CORRECTO DE LAS APLICACIONES**		
12.2.1	Validación de los datos de entrada	4 - Gestionado	Se aplica validación de los datos de entrada en las aplicaciones para protegerlas de ataques comunes.
12.2.2	Control del procesamiento interno	4 - Gestionado	Las aplicaciones de la organización realizan un control interno de la información que manejan vigilando la integridad de los datos y evitando ataques comunes.
12.2.3	Integridad de los mensajes	2 - Repetible	Las aplicaciones no incorporan la verificación de la integridad de los mensajes aunque existen controles adicionales que pueden complementar este objetivo.
12.2.4	Validación de los datos de salida	2 - Repetible	No se realiza la validación de los datos de salida en todas las aplicaciones, pero en todos los casos se proporciona al usuario información suficiente para que evalúe su exactitud.
12.3	**CONTROLES CRIPTOGRÁFICOS**		
12.3.1	Política de uso de los controles criptográficos	1 - Inicial	No existe una política formal y aprobada por la Dirección sobre el uso de controles

			criptográficos, solo políticas implementadas por el personal de TI.
12.3.2	Gestión de claves	4 - Gestionado	La organización tiene implementado un sistema de gestión de claves, donde se generan y almacenan los certificados, contraseñas, etc. Este sistema está protegido y existe una política formal sobre su uso.
12.4	**SEGURIDAD DE LOS ARCHIVOS DEL SISTEMA**		
12.4.1	Control del software en explotación	3 - Definido	Existen procedimientos de actualización de software llevados a cabo por el personal de TI. Existen estrategias de restauración. Sin embargo, no se realizan todas las pruebas pertinentes antes de implantar el software.
12.4.2	Protección de los datos de prueba del sistema	1 - Inicial	No se establece protección adicional a los datos de prueba, se utilizan los mismos mecanismos y controles que con los datos reales.
12.4.3	Control de acceso al código fuente de los programas	4 - Gestionado	Sólo el personal autorizado tiene acceso al código fuente de los programas y éste está protegido contra modificaciones. Se realiza un registro de cambios.
12.5	**SEGURIDAD EN LOS PROCESOS DE DESARROLLO Y SOPORTE**		
12.5.1	Procedimientos de control de cambios	2 - Repetible	La organización lleva a cabo un procedimiento de gestión de cambios. Esta gestión de cambios realiza un registro de los pasos realizados y permite trazar una pequeña auditoría del proceso, pero el procedimiento necesita mejoras.
12.5.2	Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo	4 - Gestionado	Se realizan pruebas técnicas en aplicaciones y sistemas tras efectuarse cambios en el sistema operativo.
12.5.3	Restricciones a los cambios en los paquetes de software	5 - Optimizado	Todos los cambios de software son evaluados y probados y sólo se realizan si son estrictamente necesarios. Siempre se conserva el software original.
12.5.4	Fugas de información	4 - Gestionado	Se limita el riesgo de fuga de

			información privando a los empleados de escáneres o dispositivos de almacenamiento, limitándose el tamaño de salida de los correos, etc.
12.5.5	Externalización del desarrollo de software	3 - Definido	En algunos casos, se externaliza el desarrollo de software y algunos de estos contratos carecen de clausulas de interés para la organización (propiedad del código, requisitos de calidad y seguridad del software, etc.).
12.6	**GESTIÓN DE LA VULNERABILIDAD TÉCNICA**		
12.6.1	Control de las vulnerabilidades técnicas	3 - Definido	Se realizan análisis de vulnerabilidades en sistemas y software más común, pero se no se realiza en otras aplicaciones utilizadas en algunos equipos.
13	**GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN**		
13.1	**NOTIFICACIÓN DE EVENTOS Y PUNTOS DÉBILES DE SEGURIDAD DE LA INFORMACIÓN**		
13.1.1	Notificación de eventos de seguridad de la información	3 - Definido	La organización posee un sistema de gestión de incidencias donde los usuarios pueden notificar las incidencias, aunque el sistema ofrece poco detalle. No existe documentación formal del sistema.
13.1.2	Notificación de puntos débiles de seguridad	1 - Inicial	Los empleados y terceros notifican las incidencias en el sistema, pero no los puntos débiles de seguridad, muchas veces por falta de conocimiento.
13.2	**GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN Y MEJORAS**		
13.2.1	Responsabilidades y procedimientos	1 - Inicial	Los incidentes de seguridad son gestionados por el personal de TI pero no se definen responsabilidades específicas ni procedimientos claros de gestión.
13.2.2	Aprendizaje de los incidentes de seguridad de la información	1 - Inicial	No se establecen mecanismos de aprendizaje sobre los incidentes de seguridad.
13.2.3	Recopilación de evidencias	3 - Definido	Existe un procedimiento documentado de recolección de evidencias pero éste no sigue una metodología

			específica, pudiendo quedar dichas evidencias invalidadas como prueba.
14	**GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO**		
14.1	**ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN EN LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO**		
14.1.1	Inclusión de la seguridad de la información en el proceso de gestión de la continuidad del negocio	3 - Definido	La organización cuenta con un procedimiento de gestión de la continuidad del negocio, incluyendo aspectos básicos de seguridad de la información, pero que deja mucho que desear respecto a la criticidad de las actividades de la organización.
14.1.2	Continuidad del negocio y evaluación de riesgos	2 - Repetible	Los análisis de riesgos llevados a cabo en la organización no siguen una metodología correcta, por tanto, el plan de continuidad que han desarrollado es deficiente.
14.1.3	Desarrollo e implantación de planes de continuidad que incluyan la seguridad de la información	2 - Repetible	El plan de continuidad desarrollado sólo incluye aspectos básicos de seguridad de la información.
14.1.4	Marco de referencia para la planificación de la continuidad del negocio	1 - Inicial	No se mantiene un marco de referencia coherente ni consistente.
14.1.5	Pruebas, mantenimiento y reevaluación de los planes de continuidad del negocio	1 - Inicial	Las pruebas realizadas sobre los planes de continuidad del negocio no se realizan con una frecuencia determinada. La actualización de dichos planes debería llevarse a cabo más regularmente.
15	**CUMPLIMIENTO**		
15.1	**CUMPLIMIENTO DE LOS REQUISITOS LEGALES**		
15.1.1	Identificación de la legislación aplicable	5 - Optimizado	La organización cumple con la legislación vigente (LOPD, LSSI, LFE, etc.).
15.1.2	Derechos de propiedad intelectual (DPI)	5 - Optimizado	La organización cumple debidamente con la Ley de Propiedad Intelectual.
15.1.3	Protección de los documentos de la organización	5 - Optimizado	La organización almacena y protege debidamente la documentación importante y establece adecuadamente mediante políticas formales periodos de retención de la información.
15.1.4	Protección de datos y privacidad de la información de carácter	5 - Optimizado	La organización cumple con la legislación en materia de

	personal		protección de datos de carácter personal.
15.1.5	Prevención del uso indebido de los recursos de tratamiento de la información	4 - Gestionado	La organización lleva a cabo medidas técnicas para prevenir el mal uso de los recursos informáticos. Sin embargo, debería proporcionarse información al respecto a los empleados.
15.1.6	Regulación de los controles criptográficos	3 - Definido	La organización cumple con la regulación en cuanto a controles criptográficos, pero no existe documentación específica al respecto.
15.2	**CUMPLIMIENTO DE LAS POLÍTICAS Y NORMAS DE SEGURIDAD Y CUMPLIMIENTO TÉCNICO**		
15.2.1	Cumplimiento de las políticas y normas de seguridad	2 - Repetible	No se realizan auditorias formales del cumplimiento de las políticas y normas de seguridad, aunque se realizan revisiones de forma informal.
15.2.2	Comprobación del cumplimiento técnico	3 - Definido	Se llevan a cabo comprobaciones del cumplimiento técnico de los sistemas de información por el personal de TI, pero no se planifican y documentan adecuadamente.
15.3	**CONSIDERACIONES SOBRE LA AUDITORÍA DE LOS SISTEMAS DE INFORMACIÓN**		
15.3.1	Controles de auditoría de los sistemas de información	3 - Definido	Se realizan auditorias de los sistemas de información, pero los requisitos de las mismas y la periodicidad con que se realizan no están acordados con la Dirección.
15.3.2	Protección de las herramientas de auditoría de los sistemas de información	3 - Definido	Las herramientas y archivos de auditoría solamente son accesibles por el personal de TI, pero no tienen una protección especial.

Tabla 2-3: Tabla de análisis diferencial respecto a la norma ISO/IEC 27002:2005

Resumen de resultados

Una vez realizado el análisis diferencial revisando el nivel de madurez actual de cada uno de los controles de la norma ISO/IEC 27001:2005 [2] en la organización, se han introducido los datos en la herramienta *Data Security Maturity Model*, la cual nos ofrece resultados en forma numérica de este análisis.

Según dicha herramienta, el nivel de madurez promedio de la organización respecto a la norma es de 2.26/5.00, por tanto, se puede decir que el nivel de madurez es "Repetible" (escala CMM [5]). En la Figura 2-2, se puede observar un gráfico radial que

muestra la representación del estado actual respecto a cada uno de los dominios de la norma, el estado que se pretende alcanzar a corto/medio plazo y el estado óptimo o ideal de madurez.

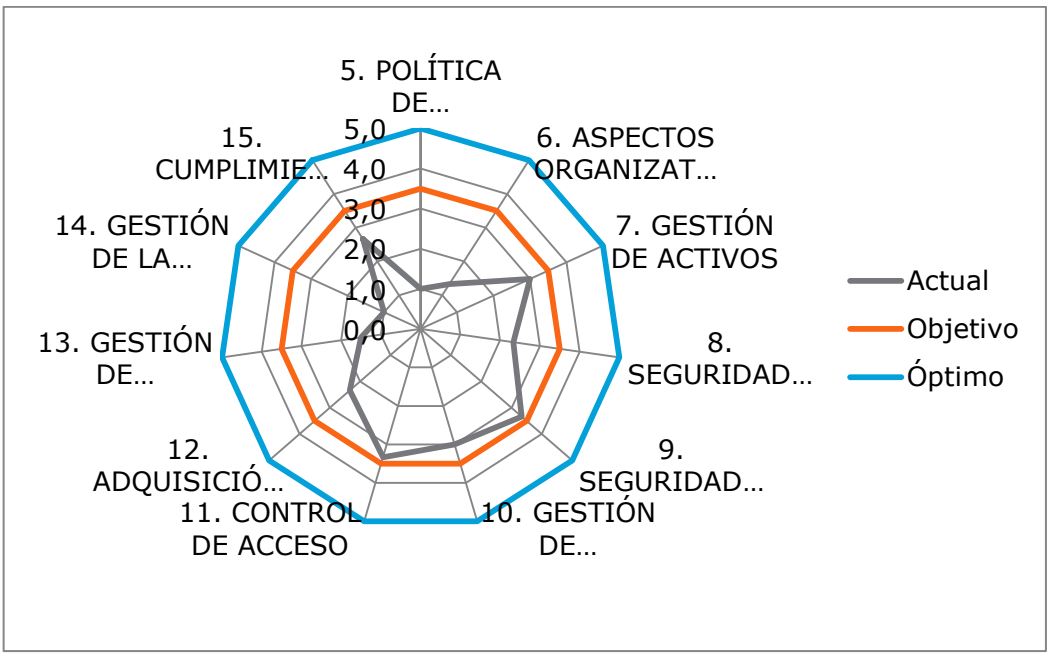

Figura 2-2: Gráfico radial de representación del análisis diferencial respecto a la ISO/IEC 27002:2005

CAPÍTULO 3. SISTEMA DE GESTIÓN DOCUMENTAL

Cualquier sistema de gestión está apoyado en un sistema de gestión documental, por tanto, un SGSI también. En este capítulo se elaborará la documentación básica para implementar un SGSI que cumpla con los requisitos documentales de la norma ISO/IEC 27001:2005 [2]. La existencia de todos estos documentos constituye una evidencia imprescindible para certificar que el SGSI está funcionando correctamente.

3.1 POLÍTICA DE SEGURIDAD

3.1.1 INTRODUCCIÓN

La información es uno de los activos más importantes en la organización. Uno de los objetivos principales es asegurar los recursos informáticos, incluyendo los sistemas de información, las redes de comunicación y sobre todo los datos que estén almacenados en cualquier medio ya que son parte integral de los servicios y gestión de la empresa.

Para la adecuada gestión de la seguridad de la información, la Dirección ha decidido implantar un sistema que aborde esta tarea de una forma metódica, documentada y basada en unos objetivos claros de seguridad y una evaluación de los riesgos a los que está sometida la información de la organización.

Se pretende que está política constituya la base para las buenas prácticas en seguridad de la información dentro de la organización, y que sea conocida y aplicada por todo el personal tanto interno como externo que traten con información de la misma.

3.1.2 OBJETIVOS

El objetivo de la presente política es establecer las directivas generales relacionadas con la seguridad de la información que contribuyan a garantizar:

1. La confidencialidad de la información.
2. La integridad de la información.
3. La disponibilidad de la información.

3.1.3 ALCANCE

Esta política se aplica a todo el ámbito de la organización, ya sean recursos humanos o tecnológicos, a todos los procesos internos o externos, a los proveedores, prestadores de servicios o cualquier otro tercero que de alguna forma interactúen habitual u ocasionalmente con la información o con los equipos y dispositivos que la almacenen, transmitan y procesen.

3.1.4 SEGURIDAD FÍSICA

El acceso físico a cualquier activo de información tangible tales como servidores, elementos de red, documentos, etc. debe estar correctamente restringido.

Control de acceso físico

El acceso a dependencias que se consideren críticas (ubicación de servidores centrales, Departamento de TI) será controlado por medio de sistemas que controlen el acceso, tales como tarjetas de proximidad y/o sistemas biométricos que limiten la entrada/salida, además de cámaras de videovigilancia, detectores de intrusión y otros medios que permitan alertar de intentos de accesos no autorizados.

Estos lugares deberán contar con carteles externos que indiquen el nivel de seguridad aplicado. Las puertas tendrán sistemas de control de tiempo de apertura con alarmas.

El ingreso de una persona no autorizada a áreas críticas, deberá ser solo con el acompañamiento, en todo momento, de alguna persona responsable del área.

Los medios utilizados para el acceso de empleados y proveedores, como por ejemplo, tarjetas, perfiles de usuarios, etc. serán desactivados o eliminados una vez se termine el vínculo de éstos con la organización. En caso de pérdida de una tarjeta de acceso, se comunicará inmediatamente al Departamento de TI para desactivarla.

Todos los empleados deben tener especial cuidado de no permitir el paso a personas no autorizadas a áreas críticas o restringidas (oficinas, despachos de Dirección, etc.).

Como mecanismo de prevención se prohíbe comer o beber dentro de instalaciones con equipos tecnológicos.

Equipos, puestos de trabajo y otros recursos

Todo equipo informático, sean propios o de terceros, que procesen información o posean conectividad con los sistemas de la organización, deben cumplir con

mecanismos de seguridad física que eviten el acceso a los mismos de personas no autorizadas.

Los equipos, equipos de comunicaciones, teléfonos, etc. no deben moverse, reubicarse o ser sacados de las instalaciones sin autorización.

Los servidores de datos, de aplicaciones y equipos de comunicaciones estarán ubicados en lugares seguros de acuerdo a lo que definen las mejores prácticas de la industria y las normas en las se basa está política.

Ninguna estación de trabajo, portátil o dispositivo móvil del exterior, podrá ser conectado a la red de la organización sin antes ser verificados y autorizados por el Departamento de TI. Las tomas de redes no utilizadas estarán desactivadas.

Protección física de la información

Todo el personal interno y externo de la organización será responsable del adecuado uso de la información suministrada para el desempeño de su labor profesional, por lo que se debe velar por su integridad, confidencialidad y disponibilidad.

Toda información crítica, secreta y privada en cualquiera de sus formas (impresa, electrónica, etc.) debe ser resguardada y estar provista de la seguridad necesaria por quien la maneja para evitar el uso indebido por parte de personal no autorizado.

3.1.5 PERÍMETRO (COMUNICACIONES Y ACCESO A LA RED INTERNA)

Los sistemas de comunicaciones como la red interna, deben estar adecuadamente limitados y protegidos por elementos de red tales como firewalls, routers u otra tecnología que realice un control de acceso a las mismas. Toda información crítica que circula por las redes de comunicación de la organización deberá estar cifrada.

Control del perímetro

Se deben instalar y mantener firewalls o componentes de red con funciones equivalentes para proteger a los segmentos de red con datos críticos contra accesos no autorizados desde el exterior, desde una zona desmilitarizada (DMZ), o desde el interior de la red.

Conexiones con redes públicas e Internet

Las redes inalámbricas se consideran no confiables por lo tanto no se permite el acceso a la red interna utilizando conexiones WiFi.

No se permiten las conexiones a través de modems.

El acceso a salas de chat y mensajería instantánea solo será habilitado al personal que justifique fehacientemente su utilización, previa autorización de la Dirección.

No se utilizarán plataformas de comunicación inseguras (salas de chat, aplicaciones de mensajería instantánea, etc.) para discutir o comentar temas relacionados con el negocio.

Todo el personal interno y externo de la organización deberá adecuarse a la legislación vigente, sobre derechos de reproducción, patentes y todo lo relacionado con derechos de autor que se aplica en Internet.

No está permitida la instalación de software o archivos obtenidos de Internet.

No está permitido el uso de los equipos de la organización para el acceso a Internet con fines personales. Se monitorizan las actividades en Internet como accesos a correo web, salas de chat, mensajería instantánea, etc.

Los empleados que accidentalmente se conecten a páginas de Internet que tengan contenidos sexuales, racistas o cualquier otro tipo de material ofensivo deberán desconectarse inmediatamente por el riesgo que estas representan y deberán informar al Departamento de TI, para que los sitios sean bloqueados.

Conexiones con terceros

La conexión entre los sistemas internos de la organización y otros sistemas de terceros debe ser aprobada y certificada por el Departamento de TI con el fin de no comprometer la seguridad de la información interna.

Se llevarán a cabo inspecciones a los sistemas de comunicación y de aplicaciones de terceros con el fin de verificar que la información se esté manejando con las medidas de seguridad acordadas.

Aspectos sobre la red interna

Toda información crítica que circula por las redes de comunicación deberá estar cifrada, para lo cual se deben utilizar protocolos y criptografía solidas.

Se deberá propiciar la segmentación de las redes de comunicaciones de tal forma que los usuarios mantengan una independencia sobre las mismas.

Servicios internos

- Intranet

El material que se publique en la Intranet debe ser revisado previamente para confirmar la actualidad e importancia de la información y evitar que incluya código malicioso como virus y/o troyanos.

- Correo electrónico

El correo electrónico no debe ser utilizado por terceros sin previa autorización.

No se debe transmitir información confidencial por correo electrónico, a no ser que este en formato protegido.

Los usuarios del correo electrónico de la organización no deben utilizar cuentas de correo electrónico que pertenezcan a otros usuarios.

Los usuarios del correo de la organización no deben enviar mensajes de correo electrónico con contenidos hostiles que molesten a los receptores del mismo, como comentarios sobre sexo, raza, religión o preferencias sexuales. Cuando un empleado reciba este tipo de mensajes, debe comunicarlo a su superior.

Ningún empleado está autorizado a monitorizar mensajes de correo electrónico.

El sistema de correo electrónico de la organización debe ser usado únicamente para propósitos laborales.

Se deben establecer procedimientos seguros para el envío de archivos adjuntos en los mensajes. Se recomienda la utilización de firma digital.

3.1.6 HARDWARE (ESTACIONES DE TRABAJO Y SERVIDORES)

Los servidores y las estaciones de trabajo deben estar convenientemente protegidos considerando la configuración de los sistemas operativos, el acceso no autorizado a los mismos, malware y actualizaciones de seguridad.

Aspectos de instalación

Todos los servicios y protocolos innecesarios e inseguros de cada servidor deberán ser deshabilitados.

Los parámetros de seguridad de cada servidor deben estar configurados adecuadamente de acuerdo a los manuales de políticas definidas, deben estar activos y actualizados.

Todo acceso administrativo que no sea de consola local, deberá estar cifrado. Se deben utilizar tecnologías como SSH, VPN o SSL/TLS o semejantes en seguridad en los casos que corresponda.

Herramientas contra software malicioso

Los programas de protección contra software malicioso (antivirus) deben estar instalados y actualizados en todas las estaciones de trabajo y servidores. Estos programas deben estar activos, actualizados y deben generar registros de auditoría.

Los programas antivirus deben tener activados la actualización automática y la exploración periódica.

El software de firewall local debe estar instalado, activado y actualizado en todas las estaciones de trabajo, en particular en los dispositivos con conectividad directa a Internet.

Parches de seguridad

Todos los equipos y software deben contar con los últimos parches de seguridad proporcionados por los proveedores que sean importantes para el buen funcionamiento del sistema. Los parches importantes de seguridad deben instalarse dentro del plazo máximo de tres meses desde su lanzamiento.

Evaluaciones de seguridad - Detección de vulnerabilidades

Deberán ejecutarse trimestralmente evaluaciones internas de vulnerabilidades por medio de herramientas especializadas para ayudar a mantener un estado seguro de la red, las aplicaciones y los servidores.

Deberá ejecutarse por lo menos anualmente una revisión de vulnerabilidades de la red, servidores, aplicaciones externas y aplicaciones internas. Esta tarea deberá ser ejecutada por una empresa especializada en este tipo de servicio.

Acceso lógico y físico

Todas las conexiones con los sistemas y redes deben ser realizadas por medio de dispositivos probados y aprobados y se debe contar con mecanismos de autenticación de usuarios.

Los equipos que pueden ser accedidos por terceros estarán protegidos por mecanismos de control aprobados por el Departamento de TI.

3.1.7 APLICACIONES Y SOFTWARE

Todos los sistemas de información utilizados por la organización deberán contemplar los aspectos mencionados a continuación relacionados a la seguridad implementada en los mismos. Los empleados deben velar por su cumplimiento.

Control de acceso

Si el sistema de control de acceso a un computador o red no está funcionando apropiadamente, debe suspenderse el acceso a todos los usuarios.

Toda transacción que afecte a información de valor, sensible o crítica debe ser procesada únicamente cuando se valide la autenticidad del origen (usuario o sistema) y se compruebe su autorización mediante un mecanismo de control de acceso o perfiles.

Todo programa, equipo y archivo que contenga fórmulas, algoritmos u otras especificaciones que se utilicen para la generación de claves debe estar controlado con las más altas medidas de seguridad.

Las contraseñas estarán cifradas en todo momento y nunca serán escritas o incorporadas dentro de los programas fuentes. Todos los sistemas deberán implementar controles que impidan la recuperación de las palabras clave almacenadas.

Todas las contraseñas emitidas inicialmente por el Departamento de TI deben ser válidas solamente para el primer acceso del usuario, inmediatamente después la aplicación deberá solicitar el cambio de la misma asegurando que solamente el propietario conozca su contraseña.

Perfiles de usuario y privilegios

- Controles de accesos

Los perfiles de usuario serán definidos de acuerdo a la función y cargo de cada empleado de tal forma que la información solo sea accedida y/o modificada por los usuarios autorizados y en los horarios establecidos.

Los usuarios no abandonarán su computador, estación de trabajo sin haber realizado el cierre de la sesión activa y bloquear su sesión.

El acceso a los sistemas debe realizarse por medio de un código de identificación y contraseña únicos para cada usuario.

Los errores de *user ID* o *password* durante el acceso no mostrarán mensajes declarando la fuente del problema, simplemente debe informar que el acceso es incorrecto.

El sistema operativo deberá bloquear la cuenta del usuario después de tres intentos fallidos y consecutivos. El bloqueo permanecerá hasta que un responsable de seguridad lo habilite de nuevo previa identificación del usuario.

- Controles sobre las cuentas de usuario

El sistema debe controlar el tiempo de inactividad del usuario y desactivar la sesión de forma automática después de que se haya cumplido el tiempo definido.

El sistema no deberá permitir que ningún usuario maneje simultáneamente sesiones en diferentes terminales, pudiendo abrir hasta las sesiones permitidas en su misma terminal.

Se recomienda que el sistema despliegue información para el usuario de la hora y la fecha del último acceso realizado por el mismo.

- Políticas y administración de contraseñas

En todos los servidores y aplicaciones deberá implementarse sistemas de complejidad de contraseñas.

El sistema debe llevar un histórico de palabras clave, de tal forma que los usuarios no usen palabras utilizadas anteriormente.

Las contraseñas nunca serán presentadas en forma legible en pantalla o impresiones.

El sistema debe obligar de forma automática a todo usuario a cambiar su contraseña según lo definido por las política.

Administración del software

La organización deberá contar con un inventario actualizado del software de su propiedad, el comprado a terceros, el desarrollado internamente o el adquirido bajo licencia.

Los ambientes de desarrollo, pruebas y producción deberán permanecer separados para su adecuada administración, operación, control y seguridad.

La instalación de software en los equipos de la organización deberá ser realizada por el personal del Departamento de TI con la debida autorización del mismo. Esta autorización se basará en la evaluación de la aplicación y la debida justificación para ser instalada.

Los programas que se encuentren en el ambiente de producción, solamente podrán ser modificados de acuerdo con los procedimientos internos establecidos y en todos los casos se considerarán planes de contingencia y recuperación.

Los datos de producción no se deberán utilizar en los entornos de desarrollo y pruebas.

Adquisición de software

La organización implementará un esquema de adquisición de software de terceros que incluya un contrato con el proveedor que contemple cláusulas para la protección de la información y del software adquirido, la documentación correspondiente y los medios de respaldo necesarios.

Las aplicaciones adquiridas de terceros o desarrolladas internamente, deberán incluir en sus especificaciones puntos de seguridad de la información.

Desarrollo de software

La organización implementará una metodología formal para el desarrollo de software seguro y las actividades de mantenimiento que cumplirán con las políticas, normas, procedimientos, controles y otras definiciones del proyecto aplicables en el desarrollo de sistemas y exigibles por el negocio.

Los controles implementados deberán ser como mínimo los exigidos en los puntos relacionados a adquisición de software. Su revisión deberá estar incluida en los planes de auditoría de sistemas.

Para el desarrollo de software solamente podrán ser utilizados generadores y herramientas de los cuales se tenga certeza de su comportamiento seguro y confiable, y que además, haya sido aprobado por el Departamento de TI.

Toda clave o llave de cifrado utilizada en el entorno de pruebas y desarrollo nunca será instalada en el ambiente de producción. Con esto se garantiza que los desarrolladores de software no tendrán conocimiento de las claves y llaves en producción.

Las aplicaciones web deberán ser desarrolladas en base a directrices de codificación segura (por ejemplo, OWASP). Las aplicaciones web públicas deberán ser chequeadas por métodos manuales o automáticos por lo menos una vez al año o después de cada cambio.

Pruebas de software

El ambiente de pruebas será lo más idéntico posible en configuración al ambiente de producción.

Si hay necesidad de introducir llaves o claves utilizadas en el ambiente de producción, éstas deberán ser introducidas y utilizadas de manera segura.

Una vez se hayan realizado todos los cambios al software, detectados durante las pruebas, deberá ejecutarse nuevamente una serie de pruebas integrales, que garanticen su correcto funcionamiento.

El código fuente será revisado en búsqueda de códigos mal intencionados o debilidades de seguridad, utilizando herramientas automáticas, para luego ser compilado y transferido a producción.

Puesta en producción del software

Para la puesta en producción de algún software, deberá existir autorización del responsable de la aplicación, la conformidad del usuario final y la autorización por parte del Departamento de TI.

Las características utilizadas en el entorno de pruebas y que son innecesarias en el ambiente de producción serán identificadas y desactivadas en el momento de la instalación del software.

Antes de la puesta en producción se deberán probar los parches de seguridad asociados y los cambios de configuración del software y del sistema.

Mantenimiento del software

Cuando un tercero efectúe ajustes a algún software deberá firmar un acuerdo de confidencialidad y utilización no autorizada del mismo.

Por cada mantenimiento a la versión del software, también se actualizarán las versiones de respaldo.

Las actualizaciones de software requeridas por la organización deberán contemplar el cumplimiento de los procedimientos de licenciamiento respectivo.

3.1.8 CLASIFICACIÓN, ALMACENAMIENTO Y ADMINISTRACIÓN DE LA INFORMACIÓN

Los empleados de la empresa son responsables de la información que manejan y deberán seguir las siguientes directrices para protegerla y evitar pérdidas, accesos no autorizados y utilización indebida de la misma.

La organización administra, procesa y transmite información que no es de su propiedad, sino de los clientes para quienes presta servicio, por lo tanto la responsabilidad en la custodia de los datos es de vital importancia para garantizar la continuidad de los servicios y del negocio.

Clasificación de la información

Toda la información contenida en los sistemas de la organización deberá ser clasificada de acuerdo a su nivel de sensibilidad. Para ello, se establecen las siguientes categorías:

- CONFIDENCIAL: Información considerada sensible y controlada, que solamente puede ser divulgada interna o externamente a persona o grupo reducido de personas debidamente autorizadas.
- USO INTERNO: Información de divulgación interna segura, no recomendada para divulgación externa.
- PÚBLICA: Información que puede ser divulgada interna y externamente sin riesgos para la organización.

Los responsables de la información serán los encargados de clasificar, proteger y autorizar el acceso a la información. Los responsables asumen el papel de tutores de la información, ya que la propiedad siempre será la propia organización.

Toda información debe etiquetarse según la categoría definida y todos los datos que se divulguen por cualquier medio deben mostrar la clasificación de sensibilidad de la información.

Cuando se consolida información con varias clasificaciones de sensibilidad, los controles usados deben proteger la información más sensible y se deben clasificar con el máximo nivel de restricción que contenga la misma. En caso de ser necesario compartir información sensible desde estaciones de trabajo, se debe utilizar la seguridad que ofrecen los sistemas para restringir el acceso a través de claves o usuarios específicos.

Almacenamiento de la información

- Almacenamiento y respaldo de la información

Las bases de datos que contengan datos críticos deben estar en el segmento de red de datos críticos, segregada de la DMZ.

Los datos confidenciales de autenticación de los usuarios no deberán almacenarse aunque estén cifrados.

Toda información administrada por la organización debe tener una copia de respaldo completa y actualizada, en un sitio externo a la ubicación en que se procesan dichos datos.

Todos los medios físicos donde la información de valor, sensitiva y crítica es almacenada por periodos mayores de seis meses deben mantenerse almacenados bajo condiciones ambientales de temperatura y humedad óptimas que permitan conservar la información.

La organización debe contar con un procedimiento para la restauración de copias de seguridad o *backups*. Estará administrado por el Departamento de TI.

Toda la información contable, de impuestos y de tipo legal debe ser conservada de acuerdo con las normas legales vigentes.

- Administración de llaves criptográficas

Las claves criptográficas utilizadas para el cifrado de los datos del cliente, deberán estar clasificadas como información CONFIDENCIAL y ser protegidas contra divulgación y uso indebido, guardándolas de forma segura en la menor cantidad de ubicaciones y formas posibles.

Todos los procesos y los procedimientos de gestión de claves criptográficas que se utilizan para el cifrado de los datos del cliente deben estar documentados.

Almacenamiento y transmisión por distintos medios

Toda información crítica solamente será remitida fuera de las instalaciones de la organización de forma segura, cumpliendo con los procedimientos establecidos.

Toda la información transmitida por medios como por ejemplo el fax, correo electrónico, chats, etc. deberán seguir procedimientos establecidos para asegurar la confidencialidad e integridad de la información.

No deben enviarse datos críticos por medio de tecnologías de mensajería de usuario final (por ejemplo, el correo electrónico, la mensajería instantánea o el chat) si no están cifrados, en particular los siguientes:

- Número de cuenta corriente o de tarjeta.
- Nombre del titular.
- Fecha de vencimiento de tarjetas.
- Datos completos de la banda magnética de la tarjeta.
- Códigos de seguridad CAV2/CVC2/CVV2/CID.
- Código PIN.

Toda información crítica que aparece en recibos generados por computador, y entregados a clientes, debe ser truncada o enmascarada siguiendo lo que recomienda la norma de presentar solo los primeros seis dígitos y los cuatro últimos.

Eliminación de datos

La eliminación de la información debe seguir procedimientos seguros y debidamente aprobados por el Departamento de TI.

Administración de la información

Cualquier tipo de información interna no puede ser vendida, transferida o intercambiada con terceros para ningún propósito diferente al del negocio. En caso de que la información sea requerida por auditores internos o externos, la entrega de dicha documentación deberá ser autorizada por el propietario de la información solicitada.

