Máster Interuniversitario en Seguridad de las Tecnologías de la Información y de las Comunicaciones

Trabajo Final de Máster

Elaboración de un Plan de Implementación de la ISO/IEC 27001:2013

CENTRO DE INVESTIGACIÓN DE TECNOLOGÍAS PARA LAS COMUNICACIONES

Nombre Estudiante: Soraya Mª Jiménez Beamud

Programa: Máster Universitario en Seguridad de las Tecnologías de la Información y de las Comunicaciones (MISTIC)

Área: Sistemas de Gestión de la Seguridad de la Información

Nombre Consultor: Antonio José Segovia Henares

Profesor responsable de la asignatura: Carles Garrigues Olivella

Centro: Universitat Oberta de Catalunya

Fecha entrega: Junio 2016

FICHA DEL TRABAJO FINAL

Título del trabajo:	*Elaboración de un plan de implementación de la ISO/IEC 27001:2013*
Nombre del autor:	*Soraya Mª Jiménez Beamud*
Nombre del consultor/a:	*Antonio José Segovia Henares*
Nombre del PRA:	*Carles Garrigues Olivella*
Fecha de entrega (mm/aaaa):	Junio 2016
Titulación::	Máster Universitario en Seguridad de las Tecnologías de la Información y de las Comunicaciones (MISTIC)
Área del Trabajo Final:	*Sistemas de Gestión de la Seguridad de la Información*
Idioma del trabajo:	*Castellano*
Palabras clave	*Seguridad, ISO 27001, riesgo*

Resumen del Trabajo:

El proyecto que se presenta en este documento forma parte del Trabajo Final de Máster del Máster Interuniversitario de Seguridad de las Tecnologías de la Información y de las Comunicaciones. El objetivo es el desarrollo de un Plan de Implementación de un Sistema de Gestión de Seguridad de la Información en la organización ficticia CEINTECO, un centro de investigación de nuevas tecnologías de las comunicaciones, siguiendo la norma ISO/IEC 27001:2013.

En primer lugar se ha descrito la organización sobre la que se realiza el proyecto y se ha realizado un análisis diferencial respecto a las normas ISO 27001:2013 e ISO 27002:2013 para conocer el punto de partida del proyecto.

En la segunda fase se han definido los documentos necesarios para el cumplimiento normativo de la ISO 27001:2013 política de seguridad, procedimiento de auditorías internas, gestión de indicadores, procedimiento de revisión por la Dirección, gestión de roles y responsabilidades, declaración de aplicabilidad y metodología de análisis de riesgos.

A continuación, en la fase 3, se ha realizado el análisis de riesgos de la organización siguiendo la metodología MAGERIT. Para ello, se han identificado todos los activos de la organización y se han valorado. Posteriormente, se han analizado las posibles amenazas a las que está expuesta la organización y, por último, se ha obtenido el impacto y riesgo potencial de cada uno de los activos identificados.

En la cuarta fase se han planificado diversos proyectos a realizar con el fin de reducir los principales riesgos encontrados y así mejorar el estado de la seguridad de la información de la organización.

En la fase 5, se ha obtenido el grado de madurez de la organización con respecto a las normas ISO 27002:2013 y 27001:2013 y se han presentado los resultados obtenidos.

Tras haber finalizado todas las fases del proyecto, se ha mejorado la seguridad de la información de la organización.

Abstract:

The project present in this document is part of the Master's degree dissertation "Security of Information and Communication Technologies". The aim of the project is to develop an Information Security Management System (ISMS) Implementation Plan of a fictitious organization called CEINTECO, a research center of new communications technologies, following the ISO/IEC 27001:2013 standard.

Firstly, the organization on which the project is implemented has been described. Also, in order to establish the starting point of the project, a differential analysis regarding ISO 27001:2013 and ISO 27002:2013 has been done.

In the project's second phase the documents required to accomplish the ISO 27001:2013 have been defined: security policy, procedure of internal audits, indicators management, management review procedure, roles and responsibilities management, statement of applicability and risk analysis methodology.

In phase 3, the company's risk analysis has been done following MAGERIT methodology. To do this, all the organization's assets have been identified and valued. Subsequently, the potential threats to which the organization is exposed have been analyzed. Finally, the impact and potential risk of each identified asset have been calculated.

In phase 4, different projects have been planned in order to reduce the encountered main risks as well as improve the condition of the organization's information security.

Lastly, the company's ISMS maturity with respect to the ISO 27002:2013 and ISO 27001:2013 standards have been obtained and shown.

After having finalized all the phases of the project, the organization's information security has been improved.

Contenido

ÍNDICE DE IMÁGENES

ÍNDICE DE TABLAS

1. Fase 1: Situación actual: Contextualización, Objetivos y Análisis diferencial.

1.1. Introducción

El objeto del presente documento es elaborar un Plan de Implementación de la norma ISO/IEC 27001:2013, o Plan Director de Seguridad. Éste es un aspecto clave en cualquier organización que desee alinear sus objetivos y principios de seguridad de la información a la normativa internacional de referencia.

La información es, actualmente, uno de los principales activos en la mayoría de las organizaciones y protegerla se ha vuelto de vital importancia. La digitalización de dicha información y el uso de sistemas y procesos informáticos para su tratamiento ha llevado a la aparición de amenazas antes inexistentes, como los virus informáticos, el *hacking* o la ingeniería social. Para luchar contra estas amenazas surgió el término de seguridad de la información, cuya finalidad es asegurar la confidencialidad, integridad y disponibilidad de los sistemas de la información de una empresa haciendo uso de medidas técnicas, organizativas y legales.

Para llevar a cabo las políticas y los objetivos de seguridad, las organizaciones deben plantearse implementar un Sistema de Gestión de la Seguridad de la Información (SGSI). Éste comprende la política, estructura organizativa, los procedimientos y los recursos necesarios para implantar la gestión de la seguridad de la información y proporciona mecanismos para la salvaguarda de los activos de la información y de los sistemas que los procesan, en concordancia con las políticas de seguridad y planes estratégicos de la organización.

Por tanto, un Plan Director de Seguridad constituye la hoja de ruta que debe seguir cualquier empresa para implantar un SGSI y así gestionar de manera adecuada la seguridad de la información, permitiendo conocer tanto el estado actual de la misma como las directrices que debe seguir para mejorarla.

Existen diversos estándares de seguridad de la información con reconocimiento a nivel internacional aplicables a cualquier tipo de organización. Estos estándares son muy buenas guías de referencia para la gestión de la seguridad de la información de la empresa. Entre estos estándares se encuentran las normas de la familia ISO 27000. Éstas son las que van a servir como guía para la realización de este proyecto.

1.2. Familia ISO/IEC 27000

La familia ISO 27000 son un conjunto de normas, estándares, guías e informes técnicos desarrollados por la ISO (*International Organization for Standardization*) y por la IEC (*International Electrotechnical Commision*) que fueron creadas para facilitar la implantación de Sistemas de Gestión de Seguridad de la Información en las organizaciones y que proporcionan un marco de gestión de la seguridad de la información utilizable por cualquier tipo de organización.

1.2.1. Origen

En 1995 apareció por primera vez la norma BS 7799 (BS 7799-1) de BSI (*British Standards Intitution*) con el fin de proporcionar a cualquier empresa un conjunto de buenas prácticas para la gestión de la seguridad de su información.

Tres años más tarde, en 1998, se publicó la segunda parte de la norma BS 7799 (BS 7799-2), que establecía los requisitos de los sistemas de gestión de la seguridad de la información para ser certificable por una entidad independiente.

En 1999 se revisaron ambas normas BS 7799.

En el año 2000 ISO adoptó, sin grandes cambios, la BS 7799-1 y la llamó ISO/IEC 17799.

En 2002 se revisó la BS 7799-2 para adecuarse a la filosofía ISO de sistemas de gestión.

En 2005, ISO publicó como estándar la ISO/IEC 27001, basada en la norma BS 7799-2. También se revisó y actualizó la ISO/IEC 17799.

En el año 2007 la norma ISO/IEC 17799 pasó a denominarse ISO/IEC 27002:2005. En este año también se publicó la ISO/IEC 27006:2007.

En 2008 se publicó la ISO/IEC 27005:2008.

En 2009 se publicaron las ISO/IEC 27000:2009 y la ISO/IEC 27004:2009.

En 2010 se publicó la ISO/IEC 27003.

En 2013 se publican las nuevas versiones de las ISO/IEC 27001 e ISO/IEC 27002.