El acceso a depósitos de información (almacenamiento físico o medio magnético) debe restringirse únicamente a personal autorizado.

Cuando la información crítica no está siendo utilizada se la debe guardar en sitios destinados para el efecto, los cuales deben contar con las debidas medidas de seguridad que garanticen su confidencialidad e integridad.

En cualquier momento, el propietario de la información en colaboración con el jefe de Departamento de TI puede reclasificar el nivel de sensibilidad inicialmente aplicado a la información.

Toda divulgación de información CONFIDENCIAL o de USO INTERNO a terceras personas debe estar acompañada por un contrato de confidencialidad que describa explícitamente qué información es restringida y como puede ser usada.

Todos los medios de almacenamiento utilizados en el proceso de construcción, asignación, distribución o encriptación de claves o PIN se deben someter a un proceso de destrucción inmediatamente después de ser usados.

Cuando las palabras claves o números de identificación personal (PIN) sean generados por el sistema, deben ser impresos inmediatamente y nunca ser almacenados en los sistemas.

Validaciones, controles y manejo de errores

Para reducir la probabilidad de ingreso erróneo de datos de alta sensibilidad, todos los procedimientos de ingreso de información deben contener controles de validación.

Todos los errores cometidos por los empleados y que son detectados por los clientes deben cumplir con un proceso de investigación de acuerdo con los procedimientos y tiempos establecidos.

Los controles establecidos en los procesos y las vulnerabilidades de seguridad detectados en los procesos y recursos informáticos, no pueden ser dados a conocer a terceros por parte de los empleados.

3.1.9 RESPONSABILIDADES DEL PERSONAL

La responsabilidad de la seguridad de la información es una obligación de cada funcionario de la organización.

Perfil de usuario, identificación y contraseña de acceso

La identificación del usuario (ID usuario) debe ser único para cada usuario habilitado en los sistemas de la organización.

La identificación, el perfil y la contraseña de acceso del usuario serán de uso personal e intransferible.

Los mecanismos de acceso para el uso de los recursos informáticos otorgados a los usuarios, será exclusiva responsabilidad de cada uno y cuando sean ingresados en los sistemas deberán ser protegidos contra su divulgación a terceros.

El Departamento de TI implementará los medios necesarios para salvaguardar la integridad de la identificación, perfil y contraseña de acceso del usuario.

Las contraseñas se transmitirán o se almacenarán en forma ilegible mediante una sólida criptografía.

Los usuarios serán responsables de todas las actividades llevadas a cabo con su identificación, perfil y contraseña de acceso.

Uso apropiado de la información

Los usuarios no deberán instalar software de aplicación para obtener información de forma no autorizada. Los usuarios finales no tendrán nivel de "Administrador" en sus equipos personales.

Los usuarios no deberán acceder de forma no autorizada a aplicaciones, servidores, estaciones de trabajo individuales y redes informáticas con el propósito de obtener información confidencial o datos no relacionados con su actividad laboral.

Los usuarios tienen la responsabilidad de controlar la integridad, confidencialidad, disponibilidad y trazabilidad de la información que utilicen, especialmente si la información está clasificada como crítica.

Los usuarios deben informar inmediatamente al Departamento de TI de la ocurrencia de intentos de acceso indebido al sistema, aparición de virus informático, ejecución de programas desconocidos y errores del sistema que otorguen facilidades de acceso no previstas en la definición de su perfil de usuario.

3.1.10 REGISTRO DE AUDITORÍA

Los registros de auditoría o logs pueden ser utilizados por la organización en todos los casos que se consideren necesarios (investigaciones internas, investigaciones externas, etc.).

Administración de logs

Se debe establecer un proceso para vincular todos los accesos a componentes del sistema a cada usuario en particular. Estas medidas se tomarán con el requisito específico de rastrear y monitorizar todos los accesos a los recursos del sistema que luego podrán ser utilizados para determinar y/o reconstruir los eventos ocurridos en los componentes del sistema.

Todos los archivos de logs de los diferentes sistemas deben almacenarse por periodos definidos según su criticidad y la exigencia de la legislación vigente. Además, deben ser custodiados de forma segura para que no puedan ser modificados y para que puedan ser leídos únicamente por personas autorizadas. Todos los accesos a datos críticos, así como a los elementos de sistemas deben quedar registrados en los registros de auditoría.

Estos registros deben contener información suficiente para que por sí mismo o en conjunción con otros recursos puedan identificar las actividades realizadas y vincularlos con cada usuario en particular.

Los logs deben tener mecanismos de seguridad y control administrativo resistentes a ataques capaces de detectar y grabar eventos significativos de seguridad de la información. Estos ataques incluyen intentos de desactivar, modificar, o detectar las claves de acceso al software y/o a los mismos logs.

Para cada evento deben registrarse los siguientes datos: identificación del usuario, tipo de evento, fecha y hora, estado de éxito o falla, origen del evento, identidad o nombre de los datos, componentes del sistema o recursos comprometidos.

Los relojes de los sistemas que sean críticos deben estar sincronizados al efecto de tener la misma fecha y hora para que el registro de log sea confiable.

3.2 PROCEDIMIENTO DE AUDITORÍAS INTERNAS

3.2.1 OBJETIVO

Establecer la planificación a seguir para la realización de auditorías internas al SGSI, además de definir los requisitos requeridos para los encargados de realizar dichas auditorías y el modelo para informar de sus resultados.

3.2.2 ALCANCE

Este procedimiento es aplicable a los procesos comprendidos dentro del alcance del SGSI, bajo la norma ISO/IEC 27001:2005. Prácticamente todas las áreas de la organización realizan actividades o procesos relacionados con el SGSI, por tanto, las auditorías planificadas a continuación cubrirán casi el total de áreas de la organización.

3.2.3 PLANIFICACIÓN DE AUDITORÍAS

Una vez conseguida la certificación del SGSI de la organización en base a la norma ISO/IEC 27001, se llevarán a cabo distintas auditorías internas del mismo, con el objetivo principal de contribuir a su mejora continua, y por consiguiente, al mantenimiento de la certificación. De manera anual, se realizarán las siguientes auditorías internas en las distintas localizaciones de la organización:

Auditoria 1

- Periodo de auditoría: Meses de Enero y Febrero.

- Objetivos:
    - Supervisar las acciones llevadas a cabo para corregir las no conformidades detectadas en auditorías previas.
    - Revisión de la política de seguridad de la organización.
    - Revisión de la política de derechos de acceso y elementos de seguridad física.

Auditoría 2

- Periodo de auditoría: Meses de Abril y Mayo.
- Objetivos:
    - Supervisar las acciones llevadas a cabo para corregir las no conformidades detectadas en auditorías previas.
    - Supervisión de las medidas de protección contra código malicioso.
    - Revisión de la política de copias de seguridad.
    - Revisión de los controles criptográficos.

Auditoría 3

- Periodo de auditoría: Meses de Septiembre y Octubre.
- Objetivos:
    - Supervisar las acciones llevadas a cabo para corregir las no conformidades detectadas en auditorías previas.
    - Supervisar los mecanismos y procedimientos de gestión de incidencias.
    - Supervisión del cumplimiento de los requisitos legales.
    - Supervisión del procedimiento de auditorías internas en la organización.

Se podría decir que la realización de estas tres auditorías en cada una de las localizaciones en que se distribuye la organización conforman la realización de una gran auditoría interna en la organización, que va a permitir superar las auditorías anuales de seguimiento llevadas a cabo por parte de la entidad de certificación durante el periodo de vigencia del certificado.

3.2.4 REQUISITOS A CUMPLIR POR LOS AUDITORES INTERNOS

Los requisitos a cumplir por los auditores internos son los siguientes:

Educación, formación y experiencia

- Título Universitario en Ingeniería Informática.
- Curso de Auditor Interno ISO 27001.

- Experiencia profesional mínima de tres años en ejecución de auditorías de Sistemas de Gestión de Seguridad de la Información.
- Experiencia mínima de cinco auditorías de Sistemas de Gestión de Seguridad de la Información en entidades bancarias.

Habilidades

- Actitud ética, imparcial, sincera, honesta y discreta.
- Capacidad para el trabajo en equipo.
- Tener una actitud abierta y estar dispuesto a considerar ideas o puntos de vista alternativos.
- Mostrarse diplomático y hábil en las relaciones con la gente.
- Ser observador, constante y activamente consciente de los entornos físicos y las actividades.
- Ser perspicaz, instintivamente consciente y capaz de entender y adaptarse a las situaciones.
- Ser tenaz, persistente y orientado sobre la consecución de los objetivos.
- Tener poder de decisión, siendo capaz de alcanzar conclusiones oportunas basadas en el razonamiento lógico y el análisis.
- Mostrarse independiente en las actuaciones, relacionándose el mismo tiempo con otros de manera eficaz.

3.2.5 MODELO DE INFORME DE AUDITORÍA

En las siguientes páginas se mostrará el modelo de informe de auditoría interna de la organización.

[LOGO DE LA ORGANIZACIÓN]	**INFORME DE AUDITORÍA INTERNA**	[COD Auditoría]
		[Versión]
		PAG. 1 DE 2

1. DATOS DE LA AUDITORÍA INTERNA	
Auditoría Nº	
Norma de Referencia	
Periodo de Auditoría	
Lugar de la Auditoría	
Equipo Auditor	

2. ALCANCE DE LA AUDITORÍA INTERNA
2.1 EXCLUSIONES REPORTADAS

3. OBJETIVOS DE LA AUDITORÍA INTERNA

4. DEFINICIONES

[LOGO DE LA ORGANIZACIÓN]	**INFORME DE AUDITORÍA INTERNA**	[COD Auditoría]
		[Versión]
		PAG. 2 DE 2

5. FORTALEZAS Y DEBILIDADES	
FORTALEZAS	**DEBILIDADES**

6. RESULTADOS DE LA AUDITORÍA INTERNA

6.1 NO CONFORMIDADES

Se hallaron _____ No Conformidades (NC) durante la auditoría interna. Las No Conformidades se resumen en el siguiente cuadro:

ÁREA/PROCESO	SAC	DESCRIPCIÓN	RESPONSABLE	AUDITOR

6.2 OBSERVACIONES Y OPORTUNIDADES DE MEJORA

Las Observaciones (OBS) y Oportunidades de Mejora (OM) identificadas durante la Auditoría Interna se detallan a continuación:

7. CONCLUSIONES DE LA AUDITORÍA INTERNA

3.3 GESTIÓN DE INDICADORES

En la Tabla 3-1, se detallan los indicadores utilizados para medir la eficacia de los controles de seguridad implantados. Es necesario destacar que no se utilizan indicadores específicos para cada uno de los controles implantados, sino para aquellos más significativos y cuya medida se hace más interesante.

Por otro lado, en la Tabla 3-2, se detallan los indicadores específicos destinados a evaluar el cumplimiento de los objetivos del SGSI. Indicar que algunos de los indicadores de la Tabla 3-1 también son válidos para medir el cumplimiento de los objetivos del SGSI.

Indicador	Fórmula de medición	Valor umbral	Valor objetivo	Control/es respaldado/s
Número de revisiones de la política de seguridad por parte de la Dirección	Revisiones/año	1	2	5.1.2
Número de auditorías realizadas (internas y externas)	Auditorías/año	1	1	6.1.8, 15.3.1
Número de "No conformidades" identificadas en las auditorías	No conformidades/auditoría	Variable	Variable	6.1.8, 15.3.1
Número de cursos y asistentes por curso	- Nº cursos/trienio - Asistentes/curso	1 10	2 15	8.2.2
Número de revisiones de mantenimiento de los sistemas anti-incendio	Revisiones/año	1	3	9.1.4
% de accesos fallidos a las instalaciones físicas	(Accesos fallidos/Accesos totales) * 100	20%	5%	9.1.2
% de dispositivos extraviados respecto del total	(Dispositivos extraviados/Dispositivos inventariados) * 100	10%	1%	9.2.1, 11.3.2, 11.7.1, 15.2.1
% dispositivos reutilizados	(Nº total de equipos - equipos reutilizados/Nº total de equipos - Nº dispositivos retirados + reutilizados) * 100	75%	50%	9.2.6
% documentación de seguridad elaborada respecto a la esperada	(Nº documentos de seguridad/Nº ideal de documentos de seguridad) * 100	75%	100%	10.1.1, 10.8.1
% de cambios fallidos	(Nº de cambios fallidos/Nº total de cambios) * 100	10%	5%	10.1.2, 12.4.1, 12.5.1
% de *rollbacks* aplicados correctamente	(Nº de cambios acertados/Nº total de cambios) * 100	90%	100%	10.1.2, 12.4.1, 12.5.1
% de espacio libre en unidades de disco	(MB libres en disco/MB total disco) * 100	20%	40%	10.3.1
% de memoria disponible en	(MB libres en	20%	50%	10.3.1

servidores	memoria/MB total memoria) * 100			
% de equipos sin antivirus instalado	(Nº equipos sin antivirus/Nº total de equipos) * 100	10%	0%	10.4.1, 10.4.2
Nº de virus detectados en servidores o estaciones de trabajo	Nº de virus/mes	5	0	10.4.1, 10.4.2
% de copias de seguridad fallidas (semanalmente)	(Nº copias fallidas/Nº total de copias) * 100	10%	2%	10.5.1
Nº de soportes retirados	Soportes retirados/año	-	-	10.7.2
Nº de acuerdos de intercambio de datos	-	-	-	10.8.2
% de transacciones económicas fallidas	(Nº de transacciones fallidas/Nº total de transacciones) * 100	1%	0%	10.9.1, 10.9.2
% de sistemas monitorizados respecto del total	(Nº de sistemas monitorizados/Nº total de sistemas) * 100	10%	75%	10.10.2
% de accesos fallidos a las aplicaciones	(Nº accesos fallidos/Nº total accesos) * 100	20%	5%	11.2.1, 11.6.1
Nº de personas con permisos de administrador/root	-	4	1	11.2.2
% de equipos sin asociación a un dominio	(Nº de equipos sin asociación dominio/Nº total equipos) * 100	10%	0%	11.4.3, 11.4.6
% de accesos no autorizados a la red de la organización	(Nº accesos no autorizados a la red/Nº total de accesos) * 100	10%	0%	11.4.6
% de servidores sin política de seguridad en contraseñas	(Nº servidores sin política seguridad/Nº total de servidores) * 100	10%	0%	11.5.1, 11.5.3
Nº de incidentes de seguridad	Incidentes/año	Variable	Variable	13.1.1, 13.2.2
Tiempo de recuperación medio por indisponibilidad	Minutos	20	10	13.1.1, 13.2.2
% de disponibilidad de los sistemas de información	(Nº sistemas disponibles/Nº total sistemas) * 100	95%	100%	13.1.1, 13.2.2
% de problemas (incidencias repetitivas) identificados	(Nº problemas/Nº total incidencias) * 100	5%	1%	13.2.2
% de aplicaciones instaladas por licencia	(Nº aplicaciones instaladas/Nº licencias) * 100	90%	100%	15.1.1, 15.1.2
Nº de clausulas de confidencialidad en contratos, correos y otros documentos	-	-	-	15.1.3, 15.1.4
% de reducción de amenazas actual	% de reducción respecto al año anterior	20%	50%	Todos

Tabla 3-1: Tabla de indicadores para medición de la eficacia de los controles implantados

Indicador	Unidad de medida	Valor umbral	Valor objetivo
Análisis de riesgos realizados en la organización	Nº análisis/año	1/año	2/año
Nivel de madurez del SGSI de la organización	Escala CMM	3 - Definido	4 - Gestionado
Costes debidos a incidentes de seguridad	Euros	3500	2000
Cuestionarios de satisfacción de los clientes	- Muy satisfecho - Satisfecho - Indiferente - Poco satisfecho - Nada satisfecho	Indiferente	Muy satisfecho
Demandas por incumplimiento de normativa referente a seguridad de la información	Demandas/año	5	3

Tabla 3-2: Tabla de indicadores para medición de los objetivos del SGSI

3.4 PROCEDIMIENTO DE REVISIÓN POR LA DIRECCIÓN

3.4.1 INTRODUCCIÓN

La implementación de una política de seguridad sin el apoyo de la Dirección está destinada al fracaso, por ello es imprescindible que la Dirección proporcione medios y apoyo para llevar a cabo cualquier cambio en la cultura de la seguridad.

Es vital que la Dirección de la organización participe en la toma de decisiones relacionada con la seguridad de la información, y que revise de manera periódica los procedimientos y controles implantados para asegurar el buen funcionamiento y la mejora del Sistema de Gestión de Seguridad de la Información (SGSI).

3.4.2 OBJETIVO

El objetivo de este documento es especificar el procedimiento o acciones que debe llevar a cabo la Dirección para realizar la revisión del SGSI. Esta revisión pretende garantizar que el SGSI implantado es apropiado para los requisitos de negocio de la organización y además, demostrar su eficacia.

3.4.3 ALCANCE

Este procedimiento concernirá al SGSI en su conjunto, ya que se trata de una revisión global de los aspectos que son de interés para evaluar el funcionamiento del mismo.

3.4.4 ENTRADAS

Este proceso se inicia con la convocatoria de una revisión por parte de la Dirección, efectuada cuando la organización lo estime oportuno.

Como entradas a este proceso es recomendable utilizar:

- Los resultados de las auditorías y revisiones previas del SGSI.
- El estado de las acciones preventivas o correctivas.
- Las vulnerabilidades o amenazas no abordadas adecuadamente en la evaluación de riesgos previa.
- Los resultados de las mediciones de la eficacia.
- Las acciones de seguimiento de las revisiones anteriores.
- Las recomendaciones de mejora.

3.4.5 SALIDAS

El resultado de este proceso es la evaluación del funcionamiento del SGSI, para asegurar su conveniencia, adecuación y eficacia continuas.

Además, se concretan decisiones y acciones destinadas a:

- La mejora de la eficacia del SGSI.
- La actualización de la evaluación de riesgos y el plan de tratamiento de riesgos.
- La modificación de los procedimientos y controles que afectan a la seguridad de la información.
- Las necesidades de recursos.
- La mejora en el modo de medir la eficacia de los controles.

3.4.6 PROCEDIMIENTO

Las acciones llevadas a cabo por la Dirección para realizar la revisión del SGSI son las siguientes:

- La Dirección realizará, como máximo anualmente, revisiones del cumplimiento de todos los estándares, normas y procedimientos establecidos en el SGSI.
- La Dirección comprobará que el personal que accede a los sistemas de información de la organización conoce las normas de seguridad.
- La Dirección revisará y evaluará los registros de usuario, incidencias de seguridad, inventario de activos, etc.
- El Jefe de Departamento de TI realizará un informe sobre la revisión realizada anualmente. En éste se incluirán las incidencias y deficiencias detectadas y una relación de soluciones y propuestas de mejora.
- Se revisará que se mantiene actualizada la documentación del SGSI, utilizando para ello los resultados de los últimos informes de auditoría, las incidencias y las revisiones internas.
- La Dirección se encargará de revisar el resultado de las auditorías internas anuales y de hacer un seguimiento de las acciones correctivas (al menos semestralmente). Se actuará de la misma manera con las auditorías externas con una frecuencia de tres años, haciendo un seguimiento de las acciones al menos de forma anual.
- De forma puntual se solicitará (al menos una vez al año) un resumen de los indicadores de seguridad y se analizarán en el comité de seguridad.

3.5 GESTIÓN DE ROLES Y RESPONSABILIDADES

3.5.1 COMITÉ DE SEGURIDAD

El comité de seguridad de la organización está formado por las siguientes personas:

- Director General.
- Jefe de Departamento de TI.
- Los tres responsables de seguridad.

Y sus funciones serán las siguientes:

- Implantar los planes promovidos desde Dirección.
- Asignar roles y funciones en materia de seguridad.
- Presentar la aprobación de políticas, normas y responsabilidades en materia de seguridad.
- Validar el mapa de riesgos y sus acciones.
- Validar el plan director de seguridad.

- Supervisar el plan de continuidad de negocio.
- Velar por el cumplimiento de la legislación vigente en materia de seguridad.
- Promover la formación y cultura de la seguridad.
- Aprobar y revisar periódicamente el SGSI.

3.5.2 FUNCIONES Y OBLIGACIONES DEL PERSONAL

Los distintos empleados de la organización solo desarrollarán las funciones para las que han sido autorizados en los sistemas de información. Para asegurarlo, existen implantadas medidas organizativas y técnicas que permiten controlar sus accesos.

El personal, tanto interno como externo, que tenga relación con los sistemas de información de la organización, está obligado a respetar las normas, definidas en la política de seguridad de la organización. Aparte de las normas definidas en dicha política, y de las funciones y responsabilidades que tenga asignadas cada usuario, éstos deben respetar las siguientes normas de carácter general:

- Confidencialidad, respecto a la información y documentación de la organización que reciben o usan.
- No ceder datos de carácter personal ni usarlos con una finalidad distinta por la que han sido recogidos.
- Comunicar al responsable de seguridad cualquier incidencia respecto a la seguridad de la información.

Personal con acceso privilegiado y personal técnico

El personal técnico de la organización está compuesto de seis personas, concretamente un administrador de sistemas, tres operadores y dos técnicos de mantenimiento de sistemas y aplicaciones. A continuación, describimos las funciones y privilegios asignados a cada uno de ellos:

- Administrador de sistemas: Será el responsable de los máximos privilegios, y por tanto, su responsabilidad es mayor que la del resto, ya que una actuación errónea o incorrecta puede afectar a los sistemas. Tendrá acceso a todos los sistemas necesarios para desarrollar su función y resolver los problemas que surjan.
- Operadores: Sus actuaciones están más limitadas dentro de los sistemas de información y están supervisadas por el administrador de sistemas. No tienen acceso a los ficheros que contienen datos personales salvo que la situación lo requiera.
- Técnicos de mantenimiento de sistemas y aplicaciones: Son los responsables de la resolución de incidencias en sistemas hardware y

software. No tienen acceso a los datos de los sistemas de información salvo que la situación lo requiera.

Para este personal también serán de aplicación las normas y obligaciones establecidas para todo el personal con perfil de usuario. Algunas de las funciones y responsabilidades exclusivas del personal técnico y con acceso privilegiado son:

- Promover la incorporación de mecanismos de integridad, autentificación, control de acceso y auditoría en el diseño, implantación y operación de los sistemas de información.
- Asegurar la confidencialidad y disponibilidad de la información almacenada en los sistemas de información, así como su salvaguarda mediante copias de seguridad periódicas.
- Conceder a los usuarios los privilegios mínimos que les permitan acceder a los datos y recursos necesarios para el desarrollo de sus tareas.
- No acceder a datos aprovechando su privilegio sin autorización del jefe de Departamento de TI o el responsable de seguridad.
- Custodiar con especial cuidado los identificadores y contraseñas que dan acceso a los sistemas con privilegios de administrador.
- Notificar las incidencias oportunas ante cualquier violación de las normas de seguridad o vulnerabilidades detectadas en los sistemas.
- No revelar a terceros ninguna posible debilidad en materia de seguridad de los sistemas sin previa autorización del jefe del Departamento de TI o del responsable de seguridad.

Personal con perfil de usuario

Los usuarios con acceso a los sistemas de información solo podrán acceder a la información necesaria para el desempeño de sus funciones. Las obligaciones en materia de seguridad con las que deberán cumplir este personal son las siguientes:

- Mantener en secreto la información a la que se tiene acceso, incluso aún después de haber finalizado la relación con la organización.
- Conocer y cumplir la política de seguridad de la información y prestar especial atención a la normativa referida a la protección de datos de carácter personal.
- Respetar los procedimientos, mecanismos y dispositivos de seguridad, evitando cualquier intento de acceso no autorizado.
- Responsabilizarse con los mecanismos y controles de identificación y autenticación ante los sistemas de información, especialmente en lo referente a la elección de contraseñas de usuario seguras.
- Utilizar de manera responsable las contraseñas de acceso a los sistemas de información, y salvaguardarlas de manera que se evite que caigan en manos de personal no autorizado.
- Si un usuario tiene sospechas de que sus credenciales de acceso (identificador de usuario y contraseña) han sido comprometidas o están

siendo utilizadas por otra persona, debe proceder al cambio inmediato de contraseña y comunicar la correspondiente incidencia de seguridad.

- Proteger especialmente la información de la organización que por diversos motivos tenga que moverse fuera de la misma.
- Bloquear el acceso a ordenadores u otros dispositivos cuando se encuentre ausente de su puesto de trabajo.
- Notificar al responsable de seguridad cualquier incidencia que detecten que afecte a los datos de los sistemas de información (pérdida de información, acceso no autorizado, etc.).
- Entregar cuando sea requerido por la organización, y especialmente cuando cause baja en la empresa, las llaves, claves, tarjetas de identificación, material, documentación, equipos o dispositivos y cuantos activos sean propiedad de la misma.

Funciones y obligaciones del responsable de seguridad

El responsable de seguridad es la persona con máximo poder de decisión y responsabilidad en materia de seguridad de la información en la organización solo por debajo del jefe del Departamento de TI. En la mayoría de las situaciones será el máximo responsable al efecto, ya que el jefe del Departamento de TI ejerce una figura más corporativa. Las principales funciones de los responsables de seguridad son las siguientes:

- Asesorar en la definición de requisitos sobre las medidas de seguridad que se deben adoptar.
- Validar la implantación de los requisitos de seguridad necesarios.
- Revisar periódicamente los sistemas de información y elaborar un informe de las revisiones realizadas y los problemas detectados.
- Mantener actualizadas las normas y procedimientos en materia de seguridad de la información.
- Definir y comprobar la aplicación del procedimiento de copias de respaldo y recuperación de datos.
- Definir y comprobar la aplicación del procedimiento de notificación y gestión de incidencias.
- Controlar que las auditorías de seguridad se realicen con la frecuencia necesaria.
- Analizar los informes de auditoría y si lo considera necesario modificar las medidas correctoras para prevenir incidentes.
- Trasladar los informes de auditoría a la Dirección (Director General, jefe del Departamento de TI).
- Establecer los controles y medidas técnicas y organizativas para asegurar los sistemas de información.
- Gestionar y analizar las incidencias de seguridad que tienen lugar en la organización.

- Coordinar la puesta en marcha de las medidas de seguridad y colaborar en el cumplimiento y difusión de la política de seguridad.

3.6 METODOLOGÍA DE ANÁLISIS DE RIESGOS

La metodología que se utilizará para realizar el análisis de riesgos de la organización está basada en MAGERIT [9], ya que es la metodología recomendada por la Administración Pública española y muy extendida en el ámbito español.

Las fases que se seguirán, salvo pequeñas modificaciones, son las fases recomendadas por la metodología MAGERIT para el análisis de riesgos en una organización, y son las que se describen a continuación.

Fase 1: Identificación, clasificación y valoración de activos

En esta primera fase, se identificarán cuáles son los activos de la organización relevantes para sus procesos de negocio, y se clasificarán de acuerdo a las siguientes categorías:

- Datos (D): Activos de información de la organización.
- Comunicación (COM): Activos destinados a transportar los datos de un sitio a otro, por ejemplo, la red ADSL, red WiFi, red LAN, etc.
- Hardware (HW): Activos materiales, físicos, que actúan como depositarios temporales o permanentes de los datos, soportes de ejecución de las aplicaciones informáticas o responsables del procesado o la transmisión de los datos. Por ejemplo, soportes de almacenamiento, equipos informáticos, routers, etc.
- Software (SW): Comprende los activos en forma de aplicaciones informáticas que gestionan, analizan y transforman los datos permitiendo la explotación de la información para la prestación de los servicios. Por ejemplo, sistema de gestión de bases de datos, sistema operativo, anti virus, etc.
- Servicio (S): Esta sección contempla servicios prestados por el sistema. Por ejemplo, correo electrónico, transferencia de ficheros, infraestructura de clave pública, etc.
- Personal (P): Comprende los activos humanos de la organización: empleados, responsable de seguridad, etc.
- Instalaciones (L): Comprende los lugares donde se hospedan los sistemas de información. Por ejemplo, edificios, instalaciones de respaldo, etc.

Una vez clasificados los activos, será necesario valorarlos. Esta valoración se llevará a cabo en función de la criticidad del activo para los procesos de negocio de la organización, de acuerdo a los valores establecidos en la Tabla 3-3.

Valor	Descripción	Valor numérico
Muy Alto (MA)	Parada total de todos los servicios o de un servicio esencial de la organización. Parada total de la actividad empresarial. Afecta a la imagen de la organización. Causa un daño económico muy elevado.	5
Alto (A)	Parada de un servicio no esencial de la organización. Parada parcial de la actividad empresarial. Causa un daño económico elevado.	4
Medio (M)	Parada de un departamento o equipo de trabajo. Causa daños económicos apreciables.	3
Bajo (B)	Parada de un puesto de trabajo. No causa daños económicos apreciables.	2
Muy Bajo (MB)	No causa parada de ningún puesto de trabajo. No causa ningún tipo de daño económico.	1

Tabla 3-3: Tabla de valoración de activos

Fase 2: Identificación de las amenazas

En esta fase, deben identificarse las amenazas que pueden causar un daño sobre los activos de la organización. En este caso, las amenazas que contemplaremos son las que se proponen en MAGERIT [9]. MAGERIT, además, distingue dichas amenazas según su origen (por ejemplo, se distingue entre si la amenaza "fuego" ha sido provocada por un desastre natural o por un desastre industrial), pero en esta metodología no se tendrá en cuenta dicha distinción, sino que se tratarán las amenazas independientemente de su origen.

Una vez identificadas las amenazas, es necesario saber a qué tipo o tipos de activos afectará cada una de ellas. Esta correspondencia también nos la proporciona MAGERIT, por lo que seguiremos sus recomendaciones. También es importante saber a qué dimensión o dimensiones de la seguridad (confidencialidad, disponibilidad e integridad) afectará cada una de las amenazas. MAGERIT también nos proporciona esa información.

Por último, se debe establecer la probabilidad de ocurrencia de cada una de las amenazas. Para ello, se utilizará la escala proporcionada en la Tabla 3-4.

Probabilidad	Valor numérico
Muy Alta (MA)	5
Alta (A)	4
Media (M)	3
Baja (B)	2
Muy Baja (MB)	1

Tabla 3-4: Escala de probabilidad de ocurrencia de las amenazas

Fase 3: Cuantificación del impacto

Se denomina impacto a la medida del daño sobre el activo derivado de la materialización de una amenaza. Conociendo el valor de los activos y la degradación que causan las amenazas, es directo derivar el impacto que estas tendrían sobre el sistema. Para cada uno de los activos, habrá que cuantificar el impacto que tendrá sobre

el mismo la materialización de una amenaza. Esta cuantificación se hará en función de la escala que se muestra en la Tabla 3-5.

Impacto	Valor (en %)
Muy Alto (MA)	100%
Alto (A)	75%
Medio (M)	50%
Bajo (B)	20%
Muy Bajo (MB)	5%

Tabla 3-5: Escala de cuantificación del impacto

Fase 4: Cálculo del riesgo potencial

Una vez identificados y valorados los activos, establecida la probabilidad de ocurrencia de las amenazas, y determinado el impacto que tendrán sobre los activos la materialización de las amenazas, es posible calcular el riesgo potencial. El riesgo potencial, será a grandes rasgos, el riesgo al que estarán sometidos los activos de la organización antes de la implantación de controles o salvaguardas.

Para cada pareja activo-amenaza, se calculará el riesgo al que está sometido el activo en cada una de las tres dimensiones de la seguridad, confidencialidad, disponibilidad e integridad, siguiendo las siguientes fórmulas:

$$RP_C = Valor\ Activo\ x\ Probabilidad\ Amenaza\ x\ Impacto_{Confidencialidad}$$

$$RP_I = Valor\ Activo\ x\ Probabilidad\ Amenaza\ x\ Impacto_{Integridad}$$

$$RP_D = Valor\ Activo\ x\ Probabilidad\ Amenaza\ x\ Impacto_{Disponibilidad}$$

Una vez calculados los valores del riesgo potencial para los activos, se debe establecer el nivel de riesgo aceptable. Este nivel debe consensuarse y definirse dependiendo de la criticidad del activo en la organización.

Fase 5: Aplicación de controles o salvaguardas

Una vez conocidos los valores para el riesgo potencial de cada uno de los activos se procederá a la aplicación de controles o salvaguardas sobre las amenazas para reducir o mitigar dichos riesgos.

Los controles a aplicar serán los recogidos en la norma ISO/IEC 27002:2005 [3], de manera que se reduzca la probabilidad de ocurrencia de las amenazas y el daño que la materialización de éstas producen sobre los activos (impacto).

Fase 6: Cálculo del riesgo residual

Tras la aplicación de las salvaguardas, es el momento de calcular el riesgo residual. El riesgo residual es el riesgo al que siguen sometidos los activos de la organización después de la aplicación de las salvaguardas, y que evidentemente, será

menor que el riesgo potencial para aquellas amenazas sobre las que se hayan aplicado controles.

Para el cálculo del riesgo residual se seguirá la misma estrategia que para el cálculo del riesgo potencial, con la diferencia de que ahora la probabilidad de ocurrencia de la amenaza y el porcentaje de impacto habrán disminuido. La probabilidad de ocurrencia de la amenaza resultante y el porcentaje de impacto resultante se denominarán $Probabilidad\ Amenaza_{Residual}$ e $Impacto_{Residual}$, respectivamente. Por tanto, las fórmulas quedan de la siguiente manera:

$$RR_C = Valor\ Activo\ x\ Probabilidad\ Amenaza_{Residual}\ x\ Impacto_{Confidencialidad\ Residual}$$

$$RR_I = Valor\ Activo\ x\ Probabilidad\ Amenaza_{Residual}\ x\ Impacto_{Integridad\ Residual}$$

$$RR_D = Valor\ Activo\ x\ Probabilidad\ Amenaza_{Residual}\ x\ Impacto_{Disponibilidad\ Residual}$$

Fase 7: Gestión de riesgos

Una vez conocidos los valores de riesgo residual para los activos de la organización hay que decidir qué hacer con dicho riesgo, es decir, hay que gestionar el riesgo. Se debe decidir qué medidas de seguridad aplicar en la organización y, para ello, se debe tener presente el umbral de riesgo aceptable y el coste de la aplicación de las medidas de seguridad. A la hora de gestionar el riesgo existen tres estrategias: mitigarlo, transferirlo e ignorarlo. La organización debe valorar y adoptar la que más le interese.

3.7 DECLARACIÓN DE APLICABILIDAD

A continuación, en la Tabla 3-6, se detalla la declaración de aplicabilidad de los controles de seguridad establecidos en la organización.

Nº	Control	Aplica	Estado actual	Justificación
5.1.1	Documento de política de seguridad de la información	SI	1 - Inicial	La Dirección debe aprobar un documento de política de seguridad de la información, publicarlo y distribuirlo a todos los empleados y terceros afectados.
5.1.2	Revisión de la política de seguridad de la información	SI	1- Inicial	La política de seguridad de la información debe revisarse a intervalos planificados o siempre que se produzcan cambios significativos, a fin de asegurar que se mantenga

				su idoneidad, adecuación y eficacia.
6.1.1	Compromiso de la Dirección con la seguridad de la información	SI	0 - Inexistente	La Dirección debe prestar un apoyo activo a la seguridad dentro de la organización a través de directrices claras, un compromiso demostrado, asignaciones explícitas y el reconocimiento de las responsabilidades de seguridad de la información.
6.1.2	Coordinación de la seguridad de la información	SI	2 - Repetible	Las actividades relativas a la seguridad de la información deben ser coordinadas entre los representantes de las diferentes partes de la organización con sus correspondientes roles y funciones de trabajo.
6.1.3	Asignación de responsabilidades relativas a la seguridad de la información	SI	1 - Inicial	Deben definirse claramente todas las responsabilidades relativas a la seguridad de la información.
6.1.4	Proceso de autorización de recursos para el tratamiento de la información	SI	1 - Inicial	Por cada nuevo recurso de tratamiento de la información, debe definirse e implantarse un proceso de autorización por parte de la Dirección.
6.1.5	Acuerdos de confidencialidad	SI	2 - Repetible	Debe determinarse y revisarse periódicamente la necesidad de establecer acuerdos de confidencialidad o no revelación, que reflejen las necesidades de la organización para la protección de la información.
6.1.6	Contacto con las autoridades	SI	2 - Repetible	Deben mantenerse los contactos adecuados con las autoridades competentes.
6.1.7	Contacto con grupos de especial interés	SI	1 - Inicial	Deben mantenerse los contactos adecuados con grupos de interés especial, u otros foros, y asociaciones profesionales especializadas en seguridad.
6.1.8	Revisión independiente de la seguridad de la	SI	1 - Inicial	El enfoque de la organización para la gestión

	información			de la seguridad de la información y su implantación (es decir, los objetivos de control, los controles, las políticas, los procesos y los procedimientos para la seguridad de la información), debe someterse a una revisión independiente a intervalos planificados o siempre que se produzcan cambios significativos en la implantación de la seguridad.
6.2.1	Identificación de los riesgos derivados del acceso de terceros	SI	2 - Repetible	Debe identificarse los riesgos para la información y para los dispositivos de tratamiento de la información de la organización derivados de los procesos de negocio que requieran de terceros, e implantar los controles apropiados antes de otorgar el acceso.
6.2.2	Tratamiento de la seguridad en la relación con los clientes	SI	2 - Repetible	Deben tratarse todos los requisitos de seguridad identificados, antes de otorgar acceso a los clientes a los activos o a la información de la organización.
6.2.3	Tratamiento de seguridad en los contratos con terceros	SI	3 - Definido	Los acuerdos con terceros que conlleven acceso, procesado, comunicación o gestión, bien de la información de la organización, o de los recursos de tratamiento de la información, o bien la incorporación de productos o servicios a los recursos de tratamiento de la información, deben cubrir todos los requisitos de seguridad pertinentes.
7.1.1	Inventario de activos	SI	3 - Definido	Todos los activos deben estar claramente identificados y debe elaborarse y mantenerse un inventario de todos los activos importantes.

7.1.2	Propiedad de los activos	SI	3 - Definido	Toda la información y activos asociados con los recursos para el tratamiento de la información deben tener un propietario que forme parte de la organización y haya sido designado como propietario.
7.1.3	Uso aceptable de los activos	SI	3 - Definido	Se deben identificar, documentar e implantar las reglas para el uso aceptable de la información y de los activos asociados con los recursos para el tratamiento de la información.
7.2.1	Directrices de clasificación	SI	3 - Definido	La información debe ser clasificada según su valor, los requisitos legales, su sensibilidad y criticidad para la organización.
7.2.2	Etiquetado y manipulado de la información	SI	3 - Definido	Se debe desarrollar e implantar un conjunto adecuado de procedimientos para etiquetar y manejar la información, de acuerdo con el esquema de clasificación adoptado por la organización.
8.1.1	Funciones y responsabilidades	SI	4 - Gestionado	Las funciones y responsabilidades de seguridad de los empleados, contratistas y terceros se deben definir y documentar de acuerdo con la política de seguridad de la información de la organización.
8.1.2	Investigación de antecedentes	SI	4 - Gestionado	Se deben comprobar los antecedentes de todos los candidatos a un puesto de trabajo, de los contratistas o de los terceros.
8.1.3	Términos y condiciones de contratación	SI	4 - Gestionado	Como parte de sus obligaciones contractuales, los empleados, los contratistas y los terceros deben aceptar y firmar los términos y condiciones de su contrato de trabajo, que debe establecer sus responsabilidades y las de

				la organización en lo relativo a seguridad de la información.
8.2.1	Responsabilidades de la Dirección	SI	1 - Inicial	La Dirección debe exigir a los empleados, contratistas y terceros, que apliquen la seguridad de acuerdo con las políticas y procedimientos establecidos en la organización.
8.2.2	Concienciación, formación y capacitación en seguridad de la información	SI	1 - Inicial	Todos los empleados de la organización y, cuando corresponda, los contratistas y terceros, deben recibir una adecuada concienciación y formación, con actualizaciones periódicas, sobre las políticas y procedimientos de la organización, según corresponda con su puesto de trabajo.
8.2.3	Proceso disciplinario	SI	0 - Inexistente	Debe existir un proceso disciplinario formal para los empleados que hayan provocado alguna violación de seguridad.
8.3.1	Responsabilidad del cese o cambio	SI	4 - Gestionado	Las responsabilidades para proceder al cese en el empleo o al cambio de puesto de trabajo deben estar claramente definidas y asignadas.
8.3.2	Devolución de activos	SI	4 - Gestionado	Todos los empleados, contratistas y terceros deben devolver todos los activos de la organización que estén en su poder al finalizar su empleo, contrato o acuerdo.
8.3.3	Retirada de los derechos de acceso	SI	4 - Gestionado	Los derechos de acceso a la información y a los recursos de tratamiento de la información de todos los empleados, contratistas y terceros deben ser retirados a la finalización del empleo, del contrato o del acuerdo, o bien deben ser adaptados a los cambios producidos.
9.1.1	Perímetro de seguridad física	SI	5 - Optimizado	Se deben utilizar perímetros de seguridad para proteger

				las áreas que contienen la información y los recursos de tratamiento de la información.
9.1.2	Controles físicos de entrada	SI	5 - Optimizado	Las áreas seguras deben estar protegidas por controles de entrada adecuados, para asegurar que únicamente se permite el acceso al personal autorizado.
9.1.3	Seguridad de oficinas, despachos e instalaciones	SI	4 - Gestionado	Se deben diseñar y aplicar las medidas de seguridad físicas para las oficinas, despachos e instalaciones.
9.1.4	Protección contra las amenazas externas y de origen ambiental	SI	3 - Definido	Se debe diseñar y aplicar una protección física contra el daño causado por fuego, inundación, terremoto, explosión, revueltas sociales y otras formas de desastres naturales o provocados por el hombre.
9.1.5	Trabajo en áreas seguras	SI	4 - Gestionado	Se debe diseñar e implantar una protección física y una serie de directrices para trabajar en las áreas seguras.
9.1.6	Áreas de acceso público y de carga y descarga	SI	4 - Gestionado	Debe controlarse los puntos de acceso tales como las áreas de carga y descarga y otros puntos, a través de los que personal no autorizado pueda acceder a las instalaciones, y si es posible, dichos puntos se deben aislar de las instalaciones de tratamiento de la información para evitar accesos no autorizados.
9.2.1	Emplazamiento y protección de equipos	SI	3 - Definido	Los equipos deben situarse o protegerse de forma que se reduzcan los riesgos derivados de las amenazas y peligros de origen ambiental así como las ocasiones de que se produzcan accesos no autorizados.
9.2.2	Instalaciones de suministro	SI	3 - Definido	Los equipos deben estar protegidos contra fallos de alimentación y otras anomalías causadas por

				fallos en las instalaciones de suministro.
9.2.3	Seguridad del cableado	SI	5 - Optimizado	El cableado eléctrico y de telecomunicaciones que transmite datos o que da soporte a los servicios de información debe estar protegido frente a interceptaciones o daños.
9.2.4	Mantenimiento de los equipos	SI	4 - Gestionado	Los equipos deben recibir un mantenimiento correcto que asegure su disponibilidad y su integridad.
9.2.5	Seguridad de los equipos fuera de las instalaciones	SI	1 - Inicial	Teniendo en cuenta los diferentes riesgos que conlleva trabajar fuera de las instalaciones de la organización, deben aplicarse medidas de seguridad a los equipos situados fuera de dichas instalaciones.
9.2.6	Reutilización o retirada segura de equipos	SI	1 - Inicial	Todos los soportes de almacenamiento deben ser comprobados para confirmar que todo dato sensible y todas las licencias de software se han eliminado o bien se han borrado o sobreescrito de manera segura, antes de su retirada.
9.2.7	Retirada de materiales propiedad de la empresa	SI	1 - Inicial	Los equipos, la información o el software no deben sacarse de las instalaciones, sin autorización previa.
10.1.1	Documentación de los procedimientos de operación	SI	3 - Definido	Deben documentarse y mantenerse los procedimientos de operación y ponerse a disposición de todos los usuarios que los necesiten.
10.1.2	Gestión de cambios	SI	3 - Definido	Deben controlarse los cambios en los recursos y en los sistemas de tratamiento de la información.
10.1.3	Segregación de tareas	SI	4 - Gestionado	Las tareas y áreas de responsabilidad deben segregarse para reducir la posibilidad de que se produzcan modificaciones

				no autorizadas o no intencionadas o usos indebidos de los activos de la organización.
10.1.4	Separación de los recursos de desarrollo, prueba y operación	SI	3 - Definido	Deben separarse los recursos de desarrollo, de pruebas y de operación, para reducir los riesgos de acceso no autorizado o los cambios en el sistema en producción.
10.2.1	Provisión de servicios	SI	3 - Definido	Se debe comprobar que los controles de seguridad, las definiciones de los servicios y los niveles de provisión, incluidos en el acuerdo de provisión de servicios por terceros, han sido implantados, puestos en operación y son mantenidos por parte de un tercero.
10.2.2	Supervisión y revisión de los servicios prestados por terceros	SI	3 - Definido	Los servicios, informes y registros proporcionados por un tercero deben ser objeto de supervisión y revisión periódicas, y también deberían llevarse a cabo auditorías periódicas.
10.2.3	Gestión del cambio en los servicios prestados por terceros	SI	3 - Definido	Se deben gestionar los cambios en la provisión de los servicios, incluyendo el mantenimiento y la mejora de las políticas, los procedimientos y los controles de seguridad de la información existentes, teniendo en cuenta la criticidad de los procesos y sistemas de negocio afectados así como la reevaluación de los riesgos.
10.3.1	Gestión de capacidades	SI	4 - Gestionado	La utilización de los recursos se debe supervisar y ajustar así como realizar proyecciones de los requisitos futuros de capacidad, para garantizar el rendimiento requerido del sistema.
10.3.2	Aceptación del sistema	SI	4 - Gestionado	Se deben establecer los criterios para la aceptación de nuevos sistemas de información, de las actualizaciones y de nuevas versiones de los mismos, y

				se deben llevar a cabo pruebas adecuadas de los sistemas durante el desarrollo y previamente a la aceptación.
10.4.1	Controles contra el código malicioso	SI	4 - Gestionado	Se deben implantar controles de detección, prevención y recuperación que sirvan como protección contra el código malicioso y se deben implantar procedimientos adecuados de concienciación del usuario.
10.4.2	Controles contra el código descargado en el cliente	SI	3 - Definido	Cuando se autorice el uso de código descargado en el cliente, la configuración debe garantizar que dicho código autorizado funciona de acuerdo con una política de seguridad claramente definida, y se debe evitar que se ejecute el código no autorizado.
10.5.1	Copias de seguridad de la información	SI	4 - Gestionado	Se deben realizar copias de seguridad de la información y del software, y se deben probar periódicamente conforme a la política de copias de seguridad acordada.
10.6.1	Controles de red	SI	5 - Optimizado	Las redes deben estar adecuadamente gestionadas y controladas, para que estén protegidas frente a posibles amenazas y para mantener la seguridad de los sistemas y de las aplicaciones que utilizan estas redes, incluyendo la información en tránsito.
10.6.2	Seguridad de los servicios de red	SI	4 - Gestionado	Se deben identificar las características de seguridad, los niveles de servicio, y los requisitos de gestión de todos los servicios de red y se deberían incluir en todos los acuerdos relativos a servicios de red, tanto si estos servicios se prestan dentro de la organización como si se subcontratan.
10.7.1	Gestión de soportes extraíbles	SI	1 - Inicial	Se deben establecer procedimientos para la gestión de los soportes

				extraíbles.
10.7.2	Retirada de soportes	SI	2 - Repetible	Los soportes deberían ser retirados de forma segura cuando ya no vayan a ser necesarios, mediante los procedimientos formales establecidos.
10.7.3	Procedimientos de manipulación de la información	SI	3 - Definido	Deben establecerse procedimientos para la manipulación y el almacenamiento de la información, de modo que se proteja dicha información contra la revelación no autorizada o el uso indebido.
10.7.4	Seguridad de la documentación del sistema	SI	3 - Definido	La documentación del sistema debe estar protegida contra accesos no autorizados.
10.8.1	Políticas y procedimientos de intercambio de información	SI	4 - Gestionado	Deben establecerse políticas, procedimientos y controles formales que protejan el intercambio de información mediante el uso de todo tipo de recursos de comunicación.
10.8.2	Acuerdos de intercambio	SI	3 - Definido	Deben establecerse acuerdos para el intercambio de información y de software entre la organización y los terceros.
10.8.3	Soportes físicos en tránsito	SI	3 - Definido	Durante el transporte fuera de los límites físicos de la organización, los soportes que contengan información deben estar protegidos contra accesos no autorizados, usos indebidos o deterioro.
10.8.4	Mensajería electrónica	SI	4 - Gestionado	La información que sea objeto de mensajería electrónica debe estar adecuadamente protegida.
10.8.5	Sistemas de información empresariales	SI	4 - Gestionado	Deben formularse e implantarse políticas y procedimientos para proteger la información asociada a la interconexión de los sistemas de información empresariales.
10.9.1	Comercio electrónico	SI	5 - Optimizado	La información incluida en el comercio electrónico que se transmita a través de

				redes públicas debe protegerse contra las actividades fraudulentas, las disputas contractuales, y la revelación o modificación no autorizada de dicha información.
10.9.2	Transacciones en línea	SI	5 - Optimizado	La información contenida en las transacciones en línea debe estar protegida para evitar transmisiones incompletas, errores de direccionamiento, alteraciones no autorizadas de los mensajes, la revelación, la duplicación o la reproducción no autorizadas del mensaje.
10.9.3	Información públicamente disponible	SI	4 - Gestionado	La integridad de la información puesta a disposición pública se debe proteger para evitar modificaciones no autorizadas.
10.10.1	Registros de auditoría	SI	2 - Repetible	Se deben generar registros de auditoría de las actividades de los usuarios, las excepciones y eventos de seguridad de la información, y se deberían mantener estos registros durante un periodo acordado para servir como prueba en investigaciones futuras y en la supervisión del control de acceso.
10.10.2	Supervisión del uso del sistema	SI	3 - Definido	Se deben establecer procedimientos para supervisar el uso de los recursos de tratamiento de la información y se deben revisar periódicamente los resultados de las actividades de supervisión.
10.10.3	Protección de la información de los registros	SI	4 - Gestionado	Los dispositivos de registro y la información de los registros deben estar protegidos contra manipulaciones indebidas y accesos no autorizados.
10.10.4	Registros de administración y operación	SI	2 - Repetible	Se deben registrar las actividades del administrador y del operador del sistema.

10.10.5	Registro de fallos	SI	3 - Definido	Los fallos deben ser registrados y analizados y se deberían tomar las correspondientes acciones.
10.10.6	Sincronización del reloj	SI	5 - Optimizado	Los relojes de todos los sistemas de tratamiento de la información dentro de una organización o de un dominio de seguridad, deben estar sincronizados con una única fuente precisa y acordada de tiempo.
11.1.1	Política de control de acceso	SI	4 - Gestionado	Se debe establecer, documentar y revisar una política de control de acceso basada en los requisitos del negocio y de seguridad para el acceso.
11.2.1	Registros de usuario	SI	5 - Optimizado	Debe establecerse un procedimiento formal de registro y de anulación de usuarios para conceder y revocar el acceso a todos los sistemas y servicios de información.
11.2.2	Gestión de privilegios	SI	4 - Gestionado	La asignación y el uso de privilegios deben estar restringidos y controlados.
11.2.3	Gestión de contraseñas de usuario	SI	4 - Gestionado	La asignación de contraseñas debe ser controlada a través de un proceso de gestión formal.
11.2.4	Revisión de los derechos de acceso de usuario	SI	0 - Inexistente	La Dirección debe revisar los derechos de acceso de usuario a intervalos regulares y utilizando un proceso formal.
11.3.1	Uso de contraseñas	SI	3 - Definido	Se debe requerir a los usuarios el seguir las buenas prácticas de seguridad en la selección y el uso de contraseñas.
11.3.2	Equipo de usuario desatendido	SI	3 - Definido	Los usuarios deben asegurarse de que el equipo desatendido tiene la protección adecuada.
11.3.3	Política de puesto de trabajo despejado y pantalla limpia	SI	1 - Inicial	Debe adoptarse una política de puesto de trabajo despejado de papeles y soportes de almacenamiento extraíbles junto con una política de

				pantalla limpia para los recursos de tratamiento de la información.
11.4.1	Política de uso de los servicios en red	SI	3 - Definido	Se debe proporcionar a los usuarios únicamente el acceso a los servicios para que los que hayan sido específicamente autorizados.
11.4.2	Autenticación de usuario para conexiones externas	SI	4 - Gestionado	Se deben utilizar los métodos apropiados de autenticación para controlar el acceso de los usuarios remotos.
11.4.3	Identificación de los equipos en las redes	SI	4 - Gestionado	La identificación automática de los equipos se debe considerar como un medio de autenticación de las conexiones provenientes de localizaciones y equipos específicos.
11.4.4	Diagnóstico remoto y protección de los puertos de configuración	SI	5 - Optimizado	Se debe controlar el acceso físico y lógico a los puertos de diagnóstico y de configuración.
11.4.5	Segregación de las redes	SI	5 - Optimizado	Los grupos de servicios de información, usuarios y sistemas de información deben estar segregados en redes.
11.4.6	Control de la conexión a la red	SI	4 - Gestionado	En redes compartidas, especialmente en aquellas que traspasen las fronteras de la organización, debe restringirse la capacidad de los usuarios para conectarse a la red, esto debe hacerse de acuerdo a la política de control de acceso y a los requisitos de las aplicaciones empresariales.
11.4.7	Control de encaminamiento (*routing*) de red	SI	4 - Gestionado	Se deben implantar controles de encaminamiento (*routing*) de redes para asegurar que las conexiones de los ordenadores y los flujos de información no violan la política de control de acceso de las aplicaciones empresariales.
11.5.1	Procedimientos seguros de inicio de sesión	SI	4 - Gestionado	El acceso a los sistemas operativos se debe controlar por medio de un

				procedimiento seguro de inicio de sesión.
11.5.2	Identificación y autenticación de usuario	SI	3 - Definido	Todos los usuarios deben tener un identificador único (ID de usuario), para su uso personal y exclusivo, y se debe elegir una técnica adecuada de autenticación para confirmar la identidad solicitada al usuario.
11.5.3	Sistema de gestión de contraseñas	SI	5 - Optimizado	Los sistemas para la gestión de contraseñas deben ser interactivos y establecer contraseñas de calidad.
11.5.4	Uso de los recursos del sistema	SI	3 - Definido	Se debe restringir y controlar de una manera rigurosa el uso de programas y utilidades que puedan ser capaces de invalidar los controles del sistema y de la aplicación.
11.5.5	Desconexión automática de sesión	SI	3 - Definido	Las sesiones inactivas deben cerrarse después de un periodo de inactividad definido.
11.5.6	Limitación del tiempo de conexión	SI	4 - Gestionado	Para proporcionar seguridad adicional a las aplicaciones de alto riesgo, se deben utilizar restricciones en los tiempos de conexión.
11.6.1	Restricción del acceso a la información	SI	4 - Gestionado	Se debe restringir el acceso a la información y a las aplicaciones a los usuarios y al personal de soporte, de acuerdo con la política de control de acceso definida.
11.6.2	Aislamiento de sistemas sensibles	SI	5 - Optimizado	Los sistemas sensibles deben tener un entorno dedicado (aislado) de ordenadores.
11.7.1	Ordenadores portátiles y comunicaciones móviles	SI	2 - Repetible	Se debe implantar una política formal y se deben adoptar las medidas de seguridad adecuadas para la protección contra los riesgos de la utilización de ordenadores portátiles y comunicaciones móviles.
11.7.2	Teletrabajo	SI	1 - Inicial	Se debe redactar e implantar, una política de actividades de teletrabajo, así como los planes y procedimientos de

				operación correspondientes.
12.1.1	Análisis y especificación de los requisitos de seguridad	SI	3 - Definido	En las declaraciones de los requisitos de negocio para los nuevos sistemas de información, o para mejoras de los sistemas de información ya existentes, se deben especificar los requisitos de los controles de seguridad.
12.2.1	Validación de los datos de entrada	SI	4 - Gestionado	La introducción de datos en las aplicaciones debe validarse para garantizar que dichos datos son correctos y adecuados.
12.2.2	Control del procesamiento interno	SI	4 - Gestionado	Para detectar cualquier corrupción de la información debida a errores de procesamiento o actos intencionados, se deben incorporar comprobaciones de validación en las aplicaciones.
12.2.3	Integridad de los mensajes	SI	2 - Repetible	Se deben identificar los requisitos para garantizar la autenticidad y para proteger la integridad de los mensajes en las aplicaciones y se deben identificar e implantar los controles adecuados.
12.2.4	Validación de los datos de salida	SI	2 - Repetible	Los datos de salida de una aplicación se deben validar para garantizar que el tratamiento de la información almacenada es correcto y adecuado a las circunstancias.
12.3.1	Política de uso de los controles criptográficos	SI	1 - Inicial	Se debe formular e implantar una política para el uso de los controles criptográficos para proteger la información.
12.3.2	Gestión de claves	SI	4 - Gestionado	Debe implantarse un sistema de gestión de claves para dar soporte al uso de técnicas criptográficas por parte de la organización.
12.4.1	Control del software en explotación	SI	3 - Definido	Deben estar implantados procedimientos para controlar la instalación de software en los sistemas en

				producción o en explotación.
12.4.2	Protección de los datos de prueba del sistema	SI	1 - Inicial	Los datos de prueba se deben seleccionar cuidadosamente y deberían estar protegidos y controlados.
12.4.3	Control de acceso al código fuente de los programas	SI	4 - Gestionado	Se debe restringir el acceso al código fuente de los programas.
12.5.1	Procedimientos de control de cambios	SI	2 - Repetible	La implantación de los cambios debe controlarse mediante el uso de procedimientos formales de control de cambios.
12.5.2	Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo	SI	4 - Gestionado	Cuando se modifiquen los sistemas operativos, las aplicaciones empresariales críticas deben ser revisadas y probadas para garantizar que no existen efectos adversos en las operaciones o en la seguridad de la organización.
12.5.3	Restricciones a los cambios en los paquetes de software	SI	5 - Optimizado	Se deben desaconsejar las modificaciones en los paquetes de software, limitándose a los cambios necesarios, y todos los cambios deben ser objeto de un control riguroso.
12.5.4	Fugas de información	SI	4 - Gestionado	Deben evitarse las situaciones que permitan que se produzcan fugas de información.
12.5.5	Externalización del desarrollo de software	SI	3 - Definido	La externalización del desarrollo de software debe ser supervisada y controlada por la organización.
12.6.1	Control de las vulnerabilidades técnicas	SI	3 - Definido	Se debe obtener la información adecuada acerca de las vulnerabilidades técnicas de los sistemas de información que están siendo utilizados, evaluar la exposición de la organización a dichas vulnerabilidades y adoptar las medidas adecuadas para afrontar el riesgo asociado.
13.1.1	Notificación de eventos de seguridad de la	SI	3 - Definido	Los eventos de seguridad de la información se deben

	información			notificar a través de los canales adecuados de gestión lo antes posible.
13.1.2	Notificación de puntos débiles de seguridad	SI	1 - Inicial	Todos los trabajadores, contratistas y terceros deben comunicar estos incidentes a su director, o directamente al proveedor de servicios, lo antes posible para evitar incidentes de seguridad de la información. El mecanismo de comunicación debe ser todo lo fácil, accesible y disponible que sea posible.
13.2.1	Responsabilidades y procedimientos	SI	1 - Inicial	Se deben establecer las responsabilidades y procedimientos de gestión para garantizar una respuesta rápida, efectiva y ordenada a los incidentes de seguridad de la información.
13.2.2	Aprendizaje de los incidentes de seguridad de la información	SI	1 - Inicial	Deben existir mecanismos que permitan cuantificar y supervisar los tipos, volúmenes y costes de los incidentes de seguridad de la información.
13.2.3	Recopilación de evidencias	SI	3 - Definido	Cuando se emprenda una acción contra una persona u organización, después de un incidente de seguridad de la información, que implique acciones legales (tanto civiles como penales), deben recopilarse las evidencias, y conservarse y presentarse conforme a las normas establecidas en la jurisdicción correspondiente.
14.1.1	Inclusión de la seguridad de la información en el proceso de gestión de la continuidad del negocio	SI	3 - Definido	Debe desarrollarse y mantenerse un proceso para la continuidad del negocio en toda la organización, que gestione los requisitos de seguridad de la información necesarios para la continuidad del negocio.
14.1.2	Continuidad del negocio y evaluación de riesgos	SI	2 - Repetible	Deben identificarse los eventos que puedan causar

				interrupciones en los procesos de negocio, así como la probabilidad de que se produzcan tales interrupciones, sus efectos y sus consecuencias para la seguridad de la información.
14.1.3	Desarrollo e implantación de planes de continuidad que incluyan la seguridad de la información	SI	2 - Repetible	Deben desarrollarse e implantarse planes para mantener o restaurar las operaciones y garantizar la disponibilidad de la información en el nivel y en el tiempo requerido, después de una interrupción o un fallo de los procesos críticos de negocio.
14.1.4	Marco de referencia para la continuidad del negocio	SI	1 - Inicial	Debe mantenerse un único marco de referencia para los planes de continuidad del negocio, para asegurar que todos los planes sean coherentes, para cumplir los requisitos de seguridad de la información de manera consistente y para identificar las prioridades de realización de pruebas y del mantenimiento.
14.1.5	Pruebas, mantenimiento y reevaluación de los planes de continuidad del negocio	SI	1 - Inicial	Los planes de continuidad del negocio deben probarse y actualizarse periódicamente para asegurar que están al día y que son efectivos.
15.1.1	Identificación de la legislación aplicable	SI	5 - Optimizado	Todos los requisitos pertinentes, tanto legales como reglamentarios o contractuales, y el enfoque de la organización para cumplir dichos requisitos, deben estar definidos, documentados y mantenerse actualizados de forma explícita para cada sistema de información de la organización.
15.1.2	Derechos de propiedad intelectual (DPI)	SI	5 - Optimizado	Deben implantarse procedimientos adecuados para garantizar el cumplimiento de los requisitos legales, reglamentarios y

				contractuales sobre el uso de material, con respecto al cual puedan existir derechos de propiedad intelectual y sobre el uso de productos de software propietario.
15.1.3	Protección de los documentos de la organización	SI	5 - Optimizado	Los documentos importantes deben estar protegidos contra la pérdida, destrucción y falsificación de acuerdo con los requisitos legales, reglamentarios, contractuales y empresariales.
15.1.4	Protección de datos y privacidad de la información de carácter personal	SI	5 - Optimizado	Debe garantizarse la protección y la privacidad de los datos según se requiera en la legislación y la reglamentación aplicables y, en su caso, en las cláusulas contractuales pertinentes.
15.1.5	Prevención del uso indebido de los recursos de tratamiento de la información	SI	4 - Gestionado	Se debe disuadir a los usuarios de utilizar los recursos de tratamiento de la información para fines no autorizados.
15.1.6	Regulación de los controles criptográficos	SI	3 - Definido	Los controles criptográficos se deben utilizar de acuerdo con todos los contratos, leyes y reglamentaciones pertinentes.
15.2.1	Cumplimiento de las políticas y normas de seguridad	SI	2 - Repetible	Los directores deben asegurarse de que todos los procedimientos de seguridad dentro de su área de responsabilidad se realizan correctamente con el fin de cumplir las políticas y normas de seguridad.
15.2.2	Comprobación del cumplimiento técnico	SI	3 - Definido	Debe comprobarse periódicamente que los sistemas de información cumplen las normas de aplicación para la implantación.
15.3.1	Controles de auditoría de los sistemas de información	SI	3 - Definido	Los requisitos y las actividades de auditoría que impliquen comprobaciones en los sistemas en producción deben ser

				cuidadosamente planificados y acordados para minimizar el riesgo de interrupciones en los procesos del negocio.
15.3.2	Protección de las herramientas de auditoría de los sistemas de información	SI	3 - Definido	El acceso a las herramientas de auditoría de los sistemas de información debe estar protegido para evitar cualquier posible peligro o uso indebido.

Tabla 3-6: Declaración de aplicabilidad

CAPÍTULO 4. ANÁLISIS DE RIESGOS

El análisis de riesgos es uno de los puntos más importantes del Plan Director de Seguridad de la organización. Según MAGERIT [9], el análisis de riesgos es una aproximación metódica para determinar el riesgo siguiendo unos pasos pautados:

1. Determinar los activos relevantes para la organización, su interrelación y su valor, en el sentido de qué perjuicio (coste) supondría su degradación.
2. Determinar a qué amenazas están expuestos aquellos activos.
3. Determinar qué salvaguardas hay dispuestas y cuán eficaces son frente al riesgo.
4. Estimar el impacto, definido como el daño sobre el activo derivado de la materialización de la amenaza.
5. Estimar el riesgo, definido como el impacto ponderado con la tasa de ocurrencia (o expectativa de materialización) de la amenaza.