1.2.2. Estándares de la familia ISO 27000

En la Imagen 1 se muestran algunas de las normas que forman parte de la familia ISO 27000.

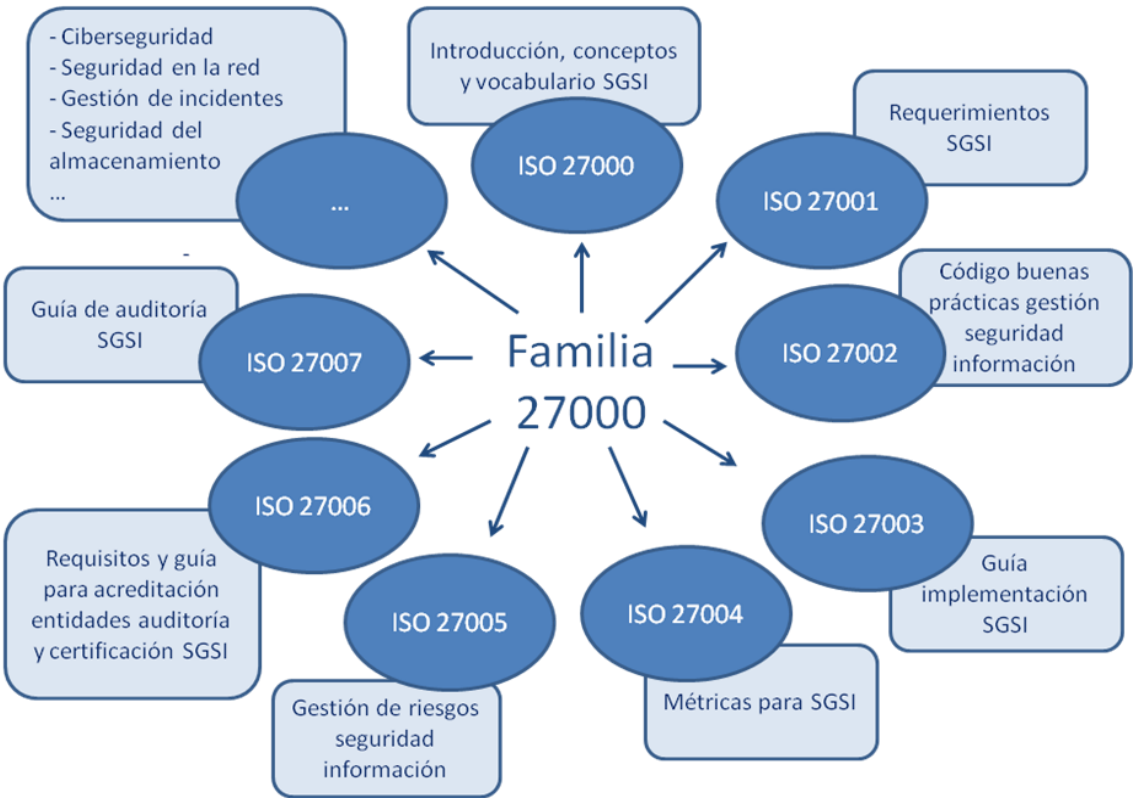


Imagen 1.Familia 27000

De estas normas, la ISO/IEC 27001 y la ISO/IEC 27002 son las que actualmente tienen mayor difusión y aceptación internacional y son en las que se basará el Plan Director de Seguridad de este proyecto.

1.2.3. Norma ISO 27001

La norma ISO/IEC 27001 recoge los requerimientos para la implantación de un sistema de gestión de la seguridad de la información y es la única norma certificable de la familia 27000. La certificación de la norma ISO/IEC 27001 confirma que la seguridad de la información de la empresa certificada ha sido implementada en cumplimiento con esta norma.

La primera versión de esta norma se publicó en 2005 reemplazando al estándar BS 7799:2, que era el utilizado hasta entonces para la gestión de la seguridad de la información.

La estructura que seguía la norma ISO 27001:2005 se muestra en la Imagen 2.