La Figura 4-1 muestra en forma de esquema el procedimiento o las fases de las que consta un análisis de riesgos.

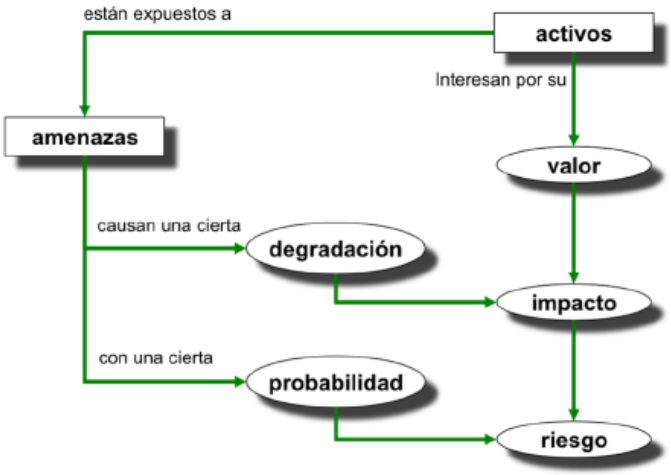

Figura 4-1: Esquema de análisis de riesgos MAGERIT

El análisis de riesgos que aquí se llevará a cabo seguirá las fases de la metodología de análisis de riesgos definida para la organización, y que, como ya se comentó, sigue en esencia la propuesta de pasos establecida en MAGERIT.

4.1 IDENTIFICACIÓN, CLASIFICACIÓN Y VALORACIÓN DE LOS ACTIVOS

La Tabla 4-1 recoge el inventario de activos de la organización. Esta tabla muestra para cada activo su categoría, propietario, valor del activo en la organización y la

valoración de la criticidad de cada activo en cada una de las dimensiones de la seguridad. Para la valoración del activo en la organización se utilizará la escala definida en la metodología de análisis de riesgos, mientras que para la valoración de las dimensiones de la seguridad, se utilizará una escala del 0 al 10, de menor a mayor criticidad.

Categoría	Activo	Propietario	Valor	Aspectos críticos		
				C	I	D
Instalaciones (I)	Sede central	Director General	Muy Alto (MA)	2	1	10
	Sucursales	Directores sucursales	Alto (A)	0	0	8
Personal (P)	Director General	-	Alto (A)	0	0	9
	Directores sucursales	-	Medio (M)	0	0	5
	Empleados sucursales	-	Bajo (B)	0	0	3
	Jefe Departamento de TI	-	Alto (A)	0	0	9
	Responsables de seguridad	-	Medio (M)	0	0	6
	Técnicos/desarrolladores	-	Bajo (B)	0	0	3
Hardware (HW)	Servidor central	Jefe Departamento de TI	Muy Alto (MA)	5	7	10
	Servidor banca online	Jefe Departamento de TI	Muy Alto (MA)	5	7	9
	Servidor de backup	Responsables de seguridad	Medio (M)	5	7	7
	Equipos de oficina	Técnicos / desarrolladores	Bajo (B)	0	5	3
	Equipos de personal de TI	Técnicos / desarrolladores	Medio (M)	2	7	3
	Switches CPD	Jefe Departamento de TI	Muy Alto (MA)	5	7	9
	Switches sucursales	Responsables de seguridad	Alto (A)	3	6	7
	Puntos de acceso	Responsables de seguridad	Medio (M)	1	4	6
	Routers CPD	Jefe Departamento de TI	Muy Alto (MA)	5	7	9
	Firewalls	Responsables de seguridad	Alto (A)	3	9	9
	Impresoras	Técnicos / desarrolladores	Muy Bajo (MB)	0	1	2
	SAI	Responsables de seguridad	Medio (M)	0	1	7
	Cámaras de videovigilancia	Responsables de seguridad	Bajo (B)	2	6	6
	Sistema de alarma	Técnicos / desarrolladores	Muy Alto (MA)	2	9	9
	Cajeros automáticos	Técnicos / desarrolladores	Alto (A)	0	9	6

Comunicación (COM)	ISP primario	Jefe Departamento de TI	Muy Alto (A)	0	3	9
	ISP secundario	Jefe Departamento de TI	Bajo (B)	0	3	6
	Red LAN CPD	Responsables de seguridad	Muy Alto (MA)	9	9	9
	Red LAN sucursales	Técnicos / desarrolladores	Alto (A)	9	9	7
	Redes WiFi	Técnicos / desarrolladores	Medio (M)	9	9	6
Software (SW)	Windows Server 2012 Standard Edition	Técnicos / desarrolladores	Muy Alto (MA)	8	8	9
	Linux Ubuntu Server 11.10	Técnicos / desarrolladores	Muy Alto (MA)	8	8	9
	Apache Web Server	Técnicos / desarrolladores	Alto (A)	6	7	9
	Windows 8.1	Técnicos / desarrolladores	Medio (M)	3	3	5
	Aplicación Gestión Bancaria	Técnicos / desarrolladores	Muy Alto (MA)	7	9	10
	SGBD Oracle 10g	Técnicos / desarrolladores	Muy Alto (MA)	10	10	9
	ESET Smart Security 8	Responsables de seguridad	Medio (M)	3	5	7
	Windows XP Embedded	Técnicos / desarrolladores	Alto (A)	8	9	6
	Herramienta Amanda para backup	Responsables de seguridad	Medio (M)	5	7	7
Servicio (S)	Servicios de banca online	Jefe Departamento de TI	Alto (A)	10	10	8
Datos (D)	BBDD clientes	Director General	Muy Alto (MA)	10	10	9
	BBDD información financiera	Director General	Muy Alto (MA)	10	10	9
	BBDD gestión empleados	Director General	Muy Alto (MA)	10	10	8
	Sistema de Gestión Documental	Director General	Muy Alto (MA)	10	10	7

Tabla 4-1: Inventario de activos de la organización

4.2 IDENTIFICACIÓN DE LAS AMENAZAS

Se abordará esta fase del análisis de riesgos en dos pasos. En primer lugar, se llevará a cabo una identificación de todas las posibles amenazas que pueden afectar a los activos de la organización, indicando para cada una de ellas la categoría o categorías de activos y la dimensión o dimensiones de seguridad a las que puede afectar su materialización (Tabla 4-2).

Una vez identificado esto, se definirá una tabla que relacionará las categorías de activos con sus posibles amenazas, dando para cada relación la probabilidad de ocurrencia de la amenaza y el impacto de la misma en las distintas dimensiones de seguridad del activo (Tabla 4-3).

Amenaza	Categorías activos afectadas							Dimensión afectada		
	D	COM	HW	SW	S	P	L	C	I	D
Fuego			x				x			x
Daños por agua			x				x			x
Desastres naturales			x				x			x
Contaminación mecánica			x							x
Contaminación electromagnética			x							x
Avería de origen físico o lógico			x	x						x
Corte del suministro eléctrico			x							x
Condiciones inadecuadas de temperatura o humedad			x							x
Fallo de servicios de comunicaciones		x								x
Interrupción de otros servicios y suministros esenciales			x							x
Degradación de los soportes de almacenamiento de la información			x							x
Emanaciones electromagnéticas			x				x	x		
Errores de los usuarios	x			x	x			x	x	x
Errores del administrador	x	x	x	x	x			x	x	x
Errores de monitorización (log)	x								x	
Errores de configuración	x								x	
Deficiencias en la organización						x				x
Difusión de software dañino				x				x	x	x
Destrucción de información	x	x		x	x		x			x
Fugas de información	x	x	x	x	x	x	x	x		
Vulnerabilidades de los programas (software)				x				x	x	x
Errores de mantenimiento / actualización de programas (software)				x					x	x
Errores de mantenimiento / actualización de equipos (hardware)			x							x
Caída del sistema por agotamiento de recursos		x	x		x					x
Pérdida de equipos			x					x		x
Indisponibilidad del personal						x				x
Manipulación de los registros de actividad (log)	x								x	
Manipulación de la	x							x	x	x

configuración										
Suplantación de la identidad del usuario	x	x		x	x			x	x	
Abuso de privilegios de acceso	x	x	x	x	x			x	x	x
Uso no previsto		x	x	x	x		x	x	x	x
[Re-]encaminamiento de mensajes		x		x	x			x		
Alteración de secuencia		x		x	x				x	
Acceso no autorizado	x	x	x	x	x		x	x	x	
Análisis de tráfico		x						x		
Repudio	x				x				x	
Interceptación de información (escucha)		x						x		
Modificación de la información	x	x		x	x		x		x	
Manipulación de programas				x				x	x	x
Manipulación de los equipos			x					x		x
Denegación de servicio		x	x		x					x
Robo			x					x		x
Ataque destructivo			x				x			x
Ocupación enemiga							x	x		x
Extorsión						x		x	x	x
Ingeniería social (picaresca)						x		x	x	x

Tabla 4-2: Catálogo de amenazas

Categoría de activo	Amenaza	Probabilidad de ocurrencia	Impacto		
			C	I	D
Datos (D)	Errores de los usuarios	Media (M)	50%	50%	20%
	Errores del administrador	Baja (B)	75%	75%	20%
	Errores de monitorización (log)	Baja (B)		50%	
	Errores de configuración	Baja (B)		75%	
	Destrucción de información	Baja (B)			75%
	Fugas de información	Media (M)	75%		
	Manipulación de los registros de actividad (log)	Baja (B)		50%	
	Manipulación de la configuración	Baja (B)	75%	75%	75%
	Suplantación de la identidad del usuario	Media (M)	100%	75%	
	Abuso de privilegios de acceso	Media (M)	75%	75%	50%
	Acceso no autorizado	Baja (B)	75%	75%	
	Repudio	Baja (B)		75%	
	Modificación de la información	Media (M)		100%	
Comunicación (COM)	Fallo de servicios de comunicaciones	Baja (B)			75%
	Errores del administrador	Baja (B)	75%	75%	50%
	Destrucción de información	Baja (B)			50%
	Fugas de información	Media (M)	50%		
	Caída del sistema por agotamiento de recursos	Media (M)			100%

	Suplantación de la identidad del usuario	Media (M)	75%	75%	
	Abuso de privilegios de acceso	Media (M)	50%	50%	20%
	Uso no previsto	Alta (A)	5%	5%	50%
	[Re-]encaminamiento de mensajes	Baja (B)	75%		
	Alteración de secuencia	Baja (B)		75%	
	Acceso no autorizado	Baja (B)	100%	75%	
	Análisis de tráfico	Media (M)	50%		
	Interceptación de información (escucha)	Baja (B)	75%		
	Modificación de la información	Media (M)		100%	
	Denegación de servicio	Media (M)			100%
Hardware (HW)	Fuego	Baja (B)			75%
	Daños por agua	Baja (B)			50%
	Desastres naturales	Muy Baja (MB)			75%
	Contaminación mecánica	Alta (A)			50%
	Contaminación electromagnética	Muy Baja (MB)			50%
	Avería de origen físico o lógico	Alta (A)			75%
	Corte del suministro eléctrico	Alta (A)			100%
	Condiciones inadecuadas de temperatura o humedad	Baja (B)			50%
	Interrupción de otros servicios y suministros esenciales	Muy Baja (MB)			20%
	Degradación de los soportes de almacenamiento de la información	Media (M)			20%
	Emanaciones electromagnéticas	Muy Baja (MB)	20%		
	Errores del administrador	Baja (B)	75%	50%	75%
	Fugas de información	Media (M)	50%		
	Errores de mantenimiento / actualización de equipos (hardware)	Baja (B)			50%
	Caída del sistema por agotamiento de recursos	Media (M)			100%
	Pérdida de equipos	Baja (B)	50%		100%
	Abuso de privilegios de acceso	Media (M)	50%	50%	20%
	Uso no previsto	Alta (A)	5%	5%	50%
	Acceso no autorizado	Baja (B)	75%	50%	
	Manipulación de los equipos	Baja (B)	50%		75%
	Denegación de servicio	Baja (B)			100%
	Robo	Baja (B)	75%		100%
	Ataque destructivo	Muy Baja (MB)			100%
Software (SW)	Avería de origen físico o lógico	Media (M)			75%
	Errores de los usuarios	Media (M)	50%	75%	50%
	Errores del administrador	Baja (B)	75%	75%	75%
	Difusión de software dañino	Alta (A)	75%	75%	75%
	Destrucción de información	Media (M)			100%

	Fugas de información	Media (M)	75%		
	Vulnerabilidades de los programas (software)	Alta (A)	75%	75%	75%
	Errores de mantenimiento / actualización de programas (software)	Media (M)		75%	20%
	Suplantación de la identidad del usuario	Baja (B)	75%	75%	
	Abuso de privilegios de acceso	Media (M)	20%	75%	50%
	Uso no previsto	Alta (A)	20%	20%	50%
	[Re-]encaminamiento de mensajes	Baja (B)	50%		
	Alteración de secuencia	Baja (B)		20%	
	Acceso no autorizado	Media (M)	75%	50%	
	Modificación de la información	Media (M)		75%	
	Manipulación de programas	Baja (B)	75%	75%	50%
Servicio (S)	Errores de los usuarios	Alta (A)	50%	75%	20%
	Errores del administrador	Baja (B)	75%	50%	50%
	Destrucción de información	Media (M)			50%
	Fugas de información	Alta (A)	75%		
	Caída del sistema por agotamiento de recursos	Media (M)			100%
	Suplantación de la identidad del usuario	Alta (A)	100%	75%	
	Abuso de privilegios de acceso	Baja (B)	50%	75%	20%
	Uso no previsto	Media (M)	20%	20%	50%
	[Re-]encaminamiento de mensajes	Baja (B)	75%		
	Alteración de secuencia	Baja (B)		75%	
	Acceso no autorizado	Baja (B)	100%	75%	
	Repudio	Muy Baja (MB)		75%	
	Modificación de la información	Baja (B)		75%	
	Denegación de servicio	Media (M)			100%
Personal (P)	Deficiencias en la organización	Media (M)			50%
	Fugas de información	Baja (B)	100%		
	Indisponibilidad del personal	Alta (A)			75%
	Extorsión	Media (M)	75%	50%	50%
	Ingeniería social (picaresca)	Alta (A)	100%	50%	20%
Instalaciones (L)	Fuego	Baja (B)			75%
	Daños por agua	Baja (B)			50%
	Desastres naturales	Muy Baja (MB)			100%
	Emanaciones electromagnéticas	Muy Baja (MB)	5%		
	Destrucción de información	Muy Baja (MB)			5%
	Fugas de información	Media (M)	50%		
	Uso no previsto	Baja (B)	5%	20%	20%
	Acceso no autorizado	Media (M)	75%	75%	
	Modificación de la información	Media (M)		20%	
	Ataque destructivo	Media (M)			50%

	Ocupación enemiga	Muy Baja (MB)	75%		100%

Tabla 4-3: Relación entre activos y amenazas

4.3 CÁLCULO DEL RIESGO POTENCIAL

La siguiente fase del análisis de riesgos aborda el cálculo de los valores del riesgo potencial para los activos de la organización. Para el cálculo de estos valores, se aplicarán las formulas definidas en la metodología de análisis de riesgos de la organización. Este cálculo de los valores del riesgo potencial se presentará en forma de una tabla (Tabla 4-4), en la cual aparecerán para cada pareja activo-amenaza, sus valores de riesgo potencial en las dimensiones de confidencialidad, integridad y disponibilidad, RP_C, RP_I y RP_D, respectivamente.

Teniendo en cuenta los resultados obtenidos, la dirección de la organización ha establecido que el nivel de riesgo aceptable será aquel que esté por debajo de un valor de 8. Por tanto, se deberán aplicar salvaguardas o mejorar su estado actual de implantación para todas las amenazas cuya materialización represente un valor de riesgo igual o superior a éste, con el objetivo de que dicho valor quede por debajo del umbral de riesgo aceptable.

Categoría	Activo	Amenaza	Riesgo potencial		
			RP_C	RP_I	RP_D
D	BBDD clientes	Errores de los usuarios	7.5	7.5	3
		Errores del administrador	7.5	7.5	2
		Errores de monitorización (log)	0	5	0
		Errores de configuración	0	7.5	0
		Destrucción de información	0	0	7.5
		Fugas de información	11.25	0	0
		Manipulación de los registros de actividad (log)	0	5	0
		Manipulación de la configuración	7.5	7.5	7.5
		Suplantación de la identidad del usuario	15	11.25	0
		Abuso de privilegios de acceso	11.25	11.25	7.5
		Acceso no autorizado	7.5	7.5	0
		Repudio	0	7.5	0
		Modificación de la información	0	15	0
	BBDD información financiera	Errores de los usuarios	7.5	7.5	3
		Errores del administrador	7.5	7.5	2
		Errores de monitorización (log)	0	5	0
		Errores de configuración	0	7.5	0
		Destrucción de información	0	0	7.5
		Fugas de información	11.25	0	0
		Manipulación de los registros de actividad (log)	0	5	0
		Manipulación de la configuración	7.5	7.5	7.5
		Suplantación de la identidad del usuario	15	11.25	0
		Abuso de privilegios de acceso	11.25	11.25	7.5
		Acceso no autorizado	7.5	7.5	0

		Repudio	0	7.5	0
		Modificación de la información	0	15	0
	BBDD gestión empleados	Errores de los usuarios	7.5	7.5	3
		Errores del administrador	7.5	7.5	2
		Errores de monitorización (log)	0	5	0
		Errores de configuración	0	7.5	0
		Destrucción de información	0	0	7.5
		Fugas de información	11.25	0	0
		Manipulación de los registros de actividad (log)	0	5	0
		Manipulación de la configuración	7.5	7.5	7.5
		Suplantación de la identidad del usuario	15	11.25	0
		Abuso de privilegios de acceso	11.25	11.25	7.5
		Acceso no autorizado	7.5	7.5	0
		Repudio	0	7.5	0
		Modificación de la información	0	15	0
	Sistema de Gestión Documental	Errores de los usuarios	7.5	7.5	3
		Errores del administrador	7.5	7.5	2
		Errores de monitorización (log)	0	5	0
		Errores de configuración	0	7.5	0
		Destrucción de información	0	0	7.5
		Fugas de información	11.25	0	0
		Manipulación de los registros de actividad (log)	0	5	0
		Manipulación de la configuración	7.5	7.5	7.5
		Suplantación de la identidad del usuario	15	11.25	0
		Abuso de privilegios de acceso	11.25	11.25	7.5
		Acceso no autorizado	7.5	7.5	0
		Repudio	0	7.5	0
		Modificación de la información	0	15	0
COM	ISP primario	Fallo de servicios de comunicaciones	0	0	7.5
		Errores del administrador	7.5	7.5	5
		Destrucción de información	0	0	5
		Fugas de información	7.5	0	0
		Caída del sistema por agotamiento de recursos	0	0	15
		Suplantación de la identidad del usuario	11.25	11.25	0
		Abuso de privilegios de acceso	7.5	7.5	3
		Uso no previsto	1	1	10
		[Re-]encaminamiento de mensajes	7.5	0	0
		Alteración de secuencia	0	7.5	0
		Acceso no autorizado	10	7.5	0
		Análisis de tráfico	7.5	0	0
		Interceptación de información (escucha)	7.5	0	0
		Modificación de la información	0	15	0
		Denegación de servicio	0	0	15
	ISP secundario	Fallo de servicios de comunicaciones	0	0	3
		Errores del administrador	3	3	2
		Destrucción de información	0	0	2
		Fugas de información	3	0	0
		Caída del sistema por agotamiento de recursos	0	0	6
		Suplantación de la identidad del usuario	4.5	4.5	0

		Abuso de privilegios de acceso	3	3	1.2
		Uso no previsto	0.4	0.4	4
		[Re-]encaminamiento de mensajes	3	0	0
		Alteración de secuencia	0	3	0
		Acceso no autorizado	4	3	0
		Análisis de tráfico	3	0	0
		Interceptación de información (escucha)	3	0	0
		Modificación de la información	0	6	0
		Denegación de servicio	0	0	6
	Red LAN CPD	Fallo de servicios de comunicaciones	0	0	7.5
		Errores del administrador	7.5	7.5	5
		Destrucción de información	0	0	5
		Fugas de información	7.5	0	0
		Caída del sistema por agotamiento de recursos	0	0	15
		Suplantación de la identidad del usuario	11.25	11.25	0
		Abuso de privilegios de acceso	7.5	7.5	3
		Uso no previsto	1	1	10
		[Re-]encaminamiento de mensajes	7.5	0	0
		Alteración de secuencia	0	7.5	0
		Acceso no autorizado	10	7.5	0
		Análisis de tráfico	7.5	0	0
		Interceptación de información (escucha)	7.5	0	0
		Modificación de la información	0	15	0
		Denegación de servicio	0	0	15
	Red LAN sucursales	Fallo de servicios de comunicaciones	0	0	6
		Errores del administrador	6	6	4
		Destrucción de información	0	0	4
		Fugas de información	6	0	0
		Caída del sistema por agotamiento de recursos	0	0	12
		Suplantación de la identidad del usuario	9	9	0
		Abuso de privilegios de acceso	6	6	2.4
		Uso no previsto	0.8	0.8	8
		[Re-]encaminamiento de mensajes	6	0	0
		Alteración de secuencia	0	6	0
		Acceso no autorizado	8	6	0
		Análisis de tráfico	6	0	0
		Interceptación de información (escucha)	6	0	0
		Modificación de la información	0	12	0
		Denegación de servicio	0	0	12
	Redes WiFi	Fallo de servicios de comunicaciones	0	0	4.5
		Errores del administrador	4.5	4.5	3
		Destrucción de información	0	0	3
		Fugas de información	4.5	0	0
		Caída del sistema por agotamiento de recursos	0	0	9
		Suplantación de la identidad del usuario	6.75	6.75	0
		Abuso de privilegios de acceso	4.5	4.5	1.8
		Uso no previsto	0.6	0.6	6
		[Re-]encaminamiento de mensajes	4.5	0	0
		Alteración de secuencia	0	4.5	0
		Acceso no autorizado	6	4.5	0

		Análisis de tráfico	4.5	0	0
		Interceptación de información (escucha)	4.5	0	0
		Modificación de la información	0	9	0
		Denegación de servicio	0	0	9
HW	Servidor central	Fuego	0	0	7.5
		Daños por agua	0	0	5
		Desastres naturales	0	0	3.75
		Contaminación mecánica	0	0	10
		Contaminación electromagnética	0	0	2.5
		Avería de origen físico o lógico	0	0	15
		Corte del suministro eléctrico	0	0	20
		Condiciones inadecuadas de temperatura o humedad	0	0	5
		Interrupción de otros servicios y suministros esenciales	0	0	1
		Degradación de los soportes de almacenamiento de la información	0	0	3
		Emanaciones electromagnéticas	1	0	0
		Errores del administrador	7.5	5	7.5
		Fugas de información	7.5	0	0
		Errores de mantenimiento / actualización de equipos (hardware)	0	0	5
		Caída del sistema por agotamiento de recursos	0	0	15
		Pérdida de equipos	5	0	10
		Abuso de privilegios de acceso	7.5	7.5	3
		Uso no previsto	1	1	10
		Acceso no autorizado	7.5	5	0
		Manipulación de los equipos	5	0	7.5
		Denegación de servicio	0	0	10
		Robo	7.5	0	10
		Ataque destructivo	0	0	5
	Servidor banca online	Fuego	0	0	7.5
		Daños por agua	0	0	5
		Desastres naturales	0	0	3.75
		Contaminación mecánica	0	0	10
		Contaminación electromagnética	0	0	2.5
		Avería de origen físico o lógico	0	0	15
		Corte del suministro eléctrico	0	0	20
		Condiciones inadecuadas de temperatura o humedad	0	0	5
		Interrupción de otros servicios y suministros esenciales	0	0	1
		Degradación de los soportes de almacenamiento de la información	0	0	3
		Emanaciones electromagnéticas	1	0	0
		Errores del administrador	7.5	5	7.5
		Fugas de información	7.5	0	0
		Errores de mantenimiento / actualización de equipos (hardware)	0	0	5
		Caída del sistema por agotamiento de recursos	0	0	15
		Pérdida de equipos	5	0	10

		Abuso de privilegios de acceso	7.5	7.5	3
		Uso no previsto	1	1	10
		Acceso no autorizado	7.5	5	0
		Manipulación de los equipos	5	0	7.5
		Denegación de servicio	0	0	10
		Robo	7.5	0	10
		Ataque destructivo	0	0	5
	Servidor de backup	Fuego	0	0	4.5
		Daños por agua	0	0	3
		Desastres naturales	0	0	2.25
		Contaminación mecánica	0	0	6
		Contaminación electromagnética	0	0	1.5
		Avería de origen físico o lógico	0	0	9
		Corte del suministro eléctrico	0	0	12
		Condiciones inadecuadas de temperatura o humedad	0	0	3
		Interrupción de otros servicios y suministros esenciales	0	0	0.6
		Degradación de los soportes de almacenamiento de la información	0	0	1.8
		Emanaciones electromagnéticas	0.6	0	0
		Errores del administrador	4.5	3	4.5
		Fugas de información	4.5	0	0
		Errores de mantenimiento / actualización de equipos (hardware)	0	0	3
		Caída del sistema por agotamiento de recursos	0	0	9
		Pérdida de equipos	3	0	6
		Abuso de privilegios de acceso	4.5	4.5	1.8
		Uso no previsto	0.6	0.6	6
		Acceso no autorizado	4.5	3	0
		Manipulación de los equipos	3	0	4.5
		Denegación de servicio	0	0	6
		Robo	4.5	0	6
		Ataque destructivo	0	0	3
	Equipos de oficina	Fuego	0	0	3
		Daños por agua	0	0	2
		Desastres naturales	0	0	1.5
		Contaminación mecánica	0	0	4
		Contaminación electromagnética	0	0	1
		Avería de origen físico o lógico	0	0	6
		Corte del suministro eléctrico	0	0	8
		Condiciones inadecuadas de temperatura o humedad	0	0	2
		Interrupción de otros servicios y suministros esenciales	0	0	0.4
		Degradación de los soportes de almacenamiento de la información	0	0	1.2
		Emanaciones electromagnéticas	0.4	0	0
		Errores del administrador	3	2	3
		Fugas de información	3	0	0
		Errores de mantenimiento / actualización de equipos (hardware)	0	0	2

		Caída del sistema por agotamiento de recursos	0	0	6
		Pérdida de equipos	2	0	4
		Abuso de privilegios de acceso	3	3	1.2
		Uso no previsto	0.4	0.4	4
		Acceso no autorizado	3	2	0
		Manipulación de los equipos	2	0	3
		Denegación de servicio	0	0	4
		Robo	3	0	4
		Ataque destructivo	0	0	2
	Equipos de personal de TI	Fuego	0	0	4.5
		Daños por agua	0	0	3
		Desastres naturales	0	0	2.25
		Contaminación mecánica	0	0	6
		Contaminación electromagnética	0	0	1.5
		Avería de origen físico o lógico	0	0	9
		Corte del suministro eléctrico	0	0	12
		Condiciones inadecuadas de temperatura o humedad	0	0	3
		Interrupción de otros servicios y suministros esenciales	0	0	0.6
		Degradación de los soportes de almacenamiento de la información	0	0	1.8
		Emanaciones electromagnéticas	0.6	0	0
		Errores del administrador	4.5	3	4.5
		Fugas de información	4.5	0	0
		Errores de mantenimiento / actualización de equipos (hardware)	0	0	3
		Caída del sistema por agotamiento de recursos	0	0	9
		Pérdida de equipos	3	0	6
		Abuso de privilegios de acceso	4.5	4.5	1.8
		Uso no previsto	0.6	0.6	6
		Acceso no autorizado	4.5	3	0
		Manipulación de los equipos	3	0	4.5
		Denegación de servicio	0	0	6
		Robo	4.5	0	6
		Ataque destructivo	0	0	3
	Switches CPD	Fuego	0	0	7.5
		Daños por agua	0	0	5
		Desastres naturales	0	0	3.75
		Contaminación mecánica	0	0	10
		Contaminación electromagnética	0	0	2.5
		Avería de origen físico o lógico	0	0	15
		Corte del suministro eléctrico	0	0	20
		Condiciones inadecuadas de temperatura o humedad	0	0	5
		Interrupción de otros servicios y suministros esenciales	0	0	1
		Degradación de los soportes de almacenamiento de la información	0	0	3
		Emanaciones electromagnéticas	1	0	0
		Errores del administrador	7.5	5	7.5

		Fugas de información	7.5	0	0
		Errores de mantenimiento / actualización de equipos (hardware)	0	0	5
		Caída del sistema por agotamiento de recursos	0	0	15
		Pérdida de equipos	5	0	10
		Abuso de privilegios de acceso	7.5	7.5	3
		Uso no previsto	1	1	10
		Acceso no autorizado	7.5	5	0
		Manipulación de los equipos	5	0	7.5
		Denegación de servicio	0	0	10
		Robo	7.5	0	10
		Ataque destructivo	0	0	5
	Switches sucursales	Fuego	0	0	6
		Daños por agua	0	0	4
		Desastres naturales	0	0	3
		Contaminación mecánica	0	0	8
		Contaminación electromagnética	0	0	2
		Avería de origen físico o lógico	0	0	12
		Corte del suministro eléctrico	0	0	16
		Condiciones inadecuadas de temperatura o humedad	0	0	4
		Interrupción de otros servicios y suministros esenciales	0	0	0.8
		Degradación de los soportes de almacenamiento de la información	0	0	2.4
		Emanaciones electromagnéticas	0.8	0	0
		Errores del administrador	6	4	6
		Fugas de información	6	0	0
		Errores de mantenimiento / actualización de equipos (hardware)	0	0	4
		Caída del sistema por agotamiento de recursos	0	0	12
		Pérdida de equipos	4	0	8
		Abuso de privilegios de acceso	6	6	2.4
		Uso no previsto	0.8	0.8	8
		Acceso no autorizado	6	4	0
		Manipulación de los equipos	4	0	6
		Denegación de servicio	0	0	8
		Robo	6	0	8
		Ataque destructivo	0	0	4
	Puntos de acceso	Fuego	0	0	4.5
		Daños por agua	0	0	3
		Desastres naturales	0	0	2.25
		Contaminación mecánica	0	0	6
		Contaminación electromagnética	0	0	1.5
		Avería de origen físico o lógico	0	0	9
		Corte del suministro eléctrico	0	0	12
		Condiciones inadecuadas de temperatura o humedad	0	0	3
		Interrupción de otros servicios y suministros esenciales	0	0	0.6
		Degradación de los soportes de	0	0	1.8

		almacenamiento de la información			
		Emanaciones electromagnéticas	0.6	0	0
		Errores del administrador	4.5	3	4.5
		Fugas de información	4.5	0	0
		Errores de mantenimiento / actualización de equipos (hardware)	0	0	3
		Caída del sistema por agotamiento de recursos	0	0	9
		Pérdida de equipos	3	0	6
		Abuso de privilegios de acceso	4.5	4.5	1.8
		Uso no previsto	0.6	0.6	6
		Acceso no autorizado	4.5	3	0
		Manipulación de los equipos	3	0	4.5
		Denegación de servicio	0	0	6
		Robo	4.5	0	6
		Ataque destructivo	0	0	3
	Routers CPD	Fuego	0	0	7.5
		Daños por agua	0	0	5
		Desastres naturales	0	0	3.75
		Contaminación mecánica	0	0	10
		Contaminación electromagnética	0	0	2.5
		Avería de origen físico o lógico	0	0	15
		Corte del suministro eléctrico	0	0	20
		Condiciones inadecuadas de temperatura o humedad	0	0	5
		Interrupción de otros servicios y suministros esenciales	0	0	1
		Degradación de los soportes de almacenamiento de la información	0	0	3
		Emanaciones electromagnéticas	1	0	0
		Errores del administrador	7.5	5	7.5
		Fugas de información	7.5	0	0
		Errores de mantenimiento / actualización de equipos (hardware)	0	0	5
		Caída del sistema por agotamiento de recursos	0	0	15
		Pérdida de equipos	5	0	10
		Abuso de privilegios de acceso	7.5	7.5	3
		Uso no previsto	1	1	10
		Acceso no autorizado	7.5	5	0
		Manipulación de los equipos	5	0	7.5
		Denegación de servicio	0	0	10
		Robo	7.5	0	10
		Ataque destructivo	0	0	5
	Firewalls	Fuego	0	0	6
		Daños por agua	0	0	4
		Desastres naturales	0	0	3
		Contaminación mecánica	0	0	8
		Contaminación electromagnética	0	0	2
		Avería de origen físico o lógico	0	0	12
		Corte del suministro eléctrico	0	0	16
		Condiciones inadecuadas de temperatura o humedad	0	0	4

		Interrupción de otros servicios y suministros esenciales	0	0	0.8
		Degradación de los soportes de almacenamiento de la información	0	0	2.4
		Emanaciones electromagnéticas	0.8	0	0
		Errores del administrador	6	4	6
		Fugas de información	6	0	0
		Errores de mantenimiento / actualización de equipos (hardware)	0	0	4
		Caída del sistema por agotamiento de recursos	0	0	12
		Pérdida de equipos	4	0	8
		Abuso de privilegios de acceso	6	6	2.4
		Uso no previsto	0.8	0.8	8
		Acceso no autorizado	6	4	0
		Manipulación de los equipos	4	0	6
		Denegación de servicio	0	0	8
		Robo	6	0	8
		Ataque destructivo	0	0	4
	Impresoras	Fuego	0	0	1.5
		Daños por agua	0	0	1
		Desastres naturales	0	0	0.75
		Contaminación mecánica	0	0	2
		Contaminación electromagnética	0	0	0.5
		Avería de origen físico o lógico	0	0	3
		Corte del suministro eléctrico	0	0	4
		Condiciones inadecuadas de temperatura o humedad	0	0	1
		Interrupción de otros servicios y suministros esenciales	0	0	0.2
		Degradación de los soportes de almacenamiento de la información	0	0	0.6
		Emanaciones electromagnéticas	0.2	0	0
		Errores del administrador	1.5	1	1.5
		Fugas de información	1.5	0	0
		Errores de mantenimiento / actualización de equipos (hardware)	0	0	1
		Caída del sistema por agotamiento de recursos	0	0	3
		Pérdida de equipos	1	0	2
		Abuso de privilegios de acceso	1.5	1.5	0.6
		Uso no previsto	0.2	0.2	2
		Acceso no autorizado	1.5	1	0
		Manipulación de los equipos	1	0	1.5
		Denegación de servicio	0	0	2
		Robo	1.5	0	2
		Ataque destructivo	0	0	1
	SAI	Fuego	0	0	4.5
		Daños por agua	0	0	3
		Desastres naturales	0	0	2.25
		Contaminación mecánica	0	0	6
		Contaminación electromagnética	0	0	1.5
		Avería de origen físico o lógico	0	0	9

		Corte del suministro eléctrico	0	0	12
		Condiciones inadecuadas de temperatura o humedad	0	0	3
		Interrupción de otros servicios y suministros esenciales	0	0	0.6
		Degradación de los soportes de almacenamiento de la información	0	0	1.8
		Emanaciones electromagnéticas	0.6	0	0
		Errores del administrador	4.5	3	4.5
		Fugas de información	4.5	0	0
		Errores de mantenimiento / actualización de equipos (hardware)	0	0	3
		Caída del sistema por agotamiento de recursos	0	0	9
		Pérdida de equipos	3	0	6
		Abuso de privilegios de acceso	4.5	4.5	1.8
		Uso no previsto	0.6	0.6	6
		Acceso no autorizado	4.5	3	0
		Manipulación de los equipos	3	0	4.5
		Denegación de servicio	0	0	6
		Robo	4.5	0	6
		Ataque destructivo	0	0	3
	Cámaras de videovigilancia	Fuego	0	0	3
		Daños por agua	0	0	2
		Desastres naturales	0	0	1.5
		Contaminación mecánica	0	0	4
		Contaminación electromagnética	0	0	1
		Avería de origen físico o lógico	0	0	6
		Corte del suministro eléctrico	0	0	8
		Condiciones inadecuadas de temperatura o humedad	0	0	2
		Interrupción de otros servicios y suministros esenciales	0	0	0.4
		Degradación de los soportes de almacenamiento de la información	0	0	1.2
		Emanaciones electromagnéticas	0.4	0	0
		Errores del administrador	3	2	3
		Fugas de información	3	0	0
		Errores de mantenimiento / actualización de equipos (hardware)	0	0	2
		Caída del sistema por agotamiento de recursos	0	0	6
		Pérdida de equipos	2	0	4
		Abuso de privilegios de acceso	3	3	1.2
		Uso no previsto	0.4	0.4	4
		Acceso no autorizado	3	2	0
		Manipulación de los equipos	2	0	3
		Denegación de servicio	0	0	4
		Robo	3	0	4
		Ataque destructivo	0	0	2
	Sistema de alarma	Fuego	0	0	7.5
		Daños por agua	0	0	5
		Desastres naturales	0	0	3.75

		Contaminación mecánica	0	0	10
		Contaminación electromagnética	0	0	2.5
		Avería de origen físico o lógico	0	0	15
		Corte del suministro eléctrico	0	0	20
		Condiciones inadecuadas de temperatura o humedad	0	0	5
		Interrupción de otros servicios y suministros esenciales	0	0	1
		Degradación de los soportes de almacenamiento de la información	0	0	3
		Emanaciones electromagnéticas	1	0	0
		Errores del administrador	7.5	5	7.5
		Fugas de información	7.5	0	0
		Errores de mantenimiento / actualización de equipos (hardware)	0	0	5
		Caída del sistema por agotamiento de recursos	0	0	15
		Pérdida de equipos	5	0	10
		Abuso de privilegios de acceso	7.5	7.5	3
		Uso no previsto	1	1	10
		Acceso no autorizado	7.5	5	0
		Manipulación de los equipos	5	0	7.5
		Denegación de servicio	0	0	10
		Robo	7.5	0	10
		Ataque destructivo	0	0	5
	Cajeros automáticos	Fuego	0	0	6
		Daños por agua	0	0	4
		Desastres naturales	0	0	3
		Contaminación mecánica	0	0	8
		Contaminación electromagnética	0	0	2
		Avería de origen físico o lógico	0	0	12
		Corte del suministro eléctrico	0	0	16
		Condiciones inadecuadas de temperatura o humedad	0	0	4
		Interrupción de otros servicios y suministros esenciales	0	0	0.8
		Degradación de los soportes de almacenamiento de la información	0	0	2.4
		Emanaciones electromagnéticas	0.8	0	0
		Errores del administrador	6	4	6
		Fugas de información	6	0	0
		Errores de mantenimiento / actualización de equipos (hardware)	0	0	4
		Caída del sistema por agotamiento de recursos	0	0	12
		Pérdida de equipos	4	0	8
		Abuso de privilegios de acceso	6	6	2.4
		Uso no previsto	0.8	0.8	8
		Acceso no autorizado	6	4	0
		Manipulación de los equipos	4	0	6
		Denegación de servicio	0	0	8
		Robo	6	0	8
		Ataque destructivo	0	0	4

SW	Windows Server 2012 Standard Edition	Avería de origen físico o lógico	0	0	11.25
		Errores de los usuarios	7.5	11.25	7.5
		Errores del administrador	7.5	7.5	7.5
		Difusión de software dañino	15	15	15
		Destrucción de información	0	0	15
		Fugas de información	11.25	0	0
		Vulnerabilidades de los programas (software)	15	15	15
		Errores de mantenimiento / actualización de programas (software)	0	11.25	3
		Suplantación de la identidad del usuario	7.5	7.5	0
		Abuso de privilegios de acceso	3	11.25	7.5
		Uso no previsto	4	4	10
		[Re-]encaminamiento de mensajes	5	0	0
		Alteración de secuencia	0	2	0
		Acceso no autorizado	11.25	7.5	0
		Modificación de la información	0	11.25	0
		Manipulación de programas	7.5	7.5	5
	Linux Ubuntu Server 11.10	Avería de origen físico o lógico	0	0	11.25
		Errores de los usuarios	7.5	11.25	7.5
		Errores del administrador	7.5	7.5	7.5
		Difusión de software dañino	15	15	15
		Destrucción de información	0	0	15
		Fugas de información	11.25	0	0
		Vulnerabilidades de los programas (software)	15	15	15
		Errores de mantenimiento / actualización de programas (software)	0	11.25	3
		Suplantación de la identidad del usuario	7.5	7.5	0
		Abuso de privilegios de acceso	3	11.25	7.5
		Uso no previsto	4	4	10
		[Re-]encaminamiento de mensajes	5	0	0
		Alteración de secuencia	0	2	0
		Acceso no autorizado	11.25	7.5	0
		Modificación de la información	0	11.25	0
		Manipulación de programas	7.5	7.5	5
	Apache Web Server	Avería de origen físico o lógico	0	0	9
		Errores de los usuarios	6	9	6
		Errores del administrador	6	6	6
		Difusión de software dañino	12	12	12
		Destrucción de información	0	0	12
		Fugas de información	9	0	0
		Vulnerabilidades de los programas (software)	12	12	12
		Errores de mantenimiento / actualización de programas (software)	0	9	2.4
		Suplantación de la identidad del usuario	6	6	0
		Abuso de privilegios de acceso	2.4	9	6
		Uso no previsto	3.2	3.2	8
		[Re-]encaminamiento de mensajes	4	0	0
		Alteración de secuencia	0	1.6	0
		Acceso no autorizado	9	6	0
		Modificación de la información	0	9	0

		Manipulación de programas	6	6	4
	Windows 8.1	Avería de origen físico o lógico	0	0	6.75
		Errores de los usuarios	4.5	6.75	4.5
		Errores del administrador	4.5	4.5	4.5
		Difusión de software dañino	9	9	9
		Destrucción de información	0	0	9
		Fugas de información	6.75	0	0
		Vulnerabilidades de los programas (software)	9	9	9
		Errores de mantenimiento / actualización de programas (software)	0	6.75	1.8
		Suplantación de la identidad del usuario	4.5	4.5	0
		Abuso de privilegios de acceso	1.8	6.75	4.5
		Uso no previsto	2.4	2.4	6
		[Re-]encaminamiento de mensajes	3	0	0
		Alteración de secuencia	0	1.2	0
		Acceso no autorizado	6.75	4.5	0
		Modificación de la información	0	6.75	0
		Manipulación de programas	4.5	4.5	3
	Aplicación Gestión Bancaria	Avería de origen físico o lógico	0	0	11.25
		Errores de los usuarios	7.5	11.25	7.5
		Errores del administrador	7.5	7.5	7.5
		Difusión de software dañino	15	15	15
		Destrucción de información	0	0	15
		Fugas de información	11.25	0	0
		Vulnerabilidades de los programas (software)	15	15	15
		Errores de mantenimiento / actualización de programas (software)	0	11.25	3
		Suplantación de la identidad del usuario	7.5	7.5	0
		Abuso de privilegios de acceso	3	11.25	7.5
		Uso no previsto	4	4	10
		[Re-]encaminamiento de mensajes	5	0	0
		Alteración de secuencia	0	2	0
		Acceso no autorizado	11.25	7.5	0
		Modificación de la información	0	11.25	0
		Manipulación de programas	7.5	7.5	5
	SGBD Oracle 10g	Avería de origen físico o lógico	0	0	11.25
		Errores de los usuarios	7.5	11.25	7.5
		Errores del administrador	7.5	7.5	7.5
		Difusión de software dañino	15	15	15
		Destrucción de información	0	0	15
		Fugas de información	11.25	0	0
		Vulnerabilidades de los programas (software)	15	15	15
		Errores de mantenimiento / actualización de programas (software)	0	11.25	3
		Suplantación de la identidad del usuario	7.5	7.5	0
		Abuso de privilegios de acceso	3	11.25	7.5
		Uso no previsto	4	4	10
		[Re-]encaminamiento de mensajes	5	0	0
		Alteración de secuencia	0	2	0
		Acceso no autorizado	11.25	7.5	0

		Modificación de la información	0	11.25	0
		Manipulación de programas	7.5	7.5	5
	ESET Smart Security 8	Avería de origen físico o lógico	0	0	6.75
		Errores de los usuarios	4.5	6.75	4.5
		Errores del administrador	4.5	4.5	4.5
		Difusión de software dañino	9	9	9
		Destrucción de información	0	0	9
		Fugas de información	6.75	0	0
		Vulnerabilidades de los programas (software)	9	9	9
		Errores de mantenimiento / actualización de programas (software)	0	6.75	1.8
		Suplantación de la identidad del usuario	4.5	4.5	0
		Abuso de privilegios de acceso	1.8	6.75	4.5
		Uso no previsto	2.4	2.4	6
		[Re-]encaminamiento de mensajes	3	0	0
		Alteración de secuencia	0	1.2	0
		Acceso no autorizado	6.75	4.5	0
		Modificación de la información	0	6.75	0
		Manipulación de programas	4.5	4.5	3
	Windows XP Embedded	Avería de origen físico o lógico	0	0	9
		Errores de los usuarios	6	9	6
		Errores del administrador	6	6	6
		Difusión de software dañino	12	12	12
		Destrucción de información	0	0	12
		Fugas de información	9	0	0
		Vulnerabilidades de los programas (software)	12	12	12
		Errores de mantenimiento / actualización de programas (software)	0	9	2.4
		Suplantación de la identidad del usuario	6	6	0
		Abuso de privilegios de acceso	2.4	9	6
		Uso no previsto	3.2	3.2	8
		[Re-]encaminamiento de mensajes	4	0	0
		Alteración de secuencia	0	1.6	0
		Acceso no autorizado	9	6	0
		Modificación de la información	0	9	0
		Manipulación de programas	6	6	4
	Herramienta Amanda para backup	Avería de origen físico o lógico	0	0	6.75
		Errores de los usuarios	4.5	6.75	4.5
		Errores del administrador	4.5	4.5	4.5
		Difusión de software dañino	9	9	9
		Destrucción de información	0	0	9
		Fugas de información	6.75	0	0
		Vulnerabilidades de los programas (software)	9	9	9
		Errores de mantenimiento / actualización de programas (software)	0	6.75	1.8
		Suplantación de la identidad del usuario	4.5	4.5	0
		Abuso de privilegios de acceso	1.8	6.75	4.5
		Uso no previsto	2.4	2.4	6
		[Re-]encaminamiento de mensajes	3	0	0
		Alteración de secuencia	0	1.2	0

		Acceso no autorizado	6.75	4.5	0
		Modificación de la información	0	6.75	0
		Manipulación de programas	4.5	4.5	3
S	Servicios de banca online	Errores de los usuarios	8	12	3.2
		Errores del administrador	6	4	4
		Destrucción de información	0	0	6
		Fugas de información	12	0	0
		Caída del sistema por agotamiento de recursos	0	0	12
		Suplantación de la identidad del usuario	16	12	0
		Abuso de privilegios de acceso	4	6	1.6
		Uso no previsto	2.4	2.4	6
		[Re-]encaminamiento de mensajes	6	0	0
		Alteración de secuencia	0	6	0
		Acceso no autorizado	8	6	0
		Repudio	0	3	0
		Modificación de la información	0	6	0
		Denegación de servicio	0	0	12
P	Director General	Deficiencias en la organización	0	0	6
		Fugas de información	8	0	0
		Indisponibilidad del personal	0	0	12
		Extorsión	9	6	6
		Ingeniería social (picaresca)	16	8	3.2
	Directores sucursales	Deficiencias en la organización	0	0	4.5
		Fugas de información	6	0	0
		Indisponibilidad del personal	0	0	9
		Extorsión	6.75	4.5	4.5
		Ingeniería social (picaresca)	12	6	2.4
	Empleados sucursales	Deficiencias en la organización	0	0	3
		Fugas de información	4	0	0
		Indisponibilidad del personal	0	0	6
		Extorsión	4.5	3	3
		Ingeniería social (picaresca)	8	4	1.6
	Jefe Departamento de TI	Deficiencias en la organización	0	0	6
		Fugas de información	8	0	0
		Indisponibilidad del personal	0	0	12
		Extorsión	9	6	6
		Ingeniería social (picaresca)	16	8	3.2
	Responsables de seguridad	Deficiencias en la organización	0	0	4.5
		Fugas de información	6	0	0
		Indisponibilidad del personal	0	0	9
		Extorsión	6.75	4.5	4.5
		Ingeniería social (picaresca)	12	6	2.4
	Técnicos/desarrollado-res	Deficiencias en la organización	0	0	3
		Fugas de información	4	0	0
		Indisponibilidad del personal	0	0	6
		Extorsión	4.5	3	3
		Ingeniería social (picaresca)	8	4	1.6
L	Sede central	Fuego	0	0	7.5
		Daños por agua	0	0	5
		Desastres naturales	0	0	5
		Emanaciones electromagnéticas	0.25	0	0
		Destrucción de información	0	0	0.25

		Fugas de información	7.5	0	0
		Uso no previsto	0.5	2	2
		Acceso no autorizado	11.25	11.25	0
		Modificación de la información	0	3	0
		Ataque destructivo	0	0	7.5
		Ocupación enemiga	3.75	0	5
	Sucursales	Fuego	0	0	6
		Daños por agua	0	0	4
		Desastres naturales	0	0	4
		Emanaciones electromagnéticas	0.2	0	0
		Destrucción de información	0	0	0.2
		Fugas de información	6	0	0
		Uso no previsto	0.4	1.6	1.6
		Acceso no autorizado	9	9	0
		Modificación de la información	0	2.4	0
		Ataque destructivo	0	0	6
		Ocupación enemiga	3	0	4

Tabla 4-4: Valores de riesgo potencial para los activos de la organización

4.4 APLICACIÓN DE CONTROLES

Conocidos los valores de riesgo potencial para los activos de la organización, y el umbral de riesgo aceptable definido por la dirección, el siguiente paso consiste en aplicar los controles o salvaguardas pertinentes para las amenazas cuyos valores de riesgo potencial superan dicho umbral.

Como se estableció en la metodología de análisis de riesgos, los controles utilizados serán los recogidos en la norma ISO/IEC 27002:2005 [3]. La aplicación de controles consistirá en implementar los controles que ayuden a mitigar los riesgos para cada una de las amenazas, o bien, mejorar el nivel de implantación actual de un determinado control. En la Tabla 4-5 se recoge la relación de controles aplicados a cada una de las amenazas en cuestión para una determinada categoría de activos, junto con su estado actual, el estado que se pretende alcanzar, la probabilidad de ocurrencia para la amenaza tras la aplicación o mejora del control (probabilidad de ocurrencia residual) y el impacto de la amenaza en las tres dimensiones de la seguridad tras la aplicación o mejora del control (impacto residual). Estos datos permitirán, posteriormente, realizar el cálculo del riesgo residual de los activos de la organización.

Categoría de activo	Amenaza	Control	E. Actual	E. Objetivo	P. Ocurrencia residual	Impacto residual		
						C	I	D
D	Fugas de información	5.1.1 Documento de política de seguridad de la información	1 - Inicial	2 - Repetible	Baja (B)	50%		
		5.1.2 Revisión	1 - Inicial	2 -				

		de la política de seguridad de la información		Repetible				
		6.1.5 Acuerdos de confidencialidad	2 - Repetible	3 - Definido				
		7.1.1 Inventario de activos	3 - Definido	4 - Gestionado				
		8.2.2 Concienciación, formación y capacitación en seguridad de la información	1 - Inicial	2 - Repetible				
		8.2.3 Proceso disciplinario	0 - Inexistente	1 - Inicial				
	Suplantación de la identidad del usuario	8.3.3 Retirada de los derechos de acceso	4 - Gestionado	5 - Optimizado	Baja (B)	50%	50%	
		11.2.2 Gestión de privilegios	4 - Gestionado	5 - Optimizado				
		11.2.3 Gestión de contraseñas de usuario	4 - Gestionado	5 - Optimizado				
		11.2.4 Revisión de los derechos de acceso de usuario	0 - Inexistente	1 - Inicial				
		11.3.1 Uso de contraseñas	3 - Definido	4 - Gestionado				
		11.3.2 Equipo de usuario desatendido	3 - Definido	4 - Gestionado				
		11.4.1 Política de uso de los servicios en red	3 - Definido	4 - Gestionado				
		11.4.2 Autenticación de usuario para conexiones externas	4 - Gestionado	5 - Optimizado				
		11.5.1 Procedimientos seguros de inicio de sesión	4 - Gestionado	5 - Optimizado				
		11.5.2 Identificación y autenticación de usuario	3 - Definido	4 - Gestionado				
		11.5.5 Desconexión automática de sesión	3 - Definido	4 - Gestionado				
		11.6.1	4 -	5 -				

		Restricción del acceso a la información	Gestionado	Optimizado				
	Abuso de privilegios de acceso	8.3.3 Retirada de los derechos de acceso	4 - Gestionado	5 - Optimizado	Baja (B)	50%	50%	20%
		11.1.1 Política de control de acceso	4 - Gestionado	5 - Optimizado				
		11.2.2 Gestión de privilegios	4 - Gestionado	5 - Optimizado				
		11.2.4 Revisión de los derechos de acceso de usuario	0 - Inexistente	1 - Inicial				
		11.6.1 Restricción del acceso a la información	4 - Gestionado	5 - Optimizado				
	Modificación de la información	10.1.2 Gestión de cambios	3 - Definido	4 - Gestionado	Baja (B)		50%	
		10.5.1 Copias de seguridad de la información	4 - Gestionado	5 - Optimizado				
		10.8.1 Políticas y procedimientos de intercambio de información	4 - Gestionado	5 - Optimizado				
		10.8.3 Soportes físicos en tránsito	3 - Definido	4 - Gestionado				
		10.8.5 Sistemas de información empresariales	4 - Gestionado	5 - Optimizado				
		11.6.1 Restricción del acceso a la información	4 - Gestionado	5 - Optimizado				
COM	Caída del sistema por agotamiento de recursos	10.3.1 Gestión de capacidades	4 - Gestionado	5 - Optimizado	Baja (B)			50%
		10.3.2 Aceptación del sistema	4 - Gestionado	5 - Optimizado				
	Suplantación de la identidad del usuario	8.3.3 Retirada de los derechos de acceso	4 - Gestionado	5 - Optimizado	Baja (B)	50%	50%	
		11.2.2 Gestión de privilegios	4 - Gestionado	5 - Optimizado				
		11.2.3 Gestión de contraseñas de usuario	4 - Gestionado	5 - Optimizado				
		11.2.4 Revisión de los derechos	0 - Inexistente	1 - Inicial				

		de acceso de usuario						
		11.3.1 Uso de contraseñas	3 - Definido	4 - Gestionado				
		11.3.2 Equipo de usuario desatendido	3 - Definido	4 - Gestionado				
		11.4.1 Política de uso de los servicios en red	3 - Definido	4 - Gestionado				
		11.4.2 Autenticación de usuario para conexiones externas	4 - Gestionado	5 - Optimizado				
		11.5.1 Procedimientos seguros de inicio de sesión	4 - Gestionado	5 - Optimizado				
		11.5.2 Identificación y autenticación de usuario	3 - Definido	4 - Gestionado				
		11.5.5 Desconexión automática de sesión	3 - Definido	4 - Gestionado				
		11.6.1 Restricción del acceso a la información	4 - Gestionado	5 - Optimizado				
	Uso no previsto	5.1.1 Documento de política de seguridad de la información	1 - Inicial	2 - Repetible	Media (M)	5%	5%	20%
		7.1.3 Uso aceptable de los activos	3 - Definido	4 - Gestionado				
		8.3.2 Proceso disciplinario	0 - Inexistente	1 - Inicial				
		10.10.1 Registros de auditoría	2 - Repetible	3 - Definido				
		10.10.2 Supervisión del uso del sistema	3 - Definido	4 - Gestionado				
		10.10.4 Registros de administración y operación	2 - Repetible	3 - Definido				
	Acceso no autorizado	11.1.1 Política de control de acceso	4 - Gestionado	5 - Optimizado	Baja (B)	50%	50%	

		11.2.2 Gestión de privilegios	4 - Gestionado	5 - Optimizado				
		11.3.1 Uso de contraseñas	3 - Definido	4 - Gestionado				
		11.4.1 Política de uso de los servicios en red	3 - Definido	4 - Gestionado				
		11.4.2 Autenticación de usuario para conexiones externas	4 - Gestionado	5 - Optimizado				
		11.4.6 Control de la conexión a la red	4 - Gestionado	5 - Optimizado				
		11.5.1 Procedimientos seguros de inicio de sesión	4 - Gestionado	5 - Optimizado				
		11.5.2 Identificación y autenticación de usuario	3 - Definido	4 - Gestionado				
		11.5.4 Uso de los recursos del sistema	3 - Definido	4 - Gestionado				
		11.7.1 Ordenadores portátiles y comunicaciones móviles	2 - Repetible	3 - Definido				
		11.7.2 Teletrabajo	1 - Inicial	2 - Repetible				
	Modificación de la información	10.1.2 Gestión de cambios	3 - Definido	4 - Gestionado	Baja (B)		50%	
		10.5.1 Copias de seguridad de la información	4 - Gestionado	5 - Optimizado				
		10.8.1 Políticas y procedimientos de intercambio de información	4 - Gestionado	5 - Optimizado				
		10.8.3 Soportes físicos en tránsito	3 - Definido	4 - Gestionado				
		10.8.5 Sistemas de información empresariales	4 - Gestionado	5 - Optimizado				
		11.6.1 Restricción del acceso a la información	4 - Gestionado	5 - Optimizado				
	Denegación de	9.2.1	3 -	4 -	Baja (B)			75%

	servicio	Emplazamiento y protección de equipos	Definido	Gestionado				
		9.2.2 Instalaciones de suministro	3 - Definido	4 - Gestionado				
		9.2.4 Mantenimiento de los equipos	4 - Gestionado	5 - Optimizado				
		13.1.1 Notificación de eventos de seguridad de la información	3 - Definido	4 - Gestionado				
		13.2.2 Aprendizaje de los incidentes de seguridad de la información	1 - Inicial	2 - Repetible				
		13.2.3 Recopilación de evidencias	3 - Definido	4 - Gestionado				
		14.1.1 Inclusión de la seguridad de la información en el proceso de gestión de la continuidad del negocio	3 - Definido	4 - Gestionado				
HW	Contaminación mecánica	9.2.1 Emplazamiento y protección de equipos	3 - Definido	4 - Gestionado	Media (M)			20%
		9.2.4 Mantenimiento de los equipos	4 - Gestionado	5 - Optimizado				
	Avería de origen físico o lógico	9.2.4 Mantenimiento de los equipos	4 - Gestionado	5 - Optimizado	Media (M)			50%
		9.2.5 Seguridad de los equipos fuera de las instalaciones	1 - Inicial	2 - Repetible				
		12.4.3 Control de acceso al código fuente de los programas	4 - Gestionado	5 - Optimizado				
		12.5.2 Revisión técnica de las aplicaciones tras efectuar cambios en el sistema	4 - Gestionado	5 - Optimizado				

		operativo						
		12.5.5 Externalización del desarrollo del software	3 - Definido	4 - Gestionado				
		12.6.1 Control de las vulnerabilidades técnicas	3 - Definido	4 - Gestionado				
	Corte del suministro eléctrico	9.2.2 Instalaciones de suministro	3 - Definido	4 - Gestionado	Media (M)			50%
		10.3.1 Gestión de capacidades	4 - Gestionado	5 - Optimizado				
		14.1.2 Continuidad del negocio y evaluación de riesgos	2 - Repetible	3 - Definido				
		14.1.3 Desarrollo e implantación de planes de continuidad que incluyan la seguridad de la información	2 - Repetible	3 - Definido				
	Caída del sistema por agotamiento de recursos	10.3.1 Gestión de capacidades	4 - Gestionado	5 - Optimizado	Baja (B)			50%
		10.3.2 Aceptación del sistema	4 - Gestionado	5 - Optimizado				
	Pérdida de equipos	7.1.1 Inventario de activos	3 - Definido	4 - Gestionado	Baja (B)	20%		75%
		7.1.2 Propiedad de los activos	3 - Definido	4 - Gestionado				
		7.1.3 Uso aceptable de los activos	3 - Definido	4 - Gestionado				
		8.2.2 Concienciación, formación y capacitación en seguridad de la información	1 - Inicial	2 - Repetible				
		8.2.3 Proceso disciplinario	0 - Inexistente	1 - Inicial				
		8.3.2 Devolución de activos	4 - Gestionado	5 - Optimizado				
		10.7.1 Gestión de soportes extraíbles	1 - Inicial	2 - Repetible				
		10.7.2 Retirada	2 -	3 -				

		de soportes	Repetible	Definido				
		10.7.3 Procedimientos de manipulación de la información	3 - Definido	4 - Gestionado				
		10.8.3 Soportes físicos en tránsito	3 - Definido	4 - Gestionado				
	Uso no previsto	5.1.1 Documento de política de seguridad de la información	1 - Inicial	2 - Repetible	Media (M)	5%	5%	20%
		7.1.3 Uso aceptable de los activos	3 - Definido	4 - Gestionado				
		8.3.2 Proceso disciplinario	0 - Inexistente	1 - Inicial				
		10.10.1 Registros de auditoría	2 - Repetible	3 - Definido				
		10.10.2 Supervisión del uso del sistema	3 - Definido	4 - Gestionado				
		10.10.4 Registros de administración y operación	2 - Repetible	3 - Definido				
	Denegación de servicio	9.2.1 Emplazamiento y protección de equipos	3 - Definido	4 - Gestionado	Baja (B)			75%
		9.2.2 Instalaciones de suministro	3 - Definido	4 - Gestionado				
		9.2.4 Mantenimiento de los equipos	4 - Gestionado	5 - Optimizado				
		13.1.1 Notificación de eventos de seguridad de la información	3 - Definido	4 - Gestionado				
		13.2.2 Aprendizaje de los incidentes de seguridad de la información	1 - Inicial	2 - Repetible				
		13.2.3 Recopilación de evidencias	3 - Definido	4 - Gestionado				
		14.1.1 Inclusión de la seguridad	3 - Definido	4 - Gestionado				

		de la información en el proceso de gestión de la continuidad del negocio						
	Robo	7.1.1 Inventario de activos	3 - Definido	4 - Gestionado	Baja (B)	20%		75%
		9.1.3 Seguridad de oficinas, despachos e instalaciones	4 - Gestionado	5 - Optimizado				
		9.1.6 Áreas de acceso público y de carga y descarga	4 - Gestionado	5 - Optimizado				
		9.2.1 Emplazamiento y protección de equipos	3 - Definido	4 - Gestionado				
		9.2.5 Seguridad de los equipos fuera de las instalaciones	1 - Inicial	2 - Repetible				
		10.8.3 Soportes físicos en tránsito	3 - Definido	4 - Gestionado				
SW	Avería de origen físico o lógico	9.2.4 Mantenimiento de los equipos	4 - Gestionado	5 - Optimizado	Media (M)			50%
		9.2.5 Seguridad de los equipos fuera de las instalaciones	1 - Inicial	2 - Repetible				
		12.4.3 Control de acceso al código fuente de los programas	4 - Gestionado	5 - Optimizado				
		12.5.2 Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo	4 - Gestionado	5 - Optimizado				
		12.5.5 Externalización del desarrollo del software	3 - Definido	4 - Gestionado				
		12.6.1 Control de las vulnerabilidades técnicas	3 - Definido	4 - Gestionado				
	Errores de los	8.2.2	1 - Inicial	2 -	Baja (B)	20%	50%	20%

	usuarios	Concienciación, formación y capacitación en seguridad de la información		Repetible				
		10.1.1 Documentación de los procedimientos de operación	3 - Definido	4 - Gestionado				
		10.1.2 Gestión de cambios	3 - Definido	4 - Gestionado				
		10.1.3 Segregación de tareas	4 - Gestionado	5 - Optimizado				
		10.1.4 Separación de los recursos de desarrollo, prueba y operación	3 - Definido	4 - Gestionado				
		10.5.1 Copias de seguridad de la información	4 - Gestionado	5 - Optimizado				
		12.2.1 Validación de los datos de entrada	4 - Gestionado	5 - Optimizado				
	Difusión de software dañino	8.2.2 Concienciación, formación y capacitación en seguridad de la información	1 - Inicial	2 - Repetible	Media (M)	50%	50%	50%
		8.2.3 Proceso disciplinario	0 - Inexistente	1 - Inicial				
		8.3.3 Retirada de los derechos de acceso	4 - Gestionado	5 - Optimizado				
		10.4.1 Controles contra el código malicioso	4 - Gestionado	5 - Optimizado				
		10.4.2 Controles contra el código descargado en el cliente	3 - Definido	4 - Gestionado				
		13.1.1 Notificación de eventos de seguridad de la información	3 - Definido	4 - Gestionado				
		13.2.2 Aprendizaje de los incidentes de	1 - Inicial	2 - Repetible				

		seguridad de la información						
		14.1.2 Continuidad del negocio y evaluación de riesgos	2 - Repetible	3 - Definido				
	Destrucción de información	8.2.2 Concienciación, formación y capacitación en seguridad de la información	1 - Inicial	2 - Repetible	Baja (B)			50%
		8.2.3 Proceso disciplinario	0 - Inexistente	1 - Inicial				
		8.3.2 Devolución de activos	4 - Gestionado	5 - Optimizado				
		10.1.1 Documentación de los procedimientos de operación	3 - Definido	4 - Gestionado				
		10.1.2 Gestión de cambios	3 - Definido	4 - Gestionado				
		10.1.3 Segregación de tareas	4 - Gestionado	5 - Optimizado				
		10.1.4 Separación de los recursos de desarrollo, prueba y operación	3 - Definido	4 - Gestionado				
		10.5.1 Copias de seguridad de la información	4 - Gestionado	5 - Optimizado				
	Fugas de información	5.1.1 Documento de política de seguridad de la información	1 - Inicial	2 - Repetible	Baja (B)	50%		
		6.1.5 Acuerdos de confidencialidad	2 - Repetible	3 - Definido				
		8.1.3 Términos y condiciones de contratación	4 - Gestionado	5 - Optimizado				
		8.2.2 Concienciación, formación y capacitación en seguridad de la información	1 - Inicial	2 - Repetible				