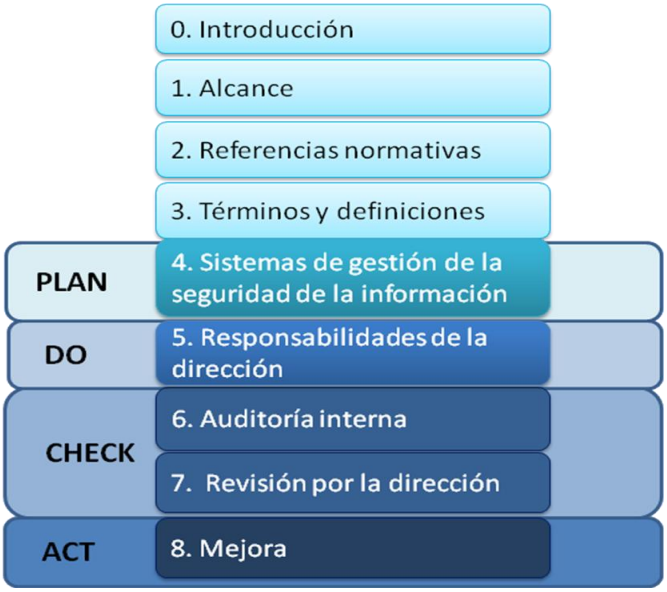


Imagen 2. Estructura ISO 27001:2005

En 2013 se publicó una nueva versión de la norma ISO 27001, la ISO/IEC 27001:2013, que es la utilizada actualmente por las organizaciones. Esta versión introdujo una serie de cambios respecto a la versión de 2005:

- Cambio en la estructura del documento para alinear bajo una misma estructura todos los documentos relacionados con los distintos sistemas de gestión existentes.
- Unificación de todos los términos comunes y las definiciones para los estándares de la gestión de sistemas.
- Eliminación de algunas definiciones y términos existentes en la versión de 2005.
- Eliminación de la sección "Enfoque del proceso" donde se describía el modelo PDCA (Plan - Do - Check - Act).
- Modificación del anexo A, en el que se pasa de tener 11 dominios a 14 y el número total de controles se reduce de 133 a 114 controles. Para ello, se han suprimido alguno de los controles de la versión de 2005, otros se han combinado y también se han creado algunos nuevos.
- Eliminación de los anexos B y C.

La nueva estructura de la norma ISO 27001:2013 queda como se muestra a continuación en la Imagen 3.

Imagen 3. Estructura ISO 27001:2013

1.2.4. Norma ISO/IEC 27002: Código de buenas prácticas

La norma ISO/IEC 27002 se trata de un 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 ISO 27001 toma como referencia a la hora de seleccionar los controles de seguridad.

Esta norma se utiliza en las organizaciones para cubrir cualquiera de los siguientes objetivos:

- Formular los requerimientos y objetivos de seguridad de la información.
- Asegurar que los riesgos de seguridad se gestionan de manera efectiva.
- Asegurar el cumplimiento de las leyes y regulaciones existentes.
- Implementar y gestionar los controles necesarios para asegurar que se alcanzan los objetivos de seguridad definidos.
- Definir nuevos procesos de gestión de seguridad o identificar y clarificar los existentes.
- Conocer el estado de las actividades de gestión de la seguridad por parte de la Dirección.
- Conocer el grado de cumplimiento de las políticas, directivas y estándares adoptados por la empresa, por parte de auditores internos y/o externos.
- Establecer políticas, directivas, estándares o procedimientos de seguridad de la información en las relaciones con terceros.

- Convertir la seguridad de la información en un facilitador del negocio.
- Proporcionar información relevante sobre el estado de la seguridad de la información a los clientes.

En la primera versión de esta norma, ISO 27002:2005, se incluyeron 11 dominios, 39 objetivos de seguridad y 133 controles.

En la Imagen 4 se muestran los dominios existentes en la versión 2005 de la ISO 27002.

Imagen 4. Dimensiones ISO 27002:2005

En 2013 se publicó una nueva versión de esta norma, la ISO 27002:2013 en la que se modificaron la cantidad de dominios y de controles, pasando a ser 14 los dominios y 114 los controles. Los 14 dominios son los que se muestran en la Imagen 5.

Imagen 5. Dimensiones ISO 27002:2013

1.3. Contextualización

La empresa CEINTECO es un centro de investigación y desarrollo de nuevas tecnologías para las comunicaciones, creada hace 10 años y ubicada en el parque científico de una universidad pública, donde desarrolla sus actividades de Investigación, Desarrollo e Innovación (I+D+i) en el área de las tecnologías de las comunicaciones.

Cuenta con un total de 85 empleados que se encuentran repartidos en distintas áreas: dirección, administración, equipo técnico y cuatro grupos de investigación, todos ubicados en el mismo edificio pero en plantas diferentes.

CEINTECO participa en importantes proyectos de I+D+i de financiación pública tanto nacionales como internacionales, así como en proyectos con empresas privadas punteras del sector realizando desarrollos.

Cada uno de los cuatro grupos de investigación de CEINTECO centra sus actividades en un área diferente de investigación. Dichas áreas son:

- Comunicaciones móviles.
  - ✓ Soluciones tecnológicas para sistemas y redes de comunicaciones móviles.
- Comunicaciones ópticas.
  - ✓ Comunicaciones ópticas de señales analógicas y digitales.
  - ✓ Sistemas de radio sobre fibra.
- Aplicaciones multimedia.
  - ✓ Comunicaciones multimedia sobre redes IP: Calidad de Servicio y Calidad de Experiencia.
  - ✓ Audio envolvente.
  - ✓ Televisión inmersiva.
- Antenas y microondas.
  - ✓ Diseño de antenas y dispositivos de comunicaciones en el rango de microondas.
  - ✓ Sistemas de comunicaciones espaciales.

CEINTECO tiene algunas medidas de seguridad implantadas. Sin embargo, éstas no se implantaron bajo ningún sistema de gestión puesto el centro empezó con pocos empleados y en aquel momento se pensó que no era necesario.

Sin embargo, en los últimos años el número de empleados se ha visto incrementado así como la cantidad de proyectos de investigación y desarrollo que se llevan a cabo en la empresa. Esto, junto al gran número de nuevas amenazas que surgen cada día contra los sistemas de información de las empresas, ha llevado al equipo de dirección a plantearse la necesidad de implementar un Sistema de Gestión de Seguridad de la Información, y han decidido que éste se base en la ISO 27001:2013 para poder certificarse en esta norma a largo plazo, una vez estén todas las medidas implantadas y funcionando correctamente.

1.3.1. Organigrama

Como se ha mencionado en el apartado anterior, la empresa se encuentra estructurada en distintas áreas. Éstas son:

- Equipo directivo, 4 personas.
- Administración, 2 personas.
- Equipo técnico, 1 persona.

- Grupos de investigación, 78 personas repartidas en cuatro grupos.

El organigrama de la empresa se muestra a continuación en la Imagen 6.