		8.2.3 Proceso disciplinario	0 - Inexistente	1 - Inicial				
		8.3.3 Retirada de los derechos de acceso	4 - Gestionado	5 - Optimizado				
		12.5.4 Fugas de información	4 - Gestionado	5 - Optimizado				
	Vulnerabilidades de los programas	12.2.1 Validación de los datos de entrada	4 - Gestionado	5 - Optimizado	Media (M)	50%	50%	50%
		12.2.2 Control del procesamiento interno	4 - Gestionado	5 - Optimizado				
		12.2.3 Integridad de los mensajes	2 - Repetible	3 - Definido				
		12.2.4 Validación de los datos de salida	2 - Repetible	3 - Definido				
		12.6.1 Control de las vulnerabilidades técnicas	3 - Definido	4 - Gestionado				
	Errores de mantenimiento / actualización de programas (software)	12.5.1 Procedimientos de control de cambios	2 - Repetible	3 - Definido	Baja (B)		50%	20%
		12.5.2 Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo	4 - Gestionado	5 - Optimizado				
	Abuso de privilegios de acceso	8.3.3 Retirada de los derechos de acceso	4 - Gestionado	5 - Optimizado	Baja (B)	5%	50%	5%
		11.1.1 Política de control de acceso	4 - Gestionado	5 - Optimizado				
		11.2.2 Gestión de privilegios	4 - Gestionado	5 - Optimizado				
		11.2.4 Revisión de los derechos de acceso de usuario	0 - Inexistente	1 - Inicial				
		11.6.1 Restricción del acceso a la información	4 - Gestionado	5 - Optimizado				
	Uso no previsto	5.1.1	1 - Inicial	2 -	Media (M)	5%	5%	20%

		Documento de política de seguridad de la información		Repetible				
		7.1.3 Uso aceptable de los activos	3 - Definido	4 - Gestionado				
		8.3.2 Proceso disciplinario	0 - Inexistente	1 - Inicial				
		10.10.1 Registros de auditoría	2 - Repetible	3 - Definido				
		10.10.2 Supervisión del uso del sistema	3 - Definido	4 - Gestionado				
		10.10.4 Registros de administración y operación	2 - Repetible	3 - Definido				
	Acceso no autorizado	11.1.1 Política de control de acceso	4 - Gestionado	5 - Optimizado	Baja (B)	50%	20%	
		11.2.2 Gestión de privilegios	4 - Gestionado	5 - Optimizado				
		11.3.1 Uso de contraseñas	3 - Definido	4 - Gestionado				
		11.4.1 Política de uso de los servicios en red	3 - Definido	4 - Gestionado				
		11.4.2 Autenticación de usuario para conexiones externas	4 - Gestionado	5 - Optimizado				
		11.4.6 Control de la conexión a la red	4 - Gestionado	5 - Optimizado				
		11.5.1 Procedimientos seguros de inicio de sesión	4 - Gestionado	5 - Optimizado				
		11.5.2 Identificación y autenticación de usuario	3 - Definido	4 - Gestionado				
		11.5.4 Uso de los recursos del sistema	3 - Definido	4 - Gestionado				
		11.7.1 Ordenadores portátiles y comunicaciones móviles	2 - Repetible	3 - Definido				
		11.7.2	1 - Inicial	2 -				

		Teletrabajo		Repetible				
	Modificación de la información	10.1.2 Gestión de cambios	3 - Definido	4 - Gestionado	Baja (B)		50%	
		10.5.1 Copias de seguridad de la información	4 - Gestionado	5 - Optimizado				
		10.8.1 Políticas y procedimientos de intercambio de información	4 - Gestionado	5 - Optimizado				
		10.8.3 Soportes físicos en tránsito	3 - Definido	4 - Gestionado				
		10.8.5 Sistemas de información empresariales	4 - Gestionado	5 - Optimizado				
		11.6.1 Restricción del acceso a la información	4 - Gestionado	5 - Optimizado				
S	Errores de los usuarios	8.2.2 Concienciación, formación y capacitación en seguridad de la información	1 - Inicial	2 - Repetible	Media (M)	20%	50%	5%
		10.1.1 Documentación de los procedimientos de operación	3 - Definido	4 - Gestionado				
		10.1.2 Gestión de cambios	3 - Definido	4 - Gestionado				
		10.1.3 Segregación de tareas	4 - Gestionado	5 - Optimizado				
		10.1.4 Separación de los recursos de desarrollo, prueba y operación	3 - Definido	4 - Gestionado				
		10.5.1 Copias de seguridad de la información	4 - Gestionado	5 - Optimizado				
		12.2.1 Validación de los datos de entrada	4 - Gestionado	5 - Optimizado				
	Fugas de información	5.1.1 Documento de política de seguridad de la	1 - Inicial	2 - Repetible	Media (M)	50%		

		información						
		6.1.5 Acuerdos de confidencialidad	2 - Repetible	3 - Definido				
		8.1.3 Términos y condiciones de contratación	4 - Gestionado	5 - Optimizado				
		8.2.2 Concienciación, formación y capacitación en seguridad de la información	1 - Inicial	2 - Repetible				
		8.2.3 Proceso disciplinario	0 - Inexistente	1 - Inicial				
		8.3.3 Retirada de los derechos de acceso	4 - Gestionado	5 - Optimizado				
		12.5.4 Fugas de información	4 - Gestionado	5 - Optimizado				
	Caídas del sistema por agotamiento de recursos	10.3.1 Gestión de capacidades	4 - Gestionado	5 - Optimizado	Baja (B)			75%
		10.3.2 Aceptación del sistema	4 - Gestionado	5 - Optimizado				
	Suplantación de la identidad del usuario	8.3.3 Retirada de los derechos de acceso	4 - Gestionado	5 - Optimizado	Baja (B)	75%	50%	
		11.2.2 Gestión de privilegios	4 - Gestionado	5 - Optimizado				
		11.2.3 Gestión de contraseñas de usuario	4 - Gestionado	5 - Optimizado				
		11.2.4 Revisión de los derechos de acceso de usuario	0 - Inexistente	1 - Inicial				
		11.3.1 Uso de contraseñas	3 - Definido	4 - Gestionado				
		11.3.2 Equipo de usuario desatendido	3 - Definido	4 - Gestionado				
		11.4.1 Política de uso de los servicios en red	3 - Definido	4 - Gestionado				
		11.4.2 Autenticación de usuario para conexiones externas	4 - Gestionado	5 - Optimizado				
		11.5.1 Procedimientos seguros de inicio de sesión	4 - Gestionado	5 - Optimizado				

		11.5.2 Identificación y autenticación de usuario	3 - Definido	4 - Gestionado				
		11.5.5 Desconexión automática de sesión	3 - Definido	4 - Gestionado				
	Acceso no autorizado	11.1.1 Política de control de acceso	4 - Gestionado	5 - Optimizado	Baja (B)	75%	50%	
		11.2.2 Gestión de privilegios	4 - Gestionado	5 - Optimizado				
		11.3.1 Uso de contraseñas	3 - Definido	4 - Gestionado				
		11.4.1 Política de uso de los servicios en red	3 - Definido	4 - Gestionado				
		11.4.2 Autenticación de usuario para conexiones externas	4 - Gestionado	5 - Optimizado				
		11.4.6 Control de la conexión a la red	4 - Gestionado	5 - Optimizado				
		11.5.1 Procedimientos seguros de inicio de sesión	4 - Gestionado	5 - Optimizado				
		11.5.2 Identificación y autenticación de usuario	3 - Definido	4 - Gestionado				
		11.5.4 Uso de los recursos del sistema	3 - Definido	4 - Gestionado				
		11.7.1 Ordenadores portátiles y comunicaciones móviles	2 - Repetible	3 - Definido				
		11.7.2 Teletrabajo	1 - Inicial	2 - Repetible				
	Denegación de servicio	9.2.1 Emplazamiento y protección de equipos	3 - Definido	4 - Gestionado	Baja (B)			75%
		9.2.2 Instalaciones de suministro	3 - Definido	4 - Gestionado				
		9.2.4 Mantenimiento de los equipos	4 - Gestionado	5 - Optimizado				

		13.1.1 Notificación de eventos de seguridad de la información	3 - Definido	4 - Gestionado				
		13.2.2 Aprendizaje de los incidentes de seguridad de la información	1 - Inicial	2 - Repetible				
		13.2.3 Recopilación de evidencias	3 - Definido	4 - Gestionado				
		14.1.1 Inclusión de la seguridad de la información en el proceso de gestión de la continuidad del negocio	3 - Definido	4 - Gestionado				
P	Fugas de información	5.1.1 Documento de política de seguridad de la información	1 - Inicial	2 - Repetible	Baja (B)	75%		
		6.1.5 Acuerdos de confidencialidad	2 - Repetible	3 - Definido				
		8.1.3 Términos y condiciones de contratación	4 - Gestionado	5 - Optimizado				
		8.2.2 Concienciación, formación y capacitación en seguridad de la información	1 - Inicial	2 - Repetible				
		8.2.3 Proceso disciplinario	0 - Inexistente	1 - Inicial				
		8.3.3 Retirada de los derechos de acceso	4 - Gestionado	5 - Optimizado				
		12.5.4 Fugas de información	4 - Gestionado	5 - Optimizado				
	Indisponibilidad del personal	8.1.1 Funciones y responsabilida-des	4 - Gestionado	5 - Optimizado	Baja (B)			75%
		8.1.2 Investigación de antecedentes	4 - Gestionado	5 - Optimizado				
		8.1.3 Términos y condiciones de	4 - Gestionado	5 - Optimizado				

		contratación						
		8.2.3 Proceso disciplinario	0 - Inexistente	1 - Inicial				
	Extorsión	11.2.2 Gestión de privilegios	4 - Gestionado	5 - Optimizado	Media (M)	50%	20%	20%
		11.2.4 Revisión de los derechos de acceso de usuario	0 - Inexistente	1 - Inicial				
	Ingeniería social (picaresca)	5.1.1 Documento de política de seguridad de la información	1 - Inicial	2 - Repetible	Media (M)	50%	50%	5%
		6.1.5 Acuerdos de confidencialidad	2 - Repetible	3 - Definido				
		8.2.2 Concienciación, formación y capacitación en seguridad de la información	1 - Inicial	2 - Repetible				
L	Acceso no autorizado	9.1.3 Seguridad de oficinas, despachos e instalaciones	4 - Gestionado	5 - Optimizado	Baja (B)	50%	50%	
		9.1.5 Trabajo en áreas seguras	4 - Gestionado	5 - Optimizado				
		9.1.6 Áreas de acceso público y de carga y descarga	4 - Gestionado	5 - Optimizado				

Tabla 4-5: Aplicación de controles

4.5 CÁLCULO DEL RIESGO RESIDUAL

Una vez aplicados los controles o salvaguardas sobre las amenazas que provocaban unos valores de riesgo sobre los activos superiores al umbral establecido por la organización, el siguiente y último paso es calcular de nuevo el riesgo al que siguen sometidos dichos activos, el riesgo residual. La manera de calcular este riesgo será la misma que la seguida para el riesgo potencial, con la diferencia de que esta vez los valores de probabilidad de frecuencia de la amenaza e impacto serán distintos para las amenazas en las que se han aplicado controles, por lo tanto, el riesgo que provocarán éstas será menor y quedará por debajo del umbral de riesgo aceptable establecido.

De nuevo, los valores para el riesgo residual se presentarán en forma de tabla (Tabla 4-6), en la cual aparecerán para cada pareja activo-amenaza, sus valores de

riesgo residual en las dimensiones de confidencialidad, integridad y disponibilidad, RR_C, RR_I y RR_D, respectivamente.

Categoría	Activo	Amenaza	Riesgo residual		
			RR_C	RR_I	RR_D
D	BBDD clientes	Errores de los usuarios	7.5	7.5	3
		Errores del administrador	7.5	7.5	2
		Errores de monitorización (log)	0	5	0
		Errores de configuración	0	7.5	0
		Destrucción de información	0	0	7.5
		Fugas de información	5	0	0
		Manipulación de los registros de actividad (log)	0	5	0
		Manipulación de la configuración	7.5	7.5	7.5
		Suplantación de la identidad del usuario	5	5	0
		Abuso de privilegios de acceso	5	5	2
		Acceso no autorizado	7.5	7.5	0
		Repudio	0	7.5	0
		Modificación de la información	0	5	0
	BBDD información financiera	Errores de los usuarios	7.5	7.5	3
		Errores del administrador	7.5	7.5	2
		Errores de monitorización (log)	0	5	0
		Errores de configuración	0	7.5	0
		Destrucción de información	0	0	7.5
		Fugas de información	5	0	0
		Manipulación de los registros de actividad (log)	0	5	0
		Manipulación de la configuración	7.5	7.5	7.5
		Suplantación de la identidad del usuario	5	5	0
		Abuso de privilegios de acceso	5	5	2
		Acceso no autorizado	7.5	7.5	0
		Repudio	0	7.5	0
		Modificación de la información	0	5	0
	BBDD gestión empleados	Errores de los usuarios	7.5	7.5	3
		Errores del administrador	7.5	7.5	2
		Errores de monitorización (log)	0	5	0
		Errores de configuración	0	7.5	0
		Destrucción de información	0	0	7.5
		Fugas de información	5	0	0
		Manipulación de los registros de actividad (log)	0	5	0
		Manipulación de la configuración	7.5	7.5	7.5
		Suplantación de la identidad del usuario	5	5	0
		Abuso de privilegios de acceso	5	5	2
		Acceso no autorizado	7.5	7.5	0
		Repudio	0	7.5	0
		Modificación de la información	0	5	0
	Sistema de Gestión Documental	Errores de los usuarios	7.5	7.5	3
		Errores del administrador	7.5	7.5	2
		Errores de monitorización (log)	0	5	0
		Errores de configuración	0	7.5	0
		Destrucción de información	0	0	7.5
		Fugas de información	5	0	0

		Manipulación de los registros de actividad (log)	0	5	0
		Manipulación de la configuración	7.5	7.5	7.5
		Suplantación de la identidad del usuario	5	5	0
		Abuso de privilegios de acceso	5	5	2
		Acceso no autorizado	7.5	7.5	0
		Repudio	0	7.5	0
		Modificación de la información	0	5	0
COM	ISP primario	Fallo de servicios de comunicaciones	0	0	7.5
		Errores del administrador	7.5	7.5	5
		Destrucción de información	0	0	5
		Fugas de información	7.5	0	0
		Caída del sistema por agotamiento de recursos	0	0	5
		Suplantación de la identidad del usuario	5	5	0
		Abuso de privilegios de acceso	7.5	7.5	3
		Uso no previsto	0.75	0.75	3
		[Re-]encaminamiento de mensajes	7.5	0	0
		Alteración de secuencia	0	7.5	0
		Acceso no autorizado	5	5	0
		Análisis de tráfico	7.5	0	0
		Interceptación de información (escucha)	7.5	0	0
		Modificación de la información	0	5	0
		Denegación de servicio	0	0	7.5
	ISP secundario	Fallo de servicios de comunicaciones	0	0	3
		Errores del administrador	3	3	2
		Destrucción de información	0	0	2
		Fugas de información	3	0	0
		Caída del sistema por agotamiento de recursos	0	0	2
		Suplantación de la identidad del usuario	2	2	0
		Abuso de privilegios de acceso	3	3	1.2
		Uso no previsto	0.3	0.3	1.2
		[Re-]encaminamiento de mensajes	3	0	0
		Alteración de secuencia	0	3	0
		Acceso no autorizado	2	2	0
		Análisis de tráfico	3	0	0
		Interceptación de información (escucha)	3	0	0
		Modificación de la información	0	2	0
		Denegación de servicio	0	0	3
	Red LAN CPD	Fallo de servicios de comunicaciones	0	0	7.5
		Errores del administrador	7.5	7.5	5
		Destrucción de información	0	0	5
		Fugas de información	7.5	0	0
		Caída del sistema por agotamiento de recursos	0	0	5
		Suplantación de la identidad del usuario	5	5	0
		Abuso de privilegios de acceso	7.5	7.5	3
		Uso no previsto	0.75	0.75	3
		[Re-]encaminamiento de mensajes	7.5	0	0
		Alteración de secuencia	0	7.5	0
		Acceso no autorizado	5	5	0
		Análisis de tráfico	7.5	0	0

		Interceptación de información (escucha)	7.5	0	0
		Modificación de la información	0	5	0
		Denegación de servicio	0	0	7.5
	Red LAN sucursales	Fallo de servicios de comunicaciones	0	0	6
		Errores del administrador	6	6	4
		Destrucción de información	0	0	4
		Fugas de información	6	0	0
		Caída del sistema por agotamiento de recursos	0	0	4
		Suplantación de la identidad del usuario	4	4	0
		Abuso de privilegios de acceso	6	6	2.4
		Uso no previsto	0.6	0.6	2.4
		[Re-]encaminamiento de mensajes	6	0	0
		Alteración de secuencia	0	6	0
		Acceso no autorizado	4	4	0
		Análisis de tráfico	6	0	0
		Interceptación de información (escucha)	6	0	0
		Modificación de la información	0	4	0
		Denegación de servicio	0	0	6
	Redes WiFi	Fallo de servicios de comunicaciones	0	0	4.5
		Errores del administrador	4.5	4.5	3
		Destrucción de información	0	0	3
		Fugas de información	4.5	0	0
		Caída del sistema por agotamiento de recursos	0	0	3
		Suplantación de la identidad del usuario	3	3	0
		Abuso de privilegios de acceso	4.5	4.5	1.8
		Uso no previsto	0.45	0.45	1.8
		[Re-]encaminamiento de mensajes	4.5	0	0
		Alteración de secuencia	0	4.5	0
		Acceso no autorizado	3	3	0
		Análisis de tráfico	4.5	0	0
		Interceptación de información (escucha)	4.5	0	0
		Modificación de la información	0	3	0
		Denegación de servicio	0	0	4.5
HW	Servidor central	Fuego	0	0	7.5
		Daños por agua	0	0	5
		Desastres naturales	0	0	3.75
		Contaminación mecánica	0	0	3
		Contaminación electromagnética	0	0	2.5
		Avería de origen físico o lógico	0	0	7.5
		Corte del suministro eléctrico	0	0	7.5
		Condiciones inadecuadas de temperatura o humedad	0	0	5
		Interrupción de otros servicios y suministros esenciales	0	0	1
		Degradación de los soportes de almacenamiento de la información	0	0	3
		Emanaciones electromagnéticas	1	0	0
		Errores del administrador	7.5	5	7.5
		Fugas de información	7.5	0	0
		Errores de mantenimiento / actualización de equipos (hardware)	0	0	5

		Caída del sistema por agotamiento de recursos	0	0	5
		Pérdida de equipos	2	0	7.5
		Abuso de privilegios de acceso	7.5	7.5	3
		Uso no previsto	0.75	0.75	3
		Acceso no autorizado	7.5	5	0
		Manipulación de los equipos	5	0	7.5
		Denegación de servicio	0	0	7.5
		Robo	2	0	7.5
		Ataque destructivo	0	0	5
	Servidor banca online	Fuego	0	0	7.5
		Daños por agua	0	0	5
		Desastres naturales	0	0	3.75
		Contaminación mecánica	0	0	3
		Contaminación electromagnética	0	0	2.5
		Avería de origen físico o lógico	0	0	7.5
		Corte del suministro eléctrico	0	0	7.5
		Condiciones inadecuadas de temperatura o humedad	0	0	5
		Interrupción de otros servicios y suministros esenciales	0	0	1
		Degradación de los soportes de almacenamiento de la información	0	0	3
		Emanaciones electromagnéticas	1	0	0
		Errores del administrador	7.5	5	7.5
		Fugas de información	7.5	0	0
		Errores de mantenimiento / actualización de equipos (hardware)	0	0	5
		Caída del sistema por agotamiento de recursos	0	0	5
		Pérdida de equipos	2	0	7.5
		Abuso de privilegios de acceso	7.5	7.5	3
		Uso no previsto	0.75	0.75	3
		Acceso no autorizado	7.5	5	0
		Manipulación de los equipos	5	0	7.5
		Denegación de servicio	0	0	7.5
		Robo	2	0	7.5
		Ataque destructivo	0	0	5
	Servidor de backup	Fuego	0	0	4.5
		Daños por agua	0	0	3
		Desastres naturales	0	0	2.25
		Contaminación mecánica	0	0	1.8
		Contaminación electromagnética	0	0	1.5
		Avería de origen físico o lógico	0	0	4.5
		Corte del suministro eléctrico	0	0	4.5
		Condiciones inadecuadas de temperatura o humedad	0	0	3
		Interrupción de otros servicios y suministros esenciales	0	0	0.6
		Degradación de los soportes de almacenamiento de la información	0	0	1.8
		Emanaciones electromagnéticas	0.6	0	0
		Errores del administrador	4.5	3	4.5

		Fugas de información	4.5	0	0
		Errores de mantenimiento / actualización de equipos (hardware)	0	0	3
		Caída del sistema por agotamiento de recursos	0	0	3
		Pérdida de equipos	1.2	0	4.5
		Abuso de privilegios de acceso	4.5	4.5	1.8
		Uso no previsto	0.45	0.45	1.8
		Acceso no autorizado	4.5	3	0
		Manipulación de los equipos	3	0	4.5
		Denegación de servicio	0	0	4.5
		Robo	1.2	0	4.5
		Ataque destructivo	0	0	3
	Equipos de oficina	Fuego	0	0	3
		Daños por agua	0	0	2
		Desastres naturales	0	0	1.5
		Contaminación mecánica	0	0	1.2
		Contaminación electromagnética	0	0	1
		Avería de origen físico o lógico	0	0	3
		Corte del suministro eléctrico	0	0	3
		Condiciones inadecuadas de temperatura o humedad	0	0	2
		Interrupción de otros servicios y suministros esenciales	0	0	0.4
		Degradación de los soportes de almacenamiento de la información	0	0	1.2
		Emanaciones electromagnéticas	0.4	0	0
		Errores del administrador	3	2	3
		Fugas de información	3	0	0
		Errores de mantenimiento / actualización de equipos (hardware)	0	0	2
		Caída del sistema por agotamiento de recursos	0	0	2
		Pérdida de equipos	0.8	0	3
		Abuso de privilegios de acceso	3	3	1.2
		Uso no previsto	0.3	0.3	1.2
		Acceso no autorizado	3	2	0
		Manipulación de los equipos	2	0	3
		Denegación de servicio	0	0	3
		Robo	0.8	0	3
		Ataque destructivo	0	0	2
	Equipos de personal de TI	Fuego	0	0	4.5
		Daños por agua	0	0	3
		Desastres naturales	0	0	2.25
		Contaminación mecánica	0	0	1.8
		Contaminación electromagnética	0	0	1.5
		Avería de origen físico o lógico	0	0	4.5
		Corte del suministro eléctrico	0	0	4.5
		Condiciones inadecuadas de temperatura o humedad	0	0	3
		Interrupción de otros servicios y suministros esenciales	0	0	0.6
		Degradación de los soportes de	0	0	1.8

		almacenamiento de la información			
		Emanaciones electromagnéticas	0.6	0	0
		Errores del administrador	4.5	3	4.5
		Fugas de información	4.5	0	0
		Errores de mantenimiento / actualización de equipos (hardware)	0	0	3
		Caída del sistema por agotamiento de recursos	0	0	3
		Pérdida de equipos	1.2	0	4.5
		Abuso de privilegios de acceso	4.5	4.5	1.8
		Uso no previsto	0.45	0.45	1.8
		Acceso no autorizado	4.5	3	0
		Manipulación de los equipos	3	0	4.5
		Denegación de servicio	0	0	4.5
		Robo	1.2	0	4.5
		Ataque destructivo	0	0	3
	Switches CPD	Fuego	0	0	7.5
		Daños por agua	0	0	5
		Desastres naturales	0	0	3.75
		Contaminación mecánica	0	0	3
		Contaminación electromagnética	0	0	2.5
		Avería de origen físico o lógico	0	0	7.5
		Corte del suministro eléctrico	0	0	7.5
		Condiciones inadecuadas de temperatura o humedad	0	0	5
		Interrupción de otros servicios y suministros esenciales	0	0	1
		Degradación de los soportes de almacenamiento de la información	0	0	3
		Emanaciones electromagnéticas	1	0	0
		Errores del administrador	7.5	5	7.5
		Fugas de información	7.5	0	0
		Errores de mantenimiento / actualización de equipos (hardware)	0	0	5
		Caída del sistema por agotamiento de recursos	0	0	5
		Pérdida de equipos	2	0	7.5
		Abuso de privilegios de acceso	7.5	7.5	3
		Uso no previsto	0.75	0.75	3
		Acceso no autorizado	7.5	5	0
		Manipulación de los equipos	5	0	7.5
		Denegación de servicio	0	0	7.5
		Robo	2	0	7.5
		Ataque destructivo	0	0	5
	Switches sucursales	Fuego	0	0	6
		Daños por agua	0	0	4
		Desastres naturales	0	0	3
		Contaminación mecánica	0	0	2.4
		Contaminación electromagnética	0	0	2
		Avería de origen físico o lógico	0	0	6
		Corte del suministro eléctrico	0	0	6
		Condiciones inadecuadas de temperatura o humedad	0	0	4

		Interrupción de otros servicios y suministros esenciales	0	0	0.8
		Degradación de los soportes de almacenamiento de la información	0	0	2.4
		Emanaciones electromagnéticas	0.8	0	0
		Errores del administrador	6	4	6
		Fugas de información	6	0	0
		Errores de mantenimiento / actualización de equipos (hardware)	0	0	4
		Caída del sistema por agotamiento de recursos	0	0	4
		Pérdida de equipos	1.6	0	6
		Abuso de privilegios de acceso	6	6	2.4
		Uso no previsto	0.6	0.6	2.4
		Acceso no autorizado	6	4	0
		Manipulación de los equipos	4	0	6
		Denegación de servicio	0	0	6
		Robo	1.6	0	6
		Ataque destructivo	0	0	4
	Puntos de acceso	Fuego	0	0	4.5
		Daños por agua	0	0	3
		Desastres naturales	0	0	2.25
		Contaminación mecánica	0	0	1.8
		Contaminación electromagnética	0	0	1.5
		Avería de origen físico o lógico	0	0	4.5
		Corte del suministro eléctrico	0	0	4.5
		Condiciones inadecuadas de temperatura o humedad	0	0	3
		Interrupción de otros servicios y suministros esenciales	0	0	0.6
		Degradación de los soportes de almacenamiento de la información	0	0	1.8
		Emanaciones electromagnéticas	0.6	0	0
		Errores del administrador	4.5	3	4.5
		Fugas de información	4.5	0	0
		Errores de mantenimiento / actualización de equipos (hardware)	0	0	3
		Caída del sistema por agotamiento de recursos	0	0	3
		Pérdida de equipos	1.2	0	4.5
		Abuso de privilegios de acceso	4.5	4.5	1.8
		Uso no previsto	0.45	0.45	1.8
		Acceso no autorizado	4.5	3	0
		Manipulación de los equipos	3	0	4.5
		Denegación de servicio	0	0	4.5
		Robo	1.2	0	4.5
		Ataque destructivo	0	0	3
	Routers CPD	Fuego	0	0	7.5
		Daños por agua	0	0	5
		Desastres naturales	0	0	3.75
		Contaminación mecánica	0	0	3
		Contaminación electromagnética	0	0	2.5
		Avería de origen físico o lógico	0	0	7.5

		Corte del suministro eléctrico	0	0	7.5
		Condiciones inadecuadas de temperatura o humedad	0	0	5
		Interrupción de otros servicios y suministros esenciales	0	0	1
		Degradación de los soportes de almacenamiento de la información	0	0	3
		Emanaciones electromagnéticas	1	0	0
		Errores del administrador	7.5	5	7.5
		Fugas de información	7.5	0	0
		Errores de mantenimiento / actualización de equipos (hardware)	0	0	5
		Caída del sistema por agotamiento de recursos	0	0	5
		Pérdida de equipos	2	0	7.5
		Abuso de privilegios de acceso	7.5	7.5	3
		Uso no previsto	0.75	0.75	3
		Acceso no autorizado	7.5	5	0
		Manipulación de los equipos	5	0	7.5
		Denegación de servicio	0	0	7.5
		Robo	2	0	7.5
		Ataque destructivo	0	0	5
		Fuego	0	0	6
		Daños por agua	0	0	4
		Desastres naturales	0	0	3
		Contaminación mecánica	0	0	2.4
		Contaminación electromagnética	0	0	2
		Avería de origen físico o lógico	0	0	6
		Corte del suministro eléctrico	0	0	6
		Condiciones inadecuadas de temperatura o humedad	0	0	4
		Interrupción de otros servicios y suministros esenciales	0	0	0.8
		Degradación de los soportes de almacenamiento de la información	0	0	2.4
	Firewalls	Emanaciones electromagnéticas	0.8	0	0
		Errores del administrador	6	4	6
		Fugas de información	6	0	0
		Errores de mantenimiento / actualización de equipos (hardware)	0	0	4
		Caída del sistema por agotamiento de recursos	0	0	4
		Pérdida de equipos	1.6	0	6
		Abuso de privilegios de acceso	6	6	2.4
		Uso no previsto	0.6	0.6	2.4
		Acceso no autorizado	6	4	0
		Manipulación de los equipos	4	0	6
		Denegación de servicio	0	0	6
		Robo	1.6	0	6
		Ataque destructivo	0	0	4
		Fuego	0	0	1.5
	Impresoras	Daños por agua	0	0	1
		Desastres naturales	0	0	0.75

		Contaminación mecánica	0	0	0.6
		Contaminación electromagnética	0	0	0.5
		Avería de origen físico o lógico	0	0	1.5
		Corte del suministro eléctrico	0	0	1.5
		Condiciones inadecuadas de temperatura o humedad	0	0	1
		Interrupción de otros servicios y suministros esenciales	0	0	0.2
		Degradación de los soportes de almacenamiento de la información	0	0	0.6
		Emanaciones electromagnéticas	0.2	0	0
		Errores del administrador	1.5	1	1.5
		Fugas de información	1.5	0	0
		Errores de mantenimiento / actualización de equipos (hardware)	0	0	1
		Caída del sistema por agotamiento de recursos	0	0	1
		Pérdida de equipos	0.4	0	1.5
		Abuso de privilegios de acceso	1.5	1.5	0.6
		Uso no previsto	0.15	0.15	0.6
		Acceso no autorizado	1.5	1	0
		Manipulación de los equipos	1	0	1.5
		Denegación de servicio	0	0	1.5
		Robo	0.4	0	1.5
		Ataque destructivo	0	0	1
	SAI	Fuego	0	0	4.5
		Daños por agua	0	0	3
		Desastres naturales	0	0	2.25
		Contaminación mecánica	0	0	1.8
		Contaminación electromagnética	0	0	1.5
		Avería de origen físico o lógico	0	0	4.5
		Corte del suministro eléctrico	0	0	4.5
		Condiciones inadecuadas de temperatura o humedad	0	0	3
		Interrupción de otros servicios y suministros esenciales	0	0	0.6
		Degradación de los soportes de almacenamiento de la información	0	0	1.8
		Emanaciones electromagnéticas	0.6	0	0
		Errores del administrador	4.5	3	4.5
		Fugas de información	4.5	0	0
		Errores de mantenimiento / actualización de equipos (hardware)	0	0	3
		Caída del sistema por agotamiento de recursos	0	0	3
		Pérdida de equipos	1.2	0	4.5
		Abuso de privilegios de acceso	4.5	4.5	1.8
		Uso no previsto	0.45	0.45	1.8
		Acceso no autorizado	4.5	3	0
		Manipulación de los equipos	3	0	4.5
		Denegación de servicio	0	0	4.5
		Robo	1.2	0	4.5
		Ataque destructivo	0	0	3

	Cámaras de videovigilancia	Fuego	0	0	3
		Daños por agua	0	0	2
		Desastres naturales	0	0	1.5
		Contaminación mecánica	0	0	1.2
		Contaminación electromagnética	0	0	1
		Avería de origen físico o lógico	0	0	3
		Corte del suministro eléctrico	0	0	3
		Condiciones inadecuadas de temperatura o humedad	0	0	2
		Interrupción de otros servicios y suministros esenciales	0	0	0.4
		Degradación de los soportes de almacenamiento de la información	0	0	1.2
		Emanaciones electromagnéticas	0.4	0	0
		Errores del administrador	3	2	3
		Fugas de información	3	0	0
		Errores de mantenimiento / actualización de equipos (hardware)	0	0	2
		Caída del sistema por agotamiento de recursos	0	0	2
		Pérdida de equipos	0.8	0	3
		Abuso de privilegios de acceso	3	3	1.2
		Uso no previsto	0.3	0.3	1.2
		Acceso no autorizado	3	2	0
		Manipulación de los equipos	2	0	3
		Denegación de servicio	0	0	3
		Robo	0.8	0	3
		Ataque destructivo	0	0	2
	Sistema de alarma	Fuego	0	0	7.5
		Daños por agua	0	0	5
		Desastres naturales	0	0	3.75
		Contaminación mecánica	0	0	3
		Contaminación electromagnética	0	0	2.5
		Avería de origen físico o lógico	0	0	7.5
		Corte del suministro eléctrico	0	0	7.5
		Condiciones inadecuadas de temperatura o humedad	0	0	5
		Interrupción de otros servicios y suministros esenciales	0	0	1
		Degradación de los soportes de almacenamiento de la información	0	0	3
		Emanaciones electromagnéticas	1	0	0
		Errores del administrador	7.5	5	7.5
		Fugas de información	7.5	0	0
		Errores de mantenimiento / actualización de equipos (hardware)	0	0	5
		Caída del sistema por agotamiento de recursos	0	0	5
		Pérdida de equipos	2	0	7.5
		Abuso de privilegios de acceso	7.5	7.5	3
		Uso no previsto	0.75	0.75	3
		Acceso no autorizado	7.5	5	0
		Manipulación de los equipos	5	0	7.5

		Denegación de servicio	0	0	7.5
		Robo	2	0	7.5
		Ataque destructivo	0	0	5
	Cajeros automáticos	Fuego	0	0	6
		Daños por agua	0	0	4
		Desastres naturales	0	0	3
		Contaminación mecánica	0	0	2.4
		Contaminación electromagnética	0	0	2
		Avería de origen físico o lógico	0	0	6
		Corte del suministro eléctrico	0	0	6
		Condiciones inadecuadas de temperatura o humedad	0	0	4
		Interrupción de otros servicios y suministros esenciales	0	0	0.8
		Degradación de los soportes de almacenamiento de la información	0	0	2.4
		Emanaciones electromagnéticas	0.8	0	0
		Errores del administrador	6	4	6
		Fugas de información	6	0	0
		Errores de mantenimiento / actualización de equipos (hardware)	0	0	4
		Caída del sistema por agotamiento de recursos	0	0	4
		Pérdida de equipos	1.6	0	6
		Abuso de privilegios de acceso	6	6	2.4
		Uso no previsto	0.6	0.6	2.4
		Acceso no autorizado	6	4	0
		Manipulación de los equipos	4	0	6
		Denegación de servicio	0	0	6
		Robo	1.6	0	6
		Ataque destructivo	0	0	4
SW	Windows Server 2012 Standard Edition	Avería de origen físico o lógico	0	0	7.5
		Errores de los usuarios	2	5	2
		Errores del administrador	7.5	7.5	7.5
		Difusión de software dañino	7.5	7.5	7.5
		Destrucción de información	0	0	5
		Fugas de información	5	0	0
		Vulnerabilidades de los programas (software)	7.5	7.5	7.5
		Errores de mantenimiento / actualización de programas (software)	0	5	2
		Suplantación de la identidad del usuario	7.5	7.5	0
		Abuso de privilegios de acceso	0.5	5	5
		Uso no previsto	0.75	0.75	3
		[Re-]encaminamiento de mensajes	5	0	0
		Alteración de secuencia	0	2	0
		Acceso no autorizado	5	2	0
		Modificación de la información	0	5	0
		Manipulación de programas	7.5	7.5	5
	Linux Ubuntu Server 11.10	Avería de origen físico o lógico	0	0	7.5
		Errores de los usuarios	2	5	2
		Errores del administrador	7.5	7.5	7.5
		Difusión de software dañino	7.5	7.5	7.5

		Destrucción de información	0	0	5
		Fugas de información	5	0	0
		Vulnerabilidades de los programas (software)	7.5	7.5	7.5
		Errores de mantenimiento / actualización de programas (software)	0	5	2
		Suplantación de la identidad del usuario	7.5	7.5	0
		Abuso de privilegios de acceso	0.5	5	5
		Uso no previsto	0.75	0.75	3
		[Re-]encaminamiento de mensajes	5	0	0
		Alteración de secuencia	0	2	0
		Acceso no autorizado	5	2	0
		Modificación de la información	0	5	0
		Manipulación de programas	7.5	7.5	5
	Apache Web Server	Avería de origen físico o lógico	0	0	6
		Errores de los usuarios	1.6	4	1.6
		Errores del administrador	6	6	6
		Difusión de software dañino	6	6	6
		Destrucción de información	0	0	4
		Fugas de información	4	0	0
		Vulnerabilidades de los programas (software)	6	6	6
		Errores de mantenimiento / actualización de programas (software)	0	4	1.6
		Suplantación de la identidad del usuario	6	6	0
		Abuso de privilegios de acceso	0.4	4	4
		Uso no previsto	0.6	0.6	2.4
		[Re-]encaminamiento de mensajes	4	0	0
		Alteración de secuencia	0	1.6	0
		Acceso no autorizado	4	1.6	0
		Modificación de la información	0	4	0
		Manipulación de programas	6	6	4
	Windows 8.1	Avería de origen físico o lógico	0	0	4.5
		Errores de los usuarios	1.2	3	1.2
		Errores del administrador	4.5	4.5	4.5
		Difusión de software dañino	4.5	4.5	4.5
		Destrucción de información	0	0	3
		Fugas de información	3	0	0
		Vulnerabilidades de los programas (software)	4.5	4.5	4.5
		Errores de mantenimiento / actualización de programas (software)	0	3	1.2
		Suplantación de la identidad del usuario	4.5	4.5	0
		Abuso de privilegios de acceso	0.3	3	3
		Uso no previsto	0.45	0.45	1.8
		[Re-]encaminamiento de mensajes	3	0	0
		Alteración de secuencia	0	1.2	0
		Acceso no autorizado	3	1.2	0
		Modificación de la información	0	3	0
		Manipulación de programas	4.5	4.5	3
	Aplicación Gestión Bancaria	Avería de origen físico o lógico	0	0	7.5
		Errores de los usuarios	2	5	2
		Errores del administrador	7.5	7.5	7.5

		Difusión de software dañino	7.5	7.5	7.5
		Destrucción de información	0	0	5
		Fugas de información	5	0	0
		Vulnerabilidades de los programas (software)	7.5	7.5	7.5
		Errores de mantenimiento / actualización de programas (software)	0	5	2
		Suplantación de la identidad del usuario	7.5	7.5	0
		Abuso de privilegios de acceso	0.5	5	5
		Uso no previsto	0.75	0.75	3
		[Re-]encaminamiento de mensajes	5	0	0
		Alteración de secuencia	0	2	0
		Acceso no autorizado	5	2	0
		Modificación de la información	0	5	0
		Manipulación de programas	7.5	7.5	5
	SGBD Oracle 10g	Avería de origen físico o lógico	0	0	7.5
		Errores de los usuarios	2	5	2
		Errores del administrador	7.5	7.5	7.5
		Difusión de software dañino	7.5	7.5	7.5
		Destrucción de información	0	0	5
		Fugas de información	5	0	0
		Vulnerabilidades de los programas (software)	7.5	7.5	7.5
		Errores de mantenimiento / actualización de programas (software)	0	5	2
		Suplantación de la identidad del usuario	7.5	7.5	0
		Abuso de privilegios de acceso	0.5	5	5
		Uso no previsto	0.75	0.75	3
		[Re-]encaminamiento de mensajes	5	0	0
		Alteración de secuencia	0	2	0
		Acceso no autorizado	5	2	0
		Modificación de la información	0	5	0
		Manipulación de programas	7.5	7.5	5
	ESET Smart Security 8	Avería de origen físico o lógico	0	0	4.5
		Errores de los usuarios	1.2	3	1.2
		Errores del administrador	4.5	4.5	4.5
		Difusión de software dañino	4.5	4.5	4.5
		Destrucción de información	0	0	3
		Fugas de información	3	0	0
		Vulnerabilidades de los programas (software)	4.5	4.5	4.5
		Errores de mantenimiento / actualización de programas (software)	0	3	1.2
		Suplantación de la identidad del usuario	4.5	4.5	0
		Abuso de privilegios de acceso	0.3	3	3
		Uso no previsto	0.45	0.45	1.8
		[Re-]encaminamiento de mensajes	3	0	0
		Alteración de secuencia	0	1.2	0
		Acceso no autorizado	3	1.2	0
		Modificación de la información	0	3	0
		Manipulación de programas	4.5	4.5	3
	Windows XP Embedded	Avería de origen físico o lógico	0	0	6
		Errores de los usuarios	1.6	4	1.6

		Errores del administrador	6	6	6
		Difusión de software dañino	6	6	6
		Destrucción de información	0	0	4
		Fugas de información	4	0	0
		Vulnerabilidades de los programas (software)	6	6	6
		Errores de mantenimiento / actualización de programas (software)	0	4	1.6
		Suplantación de la identidad del usuario	6	6	0
		Abuso de privilegios de acceso	0.4	4	4
		Uso no previsto	0.6	0.6	2.4
		[Re-]encaminamiento de mensajes	4	0	0
		Alteración de secuencia	0	1.6	0
		Acceso no autorizado	4	1.6	0
		Modificación de la información	0	4	0
		Manipulación de programas	6	6	4
	Herramienta Amanda para backup	Avería de origen físico o lógico	0	0	4.5
		Errores de los usuarios	1.2	3	1.2
		Errores del administrador	4.5	4.5	4.5
		Difusión de software dañino	4.5	4.5	4.5
		Destrucción de información	0	0	3
		Fugas de información	3	0	0
		Vulnerabilidades de los programas (software)	4.5	4.5	4.5
		Errores de mantenimiento / actualización de programas (software)	0	3	1.2
		Suplantación de la identidad del usuario	4.5	4.5	0
		Abuso de privilegios de acceso	0.3	3	3
		Uso no previsto	0.45	0.45	1.8
		[Re-]encaminamiento de mensajes	3	0	0
		Alteración de secuencia	0	1.2	0
		Acceso no autorizado	3	1.2	0
		Modificación de la información	0	3	0
		Manipulación de programas	4.5	4.5	3
S	Servicios de banca online	Errores de los usuarios	2.4	6	0.6
		Errores del administrador	6	4	4
		Destrucción de información	0	0	6
		Fugas de información	6	0	0
		Caída del sistema por agotamiento de recursos	0	0	6
		Suplantación de la identidad del usuario	6	4	0
		Abuso de privilegios de acceso	4	6	1.6
		Uso no previsto	2.4	2.4	6
		[Re-]encaminamiento de mensajes	6	0	0
		Alteración de secuencia	0	6	0
		Acceso no autorizado	6	4	0
		Repudio	0	3	0
		Modificación de la información	0	6	0
		Denegación de servicio	0	0	6
P	Director General	Deficiencias en la organización	0	0	6
		Fugas de información	6	0	0
		Indisponibilidad del personal	0	0	6
		Extorsión	6	2.4	2.4

		Ingeniería social (picaresca)	6	6	0.6
	Directores sucursales	Deficiencias en la organización	0	0	4.5
		Fugas de información	4.5	0	0
		Indisponibilidad del personal	0	0	4.5
		Extorsión	4.5	1.8	1.8
		Ingeniería social (picaresca)	4.5	4.5	0.45
	Empleados sucursales	Deficiencias en la organización	0	0	3
		Fugas de información	3	0	0
		Indisponibilidad del personal	0	0	3
		Extorsión	3	1.2	1.2
		Ingeniería social (picaresca)	3	3	0.3
	Jefe Departamento de TI	Deficiencias en la organización	0	0	6
		Fugas de información	6	0	0
		Indisponibilidad del personal	0	0	6
		Extorsión	6	2.4	2.4
		Ingeniería social (picaresca)	6	6	0.6
	Responsables de seguridad	Deficiencias en la organización	0	0	4.5
		Fugas de información	4.5	0	0
		Indisponibilidad del personal	0	0	4.5
		Extorsión	4.5	1.8	1.8
		Ingeniería social (picaresca)	4.5	4.5	0.45
	Técnicos/desarrollado-res	Deficiencias en la organización	0	0	3
		Fugas de información	3	0	0
		Indisponibilidad del personal	0	0	3
		Extorsión	3	1.2	1.2
		Ingeniería social (picaresca)	3	3	0.3
L	Sede central	Fuego	0	0	7.5
		Daños por agua	0	0	5
		Desastres naturales	0	0	5
		Emanaciones electromagnéticas	0.25	0	0
		Destrucción de información	0	0	0.25
		Fugas de información	7.5	0	0
		Uso no previsto	0.5	2	2
		Acceso no autorizado	5	5	0
		Modificación de la información	0	3	0
		Ataque destructivo	0	0	7.5
		Ocupación enemiga	3.75	0	5
	Sucursales	Fuego	0	0	6
		Daños por agua	0	0	4
		Desastres naturales	0	0	4
		Emanaciones electromagnéticas	0.2	0	0
		Destrucción de información	0	0	0.2
		Fugas de información	6	0	0
		Uso no previsto	0.4	1.6	1.6
		Acceso no autorizado	4	4	0
		Modificación de la información	0	2.4	0
		Ataque destructivo	0	0	6
		Ocupación enemiga	3	0	4

Tabla 4-6: Valores de riesgo residual para los activos de la organización

CAPÍTULO 5. PROPUESTA DE PROYECTOS

Llegados a este punto, y teniendo a disposición los niveles de cumplimiento de las normas ISO/IEC 27001 e ISO/IEC 27002 y los valores de riesgo en la organización, es momento de plantear proyectos que ayuden a mejorar el nivel de cumplimiento de estas normas y mitiguen, en la medida de lo posible, el riesgo actual en la organización. Para ello, las propuestas de proyectos que se detallan a continuación tendrán como finalidad la aplicación o mejora del nivel de madurez de las salvaguardas que ayudarán a mitigar dichos riesgos, y en consecuencia, a mejorar el nivel de cumplimiento frente a la normativa de referencia por parte de la organización.

Según se desprende de los resultados de la auditoría de cumplimiento respecto a la norma ISO/IEC 27002 en la organización y, del análisis del cálculo del riesgo potencial, existen algunos dominios de dicha norma cuya implementación en la organización es bastante deficiente o pobre. Dichos dominios son los siguientes:

- 5. Política de seguridad.
- 6. Aspectos organizativos de la seguridad de la información.
- 8. Seguridad ligada a los recursos humanos.
- 12. Adquisición, desarrollo y mantenimiento de sistemas de información.
- 13. Gestión de incidentes en la seguridad de la información.
- 14. Gestión de la continuidad del negocio.

Por tanto, los proyectos propuestos irán mayormente enfocados a mejorar estos aspectos de la norma para que, como mínimo, queden al nivel de cumplimiento del resto, pero también a contribuir en una mejor optimización de los recursos de la organización y mejora en la gestión de los procesos. Además, se busca que dichos proyectos ayuden también a refinar el nivel de cumplimiento de los dominios de la norma no mencionados.

5.1 PROYECTO 1: REDEFINICIÓN DE LA POLÍTICA DE SEGURIDAD Y ASPECTOS ORGANIZATIVOS

Descripción

Este proyecto busca establecer una política de seguridad en la organización que sea acorde con sus procesos de negocio, y que por tanto, cubra todos los aspectos de seguridad de la información de manera oportuna, además de cumplir con los requisitos que marca la norma ISO/IEC 27001. Por otra parte, se pretenden optimizar los aspectos

organizativos de seguridad de la información en la organización para alinearlos también con la normativa de referencia.

Objetivos

El primer objetivo de este proyecto es implementar una política de seguridad en la organización que cumpla con los siguientes requisitos:

- Defina la seguridad de la información y el alcance de la política en la organización.
- Cubra todos los aspectos de seguridad clave para la actividad y los procesos de negocio de la organización.
- Sea conocida y aplicada por todos los empleados de la organización y terceros afectados por su cumplimiento.
- Refleje el compromiso de la Dirección de la organización en cuanto a la seguridad de la información y en cuanto a la definición de la política de seguridad y su revisión.

Además, se deben llevar a cabo las siguientes tareas en materia de organización de la seguridad de la información dentro de la organización:

- Designación de un Comité de Seguridad por parte de la Dirección, como muestra de su compromiso con la seguridad de la información.
- Asignación de roles y responsabilidades relativas a la seguridad de la información.
- Establecer procedimientos para el aseguramiento de la seguridad en la relación con terceras partes.

Planificación temporal

La duración estimada para la realización del proyecto es de un mes. Dentro de dicho periodo, la planificación para la consecución de sus objetivos es la siguiente:

- Semanas 1 y 2: Definición total de la nueva política de seguridad. Definición de las responsabilidades relativas a la seguridad de la información.
- Semana 3: Aprobación de la política por parte de la Dirección de la organización, reflejando así su compromiso en seguridad de la información. Nombramiento del Comité de Seguridad.
- Semana 4: Distribución de la política entre los empleados de la organización y distinto personal afectado. Conocimiento por parte de los mismos al menos de los aspectos esenciales de la política.

Hasta aquí la fase inicial de implantación del proyecto. De manera anual, la política de seguridad deberá ser revisada y aprobada por la Dirección de la organización y se deben revisar los acuerdos de confidencialidad, contratos con terceros, etc. Con la

misma frecuencia, los empleados y afectados por la política de seguridad rellenarán un cuestionario para evaluar el grado de conocimiento que tienen de dicha política.

Coste

El coste económico de este proyecto vendrá producido por la contratación de un servicio externo de consultoría, que asesore a la organización a la hora de redefinir su política y sus nuevos procedimientos relativos a la seguridad de la información, de manera que cumplan con los requisitos marcados en la norma ISO/IEC 27001. El coste de este servicio de consultoría asciende a 5000 €.

La dificultad de implantación del proyecto en la organización se puede catalogar como baja. La mayor dificultad se concentra en conseguir la aceptación y el compromiso por parte de la Dirección, mientras que los empleados de la organización tendrán que hacer un pequeño esfuerzo para adecuarse a las nuevas directrices en materia de seguridad.

Beneficios

Los beneficios que obtendrá la organización con la ejecución de este proyecto son los siguientes:

- Una buena política de seguridad garantiza la reducción de los riesgos de seguridad y el impacto de las amenazas, lo cual conlleva una reducción en el gasto provocado por incidentes de seguridad de la información.
- Mayor concienciación en materia de seguridad de la información en la organización.
- Mejora y optimización de los procesos de seguridad.
- Mejora de la imagen corporativa.

5.2 PROYECTO 2: PROGRAMA DE FORMACIÓN Y SENSIBILIZACIÓN EN SEGURIDAD DE LA INFORMACIÓN

Descripción

Este proyecto pretende que los empleados de la organización adquieran la concienciación, formación y capacitación adecuadas en los procedimientos de seguridad y en el uso de los recursos de tratamiento de la información. Además, se busca que esta formación se renueve con una frecuencia establecida.

Objetivos

El objetivo de este proyecto es establecer e implantar un plan de formación, capacitación y concienciación en seguridad de la información destinado a todos los

empleados de la organización y terceros con los que exista alguna relación (clientes, proveedores, etc.). La formación debe tratar los siguientes aspectos:

- Requisitos de seguridad y responsabilidades legales de cada uno de los puestos de trabajo.
- Formación en el uso correcto de los recursos de tratamiento de la información: procedimiento de registro en el sistema (log-in), uso de paquetes de software, etc.
- Información sobre amenazas conocidas.
- Información sobre los canales adecuados para informar sobre los incidentes de la seguridad de la información.
- Información sobre el proceso disciplinario en caso de provocar alguna violación de la seguridad.

Planificación temporal

La cursos de formación se desarrollarán a lo largo de dos semanas, con una frecuencia bianual. Se pretende que los empleados adquieran progresivamente unos conocimientos que le permitan desempeñar sus tareas profesionales de manera segura. Para ello, se fijan las siguientes metas:

- Corto plazo: El empleado debe conocer los requisitos de seguridad de su puesto de trabajo y debe conocer cuál es el canal adecuado para informar sobre un posible incidente de seguridad.
- Medio plazo: El empleado debe saber hacer un uso correcto de los recursos de tratamiento de la información, manejar de manera segura el software que utiliza en el desempeño de su labor profesional y debe conocer las principales amenazas.
- Largo plazo: El empleado debe conocer cuáles son las responsabilidades legales del puesto de trabajo que desempeña, los posibles procesos disciplinarios y tener un amplio conocimiento sobre amenazas que pueden provocar incidentes de seguridad.

Coste

El coste económico de este proyecto vendrá producido por la contratación de personal externo que imparta los cursos de formación en materia de seguridad. El coste de este servicio asciende a 3500 €/año.

La dificultad de implantación de este proyecto en la organización se puede catalogar como baja, ya que lo único que requiere es implicación por parte del personal.

Beneficios

Los beneficios que obtendrá la organización con la ejecución de este proyecto son los siguientes:

- Mayor concienciación en materia de seguridad de la información.
- Incremento de la productividad de los empleados.
- Incremento en la calidad y seguridad de los servicios ofrecidos por la organización.
- Disminución de los incidentes de seguridad de la información provocados por errores de los empleados.
- Optimización del uso de los recursos de tratamiento de la información.
- Mejora de la imagen corporativa.

5.3 PROYECTO 3: DEFINICIÓN DE POLÍTICA DE CONTROLES CRIPTOGRÁFICOS Y PROCEDIMIENTOS DE CONTROL DE CAMBIOS

Descripción

Este proyecto busca, de manera general, mantener la seguridad del software y de la información manejada por las aplicaciones en la organización. Para ello, es necesario definir políticas formales destinadas a establecer procedimientos a la hora de llevar a cabo modificaciones en los sistemas y a proteger la confidencialidad, integridad y disponibilidad de la información que tratan.

Objetivos

Se puede dividir el objetivo de este proyecto en dos partes. En primer lugar, es necesario formular e implantar una política para el uso de los controles criptográficos destinada a proteger la información que cumpla con los siguientes requisitos:

- Identifique el nivel de protección necesario en base al análisis de riesgos.
- Detalle el uso del cifrado para proteger la información sensible transportada a través de dispositivos móviles o extraíbles o a través de líneas de comunicación.
- Defina procedimientos de gestión de claves.
- Establezca las funciones y responsabilidades en materia de implantación de la política y gestión de las claves.

Por otro lado, el segundo objetivo de este proyecto es definir un procedimiento de control de cambios que asegure que las modificaciones que se realicen en los sistemas de la organización se lleven a cabo de manera controlada y revisada, para comprobar que no ponen en peligro su seguridad. El procedimiento de control de cambios debe considerar al menos los siguientes aspectos:

- Registro de solicitud de cambio.
- Revisión de solicitud de cambio.

- Autorización de solicitud de cambio.
- Supervisión de la implementación del cambio.
- Revisión y registro de los cambios realizados.

Planificación temporal

El tiempo estimado de duración del proyecto es de seis semanas. Dentro de dicho periodo la planificación es la siguiente:

- Semana 1: Análisis de la evaluación de riesgos de la organización para identificar el nivel de protección necesario.
- Semanas 2 y 3: Formulación de la política de uso de controles criptográficos, teniendo en cuenta los resultados del análisis de la evaluación de riesgos y el enfoque de la Dirección.
- Semana 4: Definición del procedimiento de control de cambios en colaboración con la Dirección.
- Semanas 5 y 6: Distribución de la nueva política de uso de controles criptográficos y procedimiento de control de cambios a los empleados de la organización. Explicación de las principales modificaciones y adecuación de la organización a las nuevas normas.

De manera anual, tanto la política de uso de controles criptográficos como el procedimiento de control de cambios deben ser revisados, y su revisión debe ser aprobada por la Dirección.

Coste

La implantación de este proyecto requerirá la contratación por parte de la organización de un servicio externo de consultoría, que le asesore en la correcta definición de la política de uso de controles criptográficos y en la definición del procedimiento de control de cambios. El coste de este servicio de consultoría asciende a 7500 €.

En cuanto al coste en términos de dificultad de implantación se puede catalogar como medio, debido a que se va a llevar a cabo una redefinición profunda de varios procesos y metodologías que se venían aplicando hasta el momento, por lo que la correcta aplicación de los nuevos requiere la implicación del personal de la organización.

Beneficios

Los beneficios que obtendrá la organización con la ejecución de este proyecto son los siguientes:

- Mejora de la seguridad en el tratamiento de la información.
- Disminución de los incidentes de seguridad de la información provocados por errores de los empleados.

- Mejora en la calidad y seguridad de los servicios ofrecidos.

5.4 PROYECTO 4: MEJORA EN LA GESTIÓN DE INCIDENTES DE SEGURIDAD

Descripción

Este proyecto pretende dotar a la organización de unos procedimientos de gestión de incidentes de seguridad acordes con la criticidad de sus actividades de negocio y alineados con los estándares de referencia, a la vez que proporcionar a los empleados los conocimientos y herramientas necesarias para comunicar los posibles incidentes que se produzcan.

Objetivos

Los objetivos de este proyecto son los siguientes:

- Definir procedimientos formales de comunicación de eventos de seguridad y escalada de incidentes.
- Proporcionar información a los empleados y terceros afectados sobre los procedimientos de comunicación de los diferentes tipos de eventos y puntos débiles de seguridad.
- Definir responsabilidades a la hora de tratar incidentes y puntos débiles de seguridad de forma efectiva una vez que se hayan comunicado.
- Dotar a los empleados y terceros afectados de una solución integral para la gestión de incidencias.
- Aplicar un proceso de mejora continua en relación a la gestión de los incidentes de seguridad de la información.

Planificación temporal

La duración estimada para la realización de este proyecto es de un mes. Dentro de este periodo, la planificación es la que se muestra a continuación:

- Semanas 1 y 2: Definición de la política de gestión de incidentes de seguridad: procedimientos de comunicación, roles y responsabilidades, etc. Se contará con la colaboración de la Dirección de la organización.
- Semana 3: Adquisición e integración de la herramienta *iTop* para automatizar todo el proceso de gestión de incidentes de seguridad.
- Semana 4: Formación a los empleados y terceros afectados sobre los procedimientos de comunicación, responsabilidades, procesos disciplinarios, etc. (esta formación puede, y de hecho es lo más normal, integrarse en la formación de la que se hablaba en el Proyecto 2).

Formación sobre el manejo de la herramienta de gestión de incidentes de seguridad.

Todos las políticas y procedimientos relacionados con la gestión de incidentes de seguridad deben ser revisados de manera anual, y su revisión debe ser aprobada por la Dirección.

Costes

La implantación de este proyecto conllevaría la contratación de un servicio externo de consultoría, que asesorara a la organización sobre cómo afrontar correctamente el proceso de gestión de incidentes de seguridad, y adicionalmente, proporcionar formación a los empleados de la organización. El coste de este servicio sería de 8000 €. La herramienta utilizada para automatizar el proceso (*iTop*) es OpenSource, por lo que no habrá costes asociados a licencias.

El coste del proyecto en relación a la dificultad de su implantación en la organización se puede catalogar como medio, ya que requerirá la implicación y formación de los usuarios finales.

Beneficios

Los beneficios que obtendrá la organización con la ejecución de este proyecto son los siguientes:

- Reducción de incidentes de seguridad debido a la notificación temprana de puntos débiles de seguridad.
- Descenso en la dedicación a la resolución de incidencias.
- Aumento de la satisfacción de los clientes.
- Mejora de la imagen corporativa.

5.5 PROYECTO 5: ESTABLECIMIENTO DE UN PLAN DE CONTINUIDAD DEL NEGOCIO

Descripción

Este proyecto pretende implementar un plan de continuidad del negocio en la organización, que prevenga y minimice los efectos de posibles fallos de seguridad, desastres naturales, acciones intencionadas, etc.

Objetivos

Los objetivos o tareas que se deben llevar a cabo en la organización para la correcta implantación de un plan de continuidad del negocio son los siguientes:

- Identificar todos los activos que intervienen en los procesos críticos del negocio.
- Identificar los eventos que pueden causar interrupciones en la actividad de la organización, la probabilidad de que se produzcan, sus efectos y sus consecuencias para la seguridad de la información.
- Desarrollar e implantar un plan para mantener o restaurar las operaciones y garantizar la disponibilidad de la información en el nivel y el tiempo requerido, tras producirse una interrupción o un fallo de los procesos críticos del negocio.
- Llevar a cabo pruebas del plan de continuidad del negocio definido, para asegurar que es efectivo.
- Dotar al plan de la infraestructura tecnológica necesaria: servidores de respaldo, equipamiento de red de respaldo, SAIs, etc.
- Contratar un seguro que responda económicamente ante posibles incidentes que comprometan la seguridad de la información.

Planificación temporal

La duración estimada para la realización de este proyecto es de dos meses. Dentro de este periodo, la planificación es la que se muestra a continuación:

- Semana 1: Identificar e inventariar los activos críticos para el desempeño de la actividad de negocio de la organización.
- Semanas 2 y 3: Determinar la probabilidad con la que se producen fallos en los equipos, errores humanos, ataques intencionados u otros errores lógicos que puedan provocar una interrupción de la actividad de negocio. Además, realizar un estudio de la ubicación de la organización para determinar cuáles pueden ser los eventos de tipo físico que produzcan con más probabilidad interrupciones en el servicio: robos, incendios, desastres naturales, etc.
- Semana 4: Definir y formalizar el plan de gestión de la continuidad del negocio. El plan debe reflejar el compromiso de la Dirección de la organización y contar con su aceptación.
- Semanas 5 y 6: Deben llevarse a cabo pruebas para garantizar la eficacia del plan de continuidad del negocio. Deben realizarse las siguientes pruebas:
    - Debates acerca de cómo actuar en caso de darse distintos escenarios.
    - Simulaciones.
    - Pruebas de recuperación de sistemas.
    - Pruebas de recuperación fuera del emplazamiento principal de la organización.
    - Ensayos generales para probar que el personal, los equipos, las instalaciones y los procesos pueden afrontar las interrupciones.

- Semanas 7 y 8: Adquisición e integración de toda la infraestructura tecnológica de respaldo que garantice la continuidad del negocio en caso de interrupción de la infraestructura principal. Análisis de distintas ofertas de seguros y elección de la más conveniente para la organización.

El plan de gestión de la continuidad del negocio debe revisarse anualmente, y su revisión debe contar con la aprobación de la Dirección. Las pruebas que garantizan que el procedimiento es eficaz deben realizarse de manera periódica, y la programación de las mismas debe quedar reflejada en el plan de continuidad del negocio.

Costes

El coste de implantación de este proyecto estará determinado por la contratación de un servicio de consultoría externa que asesore a la organización en la definición del plan de continuidad del negocio, y en la programación de las distintas pruebas. Este servicio tendrá un coste de 12000 €. Por otro lado, hay que añadir el coste de adquisición de los distintos equipos de respaldo: servidores, equipamiento de red y una SAI de mayor capacidad que la que ya existe, principalmente. El coste de estos equipos asciende a 30000 €. Por último, tenemos el coste de la contratación del seguro, que asciende a 5000 €/año.

En cuanto al coste en términos de dificultad de implantación del proyecto se puede catalogar como alto, ya que requiere una importante implicación de la Dirección de la organización y del personal asociado al Departamento de TI. Además, requiere que el personal en su totalidad esté preparado ante la ocurrencia de una posible interrupción y sepa cómo actuar. También requerirá la integración de los sistemas redundantes en la infraestructura tecnológica de la organización.

Beneficios

Los beneficios que obtendrá la organización con la ejecución de este proyecto son los siguientes:

- Continuidad del negocio frente a desastres e incidentes.
- Refuerzo del valor de la imagen corporativa ante desastres.
- Reducción de las pérdidas económicas en caso de interrupciones.
- Mayor robustez de los servicios ofrecidos por la organización.

5.6 RESUMEN DE RESULTADOS

Tras la presentación de los proyectos es momento de analizar el impacto que supone la ejecución de cada uno de ellos sobre la seguridad de la organización. Además, con la implantación de los proyectos propuestos se pretende aumentar el nivel de

cumplimiento de los diferentes dominios de la norma ISO/IEC 27002. También se mostrará cómo dichos proyectos contribuyen a ello.

La Tabla 5-1 muestra el porcentaje de reducción del impacto de materialización de las amenazas que supondría la ejecución de cada uno de los proyectos propuestos. Además, se muestra la dificultad de implantación de cada uno de ellos, para que a simple vista se pueda deducir su importancia.

Proyecto	% reducción del impacto	Dificultad de implantación
1. Redefinición de la política de seguridad y aspectos organizativos	70%	Baja
2. Programa de formación y sensibilización en seguridad de la información	80%	Baja
3. Definición de política de controles criptográficos y procedimientos de control de cambios	60%	Media
4. Mejora en la gestión de incidentes de seguridad	50%	Media
5. Establecimiento de un plan de continuidad del negocio	65%	Alta

Tabla 5-1: Relación entre implantación de proyectos y reducción del impacto

El gráfico que se muestra en la Figura 5-1 refleja el nivel de cumplimiento de los dominios de la norma ISO/IEC 27002 antes y después de la realización de los proyectos. Los resultados que arroja son otro motivo más para la realización de los mismos en la organización, ya que como se puede observar, los dominios van evolucionando hacia un nivel de madurez optimizado.

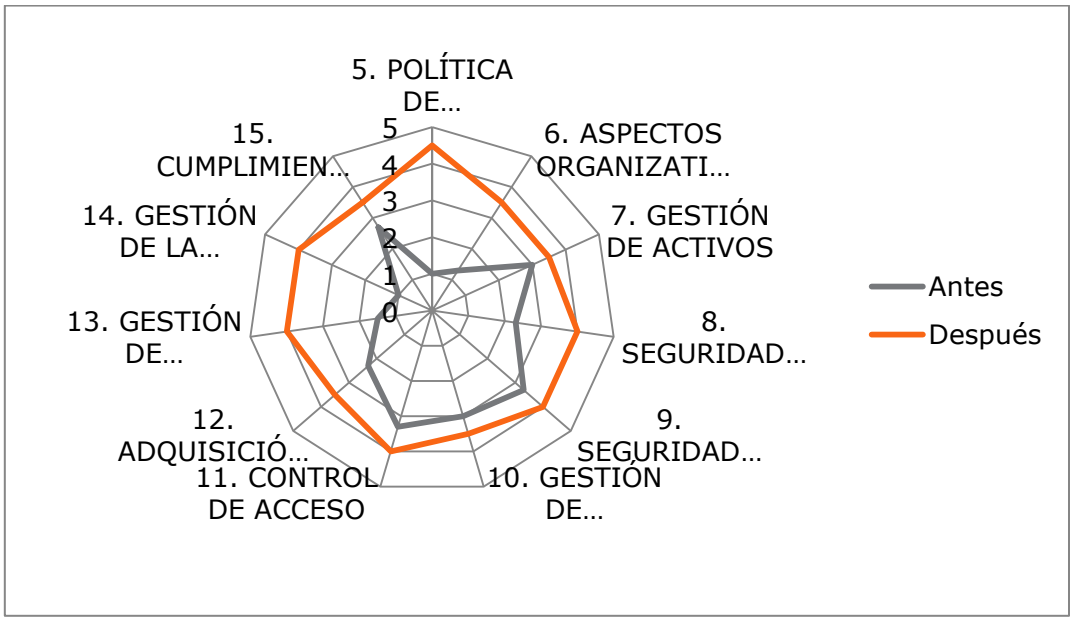

Figura 5-1: Nivel de cumplimiento antes y después de la realización de los proyectos

Finalmente, la Tabla 5-2 muestra de una manera más gráfica la distribución en el tiempo de la ejecución de los distintos proyectos.

Proyecto	Duración											
	Sep 2015		Oct 2015		Nov 2015		Dic 2015		Ene 2016		Feb 2016	
Redefinición de la política de seguridad y aspectos organizativos												
Programa de formación y sensibilización en seguridad de la información												
Definición de política de controles criptográficos y procedimientos de control de cambios												
Mejora en la gestión de incidentes de seguridad												
Establecimiento de un plan de continuidad del negocio												

Tabla 5-2: Distribución temporal de los proyectos

CAPÍTULO 6. AUDITORÍA DE CUMPLIMIENTO DE LA ISO/IEC 27002:2005

El objetivo de esta fase es evaluar hasta qué punto la empresa cumple con las buenas prácticas en materia de seguridad. Para ello, se utilizará la norma que se ha venido utilizando a lo largo de todo este trabajo, la norma ISO/IEC 27002:2005 [3], que nos servirá como marco de control del estado de la seguridad.

El estándar ISO/IEC 27002:2005, agrupa un total de 133 controles o salvaguardas, organizados en 11 dominios y 39 objetivos de control. Este estándar es internacionalmente reconocido y es perfectamente válido para la mayoría de organizaciones. Para llevar a cabo el objetivo que se plantea en esta fase, será necesario evaluar el nivel de madurez de cada uno de los controles de la norma, y por consiguiente, de cada uno de los objetivos de control y dominios de la misma. Para medir el nivel de madurez de cada uno de los controles se utilizará la escala CMM, descrita en la Tabla 2-1.

Como resultados tras la finalización de esta fase se obtendrá una tabla que recogerá el nivel de madurez con que están implantados los controles, objetivos de control y dominios de la norma. Además, también se reflejarán las no conformidades, observaciones y oportunidades de mejora detectadas en la organización. Con los resultados de esta evaluación, se elaborará posteriormente un gráfico que representará el porcentaje de controles para cada uno de los niveles de la escala CMM, y a continuación, un gráfico de radar que mostrará el nivel actual de cumplimiento de cada uno de los dominios de la norma y el nivel objetivo que se pretende alcanzar en un futuro.

6.1 EVALUACIÓN DE CUMPLIMIENTO

La Tabla 6-1 muestra el nivel de madurez de los controles, objetivos de control y dominios de la norma ISO/IEC 27002:2005 tras el proceso de gestión de riesgos en la organización.

Cláusula	Control/Objetivo de control/Dominio	Nivel de madurez	% Efectividad
5	Política de seguridad	4 - Gestionado	95%
5.1	Política de seguridad de la información	4 - Gestionado	95%
5.1.1	Documento de política de seguridad de la información	4 - Gestionado	95%
5.1.2	Revisión de la política de seguridad de la	4 - Gestionado	95%

	información		
6	Aspectos organizativos de la seguridad de la información	2 - Repetible	80%
6.1	Organización interna	2 - Repetible	70%
6.1.1	Compromiso de la Dirección con la seguridad de la información	3 - Definido	90%
6.1.2	Coordinación de la seguridad de la información	3 - Definido	90%
6.1.3	Asignación de responsabilidades relativas a la seguridad de la información	3 - Definido	90%
6.1.4	Proceso de autorización de recursos para el tratamiento de la información	2 - Repetible	50%
6.1.5	Acuerdos de confidencialidad	3 - Definido	90%
6.1.6	Contacto con las autoridades	2 - Repetible	50%
6.1.7	Contacto con grupos de especial interés	1 - Inicial	10%
6.1.8	Revisión independiente de la seguridad de la información	3 - Definido	90%
6.2	Terceros	3 - Definido	90%
6.2.1	Identificación de los riesgos derivados del acceso de terceros	3 - Definido	90%
6.2.2	Tratamiento de la seguridad en la relación con los clientes	3 - Definido	90%
6.2.3	Tratamiento de seguridad en los contratos con terceros	3 - Definido	90%
7	Gestión de activos	3 - Definido	92%
7.1	Responsabilidad sobre los activos	4 - Gestionado	95%
7.1.1	Inventario de activos	4 - Gestionado	95%
7.1.2	Propiedad de los activos	4 - Gestionado	95%
7.1.3	Uso aceptable de los activos	4 - Gestionado	95%
7.2	Clasificación de la información	3 - Definido	90%
7.2.1	Directrices de clasificación	3 - Definido	90%
7.2.2	Etiquetado y manipulado de la información	3 - Definido	90%
8	Seguridad ligada a los recursos humanos	4 - Gestionado	95%
8.1	Antes del empleo	5 - Optimizado	100%
8.1.1	Funciones y responsabilidades	5 - Optimizado	100%
8.1.2	Investigación de antecedentes	5 - Optimizado	100%
8.1.3	Términos y condiciones de contratación	5 - Optimizado	100%
8.2	Durante el empleo	3 - Definido	91%
8.2.1	Responsabilidades de la Dirección	3 - Definido	90%
8.2.2	Concienciación, formación y capacitación en seguridad de la información	4 - Gestionado	95%
8.2.3	Proceso disciplinario	3 - Definido	90%
8.3	Cese del empleo o cambio de puesto de trabajo	4 - Gestionado	96%
8.3.1	Responsabilidad del cese o cambio	4 - Gestionado	95%
8.3.2	Devolución de activos	4 - Gestionado	95%
8.3.3	Retirada de los derechos de acceso	5 - Optimizado	100%
9	Seguridad física y del entorno	2 - Repetible	81%
9.1	Áreas seguras	4 - Gestionado	98%
9.1.1	Perímetro de seguridad física	5 - Optimizado	100%
9.1.2	Controles físicos de entrada	5 - Optimizado	100%
9.1.3	Seguridad de oficinas, despachos e instalaciones	5 - Optimizado	100%

9.1.4	Protección contra las amenazas externas y de origen ambiental	3 - Definido	90%
9.1.5	Trabajo en áreas seguras	5 - Optimizado	100%
9.1.6	Áreas de acceso público y de carga y descarga	5 - Optimizado	100%
9.2	Seguridad de los equipos	2 - Repetible	65%
9.2.1	Emplazamiento y protección de los equipos	4 - Gestionado	95%
9.2.2	Instalaciones de suministro	4 - Gestionado	95%
9.2.3	Seguridad del cableado	5 - Optimizado	100%
9.2.4	Mantenimiento de los equipos	5 - Optimizado	100%
9.2.5	Seguridad de los equipos fuera de las instalaciones	2 - Repetible	50%
9.2.6	Reutilización o retirada segura de equipos	1 - Inicial	10%
9.2.7	Retirada de materiales propiedad de la empresa	1 - Inicial	10%
10	Gestión de comunicaciones y operaciones	3 - Definido	94%
10.1	Responsabilidades y procedimientos de operación	4 - Gestionado	96%
10.1.1	Documentación de los procedimientos de operación	4 - Gestionado	95%
10.1.2	Gestión de cambios	4 - Gestionado	95%
10.1.3	Segregación de tareas	5 - Optimizado	100%
10.1.4	Separación de los recursos de desarrollo, prueba y operación	4 - Gestionado	95%
10.2	Gestión de la provisión de servicios por terceros	3 - Definido	90%
10.2.1	Provisión de servicios	3 - Definido	90%
10.2.2	Supervisión y revisión de los servicios prestados por terceros	3 - Definido	90%
10.2.3	Gestión del cambio en los servicios prestados por terceros	3 - Definido	90%
10.3	Planificación y aceptación del sistema	5 - Optimizado	100%
10.3.1	Gestión de capacidades	5 - Optimizado	100%
10.3.2	Aceptación del sistema	5 - Optimizado	100%
10.4	Protección contra el código malicioso y descargable	4 - Gestionado	97%
10.4.1	Controles contra el código malicioso	5 - Optimizado	100%
10.4.2	Controles contra el código descargado en el cliente	4 - Gestionado	95%
10.5	Copias de seguridad	5 - Optimizado	100%
10.5.1	Copias de seguridad de la información	5 - Optimizado	100%
10.6	Gestión de la seguridad de las redes	4 - Gestionado	97%
10.6.1	Controles de red	5 - Optimizado	100%
10.6.2	Seguridad de los servicios de red	4 - Gestionado	95%
10.7	Manipulación de los soportes	2 - Repetible	81%
10.7.1	Gestión de soportes extraíbles	2 - Repetible	50%
10.7.2	Retirada de soportes	3 - Definido	90%
10.7.3	Procedimientos de manipulación de la información	4 - Gestionado	95%
10.7.4	Seguridad de la documentación del sistema	3 - Definido	90%
10.8	Intercambio de información	4 - Gestionado	96%
10.8.1	Políticas y procedimientos de intercambio de información	5 - Optimizado	100%

10.8.2	Acuerdos de intercambio	3 - Definido	90%
10.8.3	Soportes físicos en tránsito	4 - Gestionado	95%
10.8.4	Mensajería electrónica	4 - Gestionado	95%
10.8.5	Sistemas de información empresariales	5 - Optimizado	100%
10.9	Servicios de comercio electrónico	4 - Gestionado	98%
10.9.1	Comercio electrónico	5 - Optimizado	100%
10.9.2	Transacciones en línea	5 - Optimizado	100%
10.9.3	Información públicamente disponible	4 - Gestionado	95%
10.10	Supervisión	3 - Definido	93%
10.10.1	Registros de auditoría	3 - Definido	90%
10.10.2	Supervisión del uso del sistema	4 - Gestionado	95%
10.10.3	Protección de la información de los registros	4 - Gestionado	95%
10.10.4	Registros de administración y operación	3 - Definido	90%
10.10.5	Registro de fallos	3 - Definido	90%
10.10.6	Sincronización del reloj	5 - Optimizado	100%
11	Control de acceso	2 - Repetible	88%
11.1	Requisitos de negocio para el control de acceso	5 - Optimizado	100%
11.1.1	Política de control de acceso	5 - Optimizado	100%
11.2	Gestión de acceso de usuario	2 - Repetible	77%
11.2.1	Registros de usuario	5 - Optimizado	100%
11.2.2	Gestión de privilegios	5 - Optimizado	100%
11.2.3	Gestión de contraseñas de usuario	5 - Optimizado	100%
11.2.4	Revisión de los derechos de acceso de usuario	1 - Inicial	10%
11.3	Responsabilidades de usuario	2 - Repetible	80%
11.3.1	Uso de contraseñas	4 - Gestionado	95%
11.3.2	Equipo de usuario desatendido	4 - Gestionado	95%
11.3.3	Política de puesto de trabajo despejado y pantalla limpia	2 - Repetible	50%
11.4	Control de acceso a la red	4 - Gestionado	97%
11.4.1	Política de uso de los servicios en red	4 - Gestionado	95%
11.4.2	Autenticación de usuario para conexiones externas	5 - Optimizado	100%
11.4.3	Identificación de los equipos en las redes	4 - Gestionado	95%
11.4.4	Diagnóstico remoto y protección de los puertos de configuración	5 - Optimizado	100%
11.4.5	Segregación de las redes	5 - Optimizado	100%
11.4.6	Control de la conexión a la red	5 - Optimizado	100%
11.4.7	Control de encaminamiento (*routing*) de red	4 - Gestionado	95%
11.5	Control de acceso al sistema operativo	4 - Gestionado	96%
11.5.1	Procedimientos seguros de inicio de sesión	5 - Optimizado	100%
11.5.2	Identificación y autenticación de usuario	4 - Gestionado	95%
11.5.3	Sistema de gestión de contraseñas	5 - Optimizado	100%
11.5.4	Uso de los recursos del sistema	4 - Gestionado	95%
11.5.5	Desconexión automática de sesión	4 - Gestionado	95%
11.5.6	Limitación del tiempo de conexión	4 - Gestionado	95%
11.6	Control de acceso a las aplicaciones y a la información	5 - Optimizado	100%
11.6.1	Restricción del acceso a la información	5 - Optimizado	100%
11.6.2	Aislamiento de sistemas sensibles	5 - Optimizado	100%
11.7	Ordenadores portátiles y teletrabajo	2 - Repetible	70%

11.7.1	Ordenadores portátiles y comunicaciones móviles	3 - Definido	90%
11.7.2	Teletrabajo	2 - Repetible	50%
12	Adquisición, desarrollo y mantenimiento de los sistemas de información	2 - Repetible	89%
12.1	Requisitos de seguridad de los sistemas de información	3 - Definido	90%
12.1.1	Análisis y especificación de los requisitos de seguridad	3 - Definido	90%
12.2	Tratamiento correcto de las aplicaciones	4 - Gestionado	95%
12.2.1	Validación de los datos de entrada	5 - Optimizado	100%
12.2.2	Control del procesamiento interno	5 - Optimizado	100%
12.2.3	Integridad de los mensajes	3 - Definido	90%
12.2.4	Validación de los datos de salida	3 - Definido	90%
12.3	Controles criptográficos	3 - Definido	92%
12.3.1	Política de uso de los controles criptográficos	3 - Definido	90%
12.3.2	Gestión de claves	4 - Gestionado	95%
12.4	Seguridad de los archivos del sistema	2 - Repetible	66%
12.4.1	Control del software en explotación	3 - Definido	90%
12.4.2	Protección de los datos de prueba del sistema	1 - Inicial	10%
12.4.3	Control de acceso al código fuente de los programas	5 - Optimizado	100%
12.5	Seguridad en los procesos de desarrollo y soporte	4 - Gestionado	97%
12.5.1	Procedimientos de control de cambios	3 - Definido	90%
12.5.2	Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo	5 - Optimizado	100%
12.5.3	Restricciones a los cambios en los paquetes de software	5 - Optimizado	100%
12.5.4	Fugas de información	5 - Optimizado	100%
12.5.5	Externalización del desarrollo de software	4 - Gestionado	95%
12.6	Gestión de la vulnerabilidad técnica	4 - Gestionado	95%
12.6.1	Control de las vulnerabilidades técnicas	4 - Gestionado	95%
13	Gestión de incidentes de seguridad de la información	2 - Repetible	85%
13.1	Notificación de eventos y puntos débiles de seguridad de la información	3 - Definido	92%
13.1.1	Notificación de eventos de seguridad de la información	4 - Gestionado	95%
13.1.2	Notificación de puntos débiles de seguridad	3 - Definido	90%
13.2	Gestión de incidentes de seguridad de la información y mejoras	2 - Repetible	78%
13.2.1	Responsabilidades y procedimientos	3 - Definido	90%
13.2.2	Aprendizaje de los incidentes de seguridad de la información	2 - Repetible	50%
13.2.3	Recopilación de evidencias	4 - Gestionado	95%
14	Gestión de la continuidad del negocio	3 - Definido	91%
14.1	Aspectos de seguridad de la información en la gestión de la continuidad del negocio	3 - Definido	91%
14.1.1	Inclusión de la seguridad de la información en el proceso de gestión de la continuidad	4 - Gestionado	95%

	del negocio		
14.1.2	Continuidad del negocio y evaluación de riesgos	3 - Definido	90%
14.1.3	Desarrollo e implantación de planes de continuidad que incluyan la seguridad de la información	3 - Definido	90%
14.1.4	Marco de referencia para la planificación de la continuidad del negocio	3 - Definido	90%
14.1.5	Pruebas, mantenimiento y reevaluación de los planes de continuidad del negocio	3 - Definido	90%
15	Cumplimiento	2 - Repetible	86%
15.1	Cumplimiento de los requisitos legales	4 - Gestionado	98%
15.1.1	Identificación de la legislación aplicable	5 - Optimizado	100%
15.1.2	Derechos de propiedad intelectual (DPI)	5 - Optimizado	100%
15.1.3	Protección de los documentos de la organización	5 - Optimizado	100%
15.1.4	Protección de datos y privacidad de la información de carácter personal	5 - Optimizado	100%
15.1.5	Prevención del uso indebido de los recursos de tratamiento de la información	4 - Gestionado	95%
15.1.6	Regulación de los controles criptográficos	4 - Gestionado	95%
15.2	Cumplimiento de las políticas y normas de seguridad y cumplimiento técnico	2 - Repetible	70%
15.2.1	Cumplimiento de las políticas y normas de seguridad	2 - Repetible	50%
15.2.2	Comprobación del cumplimiento técnico	3 - Definido	90%
15.3	Consideraciones sobre la auditoría de los sistemas de información	3 - Definido	90%
15.3.1	Controles de auditoría de los sistemas de información	3 - Definido	90%
15.3.2	Protección de las herramientas de auditoría de los sistemas de información	3 - Definido	90%

Tabla 6-1: Nivel de implantación de los controles de la norma ISO/IEC 27002:2005

6.2 NO CONFORMIDADES, OBSERVACIONES Y OPORTUNIDADES DE MEJORA

La Tabla 6-2 recoge las no conformidades (NC), observaciones (OBS) y oportunidades de mejora (OM) identificadas en la organización.

Tipo	Apartado afectado	Descripción
NC Menor	6.1.4	Se han identificado recursos de tratamiento de la información en la organización que no cuentan con autorización por parte de la Dirección.
NC Menor	6.1.7	No se evidencian contactos con grupos de especial interés, foros o asociaciones especializadas en la seguridad de la información.
NC Menor	9.2.5	No se aplican las suficientes medidas de seguridad a los equipos y dispositivos que se utilizan fuera de las instalaciones de la organización.

NC Menor	9.2.6	No se evidencia ningún procedimiento formal para la reutilización o retirada segura de equipos. Los equipos se retiran y se guardan en un almacén sin tomar las oportunas medidas para el borrado de datos, licencias de software, etc.
NC Menor	9.2.7	No se precisa ningún tipo de autorización para sacar equipos fuera de las instalaciones de la organización.
NC Menor	10.7.1	No existe un inventario detallado de los soportes extraíbles propiedad de la organización, y no se requiere autorización para su utilización fuera de sus instalaciones.
NC Menor	11.2.4	No existe un proceso formal de revisión de los derechos de acceso de los usuarios por parte de la Dirección.
NC Menor	11.3.3	No existe una política de puesto de trabajo despejado de papeles, soportes extraíbles, etc. y pantalla limpia de los equipos que sea eficaz, ya que así se evidencia en las instalaciones de la organización.
NC Menor	11.7.2	No existe una política adecuada que defina los planes y procedimientos de operación correspondientes para las actividades de teletrabajo.
NC Menor	12.4.2	No se establece una protección especial para los datos de prueba.
NC Menor	13.2.2	Se evidencia la notificación y gestión de los eventos de seguridad pero no se realizan análisis *post-mortem* de los incidentes.
NC Menor	15.2.1	No existen evidencias de la revisión periódica por parte de la Dirección de los procedimientos de seguridad dentro de su área de responsabilidad.
OBS	6.1.1	El compromiso de la Dirección con la seguridad de la información debe ser aún mayor, ya que en ocasiones no se proporcionan los recursos necesarios para garantizar la misma.
OBS	6.2.2	Es necesario mejorar la definición de la política de control de acceso en relación a los accesos de los recursos de la organización por parte de los clientes.
OBS	10.7.2	Deben mejorarse algunos aspectos respecto al procedimiento de retirada de soportes.
OBS	15.3.1	Es necesario mejorar la planificación de las comprobaciones que se efectúen sobre los sistemas en producción.

Tabla 6-2: No conformidades (NC), observaciones (OBS) y oportunidades de mejora (OM) identificadas en la organización

6.3 RESUMEN DE RESULTADOS

La Tabla 6-3 nos muestra el número de controles implementados en la organización que hay para cada uno de los niveles de madurez de la escala CMM.

Nivel de madurez	Nº controles
0 - Inexistente	0
1 - Inicial	5
2 - Repetible	8
3 - Definido	38
4 - Gestionado	38
5 - Optimizado	44

Tabla 6-3: Número de controles por nivel de madurez

La Figura 6-1 muestra gráficamente el porcentaje de controles para cada uno de los niveles.

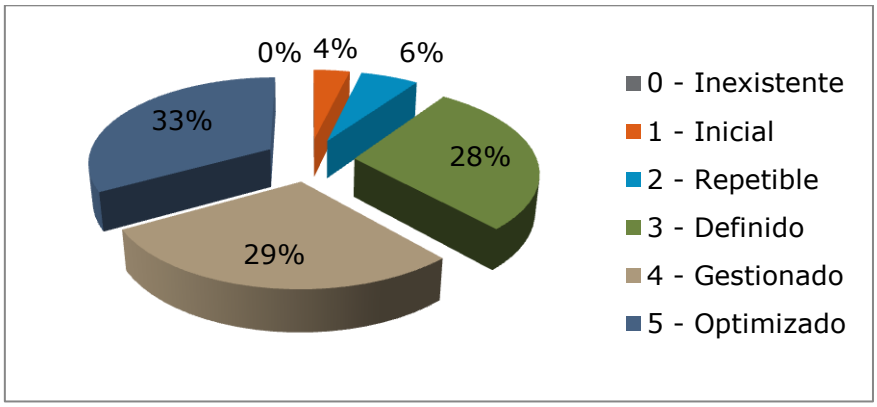

Figura 6-1: Representación gráfica del nivel de madurez de los controles implantados en la organización

Por otro lado, la Tabla 6-4 muestra la información referente al nivel de cumplimiento por dominios de la norma.

Dominio	Nivel de madurez	% Efectividad
5. Política de seguridad	4 - Gestionado	95%
6. Aspectos organizativos de la seguridad de la información	2 - Repetible	80%
7. Gestión de activos	3 - Definido	92%
8. Seguridad ligada a los recursos humanos	4 - Gestionado	95%
9. Seguridad física y del entorno	2 - Repetible	81%
10. Gestión de comunicaciones y operaciones	3 - Definido	94%
11. Control de acceso	2 - Repetible	88%
12. Adquisición, desarrollo y mantenimiento de sistemas de información	2 - Repetible	89%
13. Gestión de incidentes en la seguridad de la información	2 - Repetible	85%
14. Gestión de la continuidad del negocio	3 - Definido	91%
15. Cumplimiento	2 - Repetible	86%

Tabla 6-4: Nivel de cumplimiento de los dominios de la norma ISO/IEC 27002:2005

Se puede observar este nivel de cumplimiento de forma más gráfica mediante el gráfico de radar que muestra la Figura 6-2. En este caso, y para ser más precisos, el nivel de cumplimiento se expresa en función del porcentaje de implantación de cada uno de los dominios en la organización.

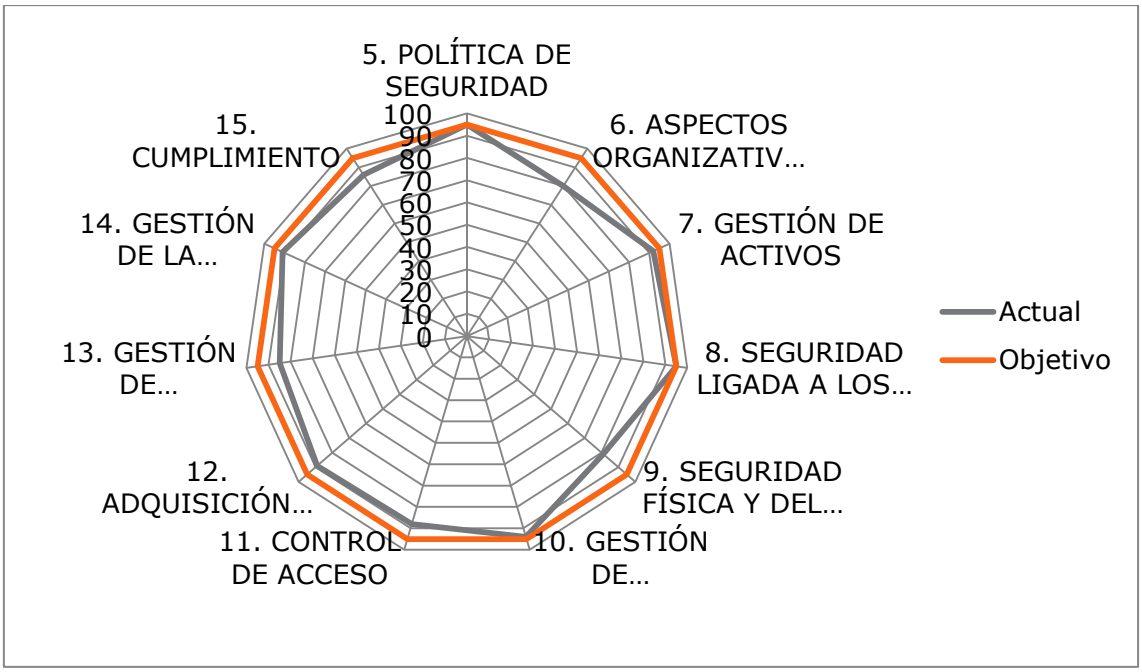

Figura 6-2: Representación gráfica del nivel de cumplimiento de los dominios de la norma ISO/IEC 27002:2005

CAPÍTULO 7. CONCLUSIONES

Tras la realización del Trabajo Fin de Máster, podemos concluir que se han cumplido los objetivos marcados al principio para la realización de este Plan de Implementación de la norma ISO/IEC 27001:2005 en una organización:

- Se ha definido de forma clara la situación previa de la organización con respecto a la Seguridad de la Información y se han definido de forma clara los objetivos y beneficios de implantar en la misma un SGSI.
- Se ha establecido y desarrollado todo el esquema documental necesario para que el SGSI cumpla con los requisitos que la norma tiene al respecto.
- Se ha realizado un análisis de riesgos en la organización, que ha permitido identificar las amenazas más graves y los puntos más débiles de seguridad en la organización.
- Se ha llevado a cabo una serie de propuestas de proyectos que ayudarán a mejorar la gestión de la seguridad en la organización.
- Se ha realizado una evaluación del nivel de cumplimiento actual con respecto a la norma ISO/IEC 27002:2005 en la organización, poniendo de manifiesto los beneficios y mejoras obtenidas con la realización de este proyecto en su conjunto.

Además de todas estas consecuciones a nivel de hitos del trabajo se han conseguido otros objetivos. Por un lado, he aprendido en qué consiste el proceso de desarrollo y elaboración de un Plan de Implementación de estas características, lo cual creo que será muy positivo para mi futuro profesional.

Por otro lado, la realización de este proyecto me ha servido para confirmar que el campo de la Gestión de la Seguridad de la Información es un campo que me atrae y me agrada mucho, y es donde me gustaría desempeñar mi labor profesional en un futuro próximo.

BIBLIOGRAFÍA

[1]. **ISACA.** Marco de Riesgos de TI. 2009.

[2]. **International Organization for Standardization.** *Information technology - Security techniques - Information security management systems - Requirements.* s.l. : ISO/IEC, 2005. ISO 27001:2005.

[3]. —. *Information technology - Security techniques - Code of practice for information security management.* s.l. : ISO/IEC, 2005. ISO 27002:2005.

[4]. **Estevan de Quesada, Rafael.** *Auditoría técnica y de certificación.* Barcelona : FUOC, 2009.

[5]. **Wikipedia.org.** Modelo de Capacidad y Madurez (CMM). [En línea] [Citado el: 2 de Marzo de 2015.] http://es.wikipedia.org/wiki/Modelo_de_Capacidad_y_Madurez.

[6]. **INCIBE.** Plan Director de Seguridad. [En línea] [Citado el: 3 de Marzo de 2015.] https://www.incibe.es/empresas/que_te_interesa/Plan_director_de_seguridad/.

[7]. **UNAD.** Fase 1: Planificar: Análisis diferencial para definición del alcance y otras actividades de planeación. [En línea] [Citado el: 3 de Marzo de 2015.] http://datateca.unad.edu.co/contenidos/233003/modulo/modulo-233003-online/511_fase_1_planificar_anlisis_diferencial_para_definicin_del_alcance_y_otras_actividades_de_planeacin.html.

[8]. **Jimeno, Jorge.** Web sobre el circulo de Deming (PDCA). [En línea] [Citado el: 4 de Marzo de 2015.] http://www.pdcahome.com/5202/ciclo-pdca/.

[9]. **Ministerio de Hacienda y Administraciones Públicas.** *MAGERIT - versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro I - Método.* Madrid : Ministerio de Hacienda y Administraciones Públicas, 2012.