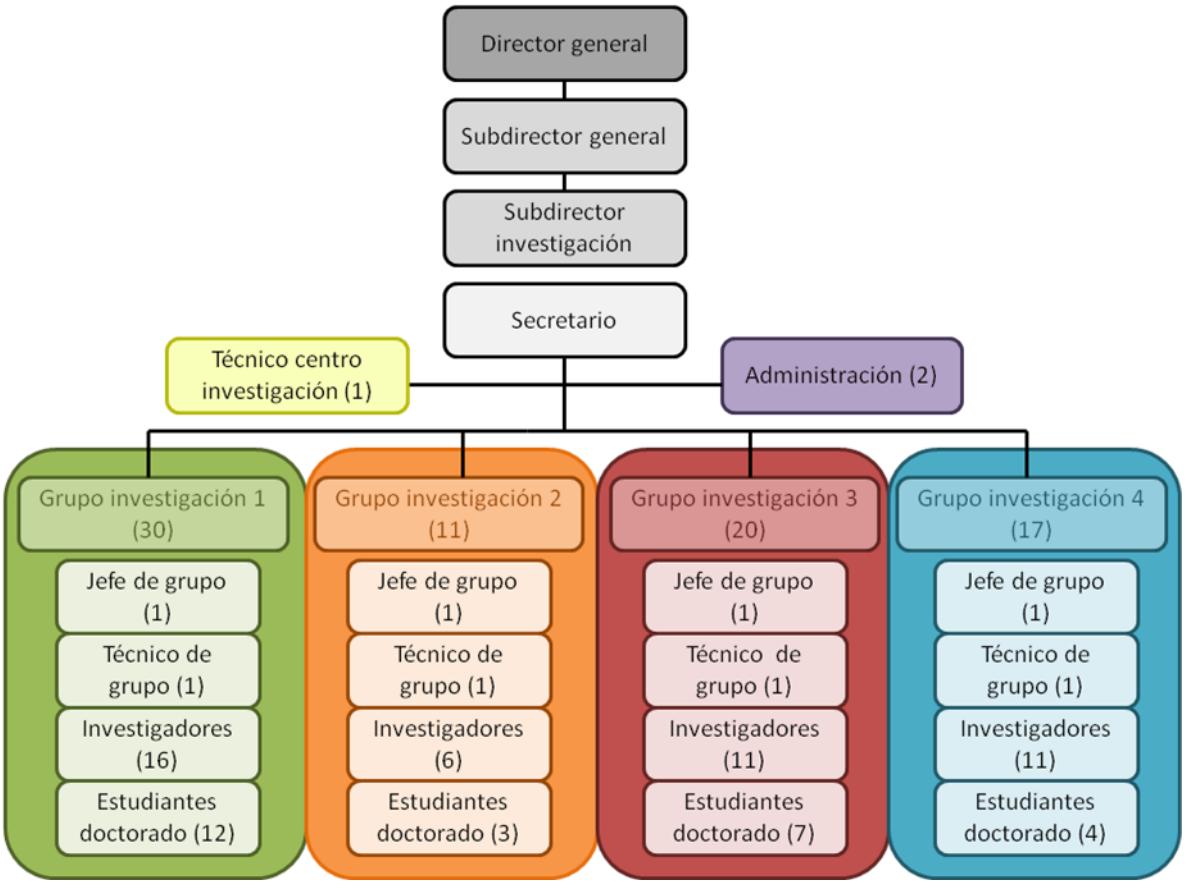


Imagen 6. Organigrama de CEINTECO

El equipo directivo de la empresa está formado por el director, el subdirector, el subdirector de investigación y el secretario. A continuación se ofrece un breve resumen de cada puesto.

- Director general. Es el máximo responsable de la empresa y el encargado de llevar las relaciones de la compañía con el exterior. Es el encargado de firmar los contratos con las empresas externas, universidades, etc.

- Subdirector general. Es la persona encargada de planificar la estrategia de la empresa y de adoptar las responsabilidades del director cuando este no está.

- Subdirector de investigación. Es la persona que hace de enlace entre la dirección y los distintos grupos de investigación de la organización así como con el departamento de investigación general de la universidad. También es la responsable de la actualización de las respectivas bases de datos con los resultados obtenidos en las investigaciones y la encargada de que se realicen actividades de formación para los empleados de la organización.

- Secretario. Es la persona encargada de asistir al director y de vigilar el buen funcionamiento de la empresa. Se encarga de la publicación de revista científica de publicación interna donde se destacan los resultados de investigación más importantes de los diferentes grupos durante el año.

El equipo de administración de la organización está formado por dos personas. Éstas se encargan de la gestión documental, es decir, de los contratos, nóminas, facturas, comunicación con RRHH de la universidad, datos empleados, etc. También se encargan de tomar las huellas a los nuevos empleados para que el técnico las introduzca en la base de datos de huellas.
En cada grupo de investigación podemos encontrar cuatro tipos de trabajadores:

- Jefe de grupo. Es la persona responsable del grupo de investigación al que pertenece. Entre sus funciones se encuentran las siguientes:

  - Realización de propuestas de proyectos de investigación con financiación pública.
  - Negociación, junto a la dirección, proyectos con empresas privadas.
  - Asistencia a las reuniones con los clientes.
  - Velar por el buen funcionamiento del grupo de investigación del grupo.
  - Realización el seguimiento de los proyectos de investigación del grupo.
  - Reporte de los progresos de los proyectos del grupo a la dirección.
  - Dirección y gestión de tesis doctorales

- Investigadores. Son las personas que trabajan investigando y/o desarrollando los distintos proyectos que se están llevando a cabo en el grupo de investigación al que pertenecen. Algunas de sus funciones son:

  - Investigación y desarrollo de los proyectos que se realizan en el grupo.
  - Realización de experimentos y/o medidas en el laboratorio del grupo.
  - Realización de desarrollos teóricos.
  - Desarrollo de software y hardware.
  - Diseminación de los resultados de las investigaciones en revistas, conferencias, seminarios, etc.
  - Soporte en la realización de propuestas de proyectos tanto con empresas privadas como de financiación pública.
  - Tutorización de estudiantes.

- Técnico de grupo. En cada grupo de investigación hay un técnico. Algunas de sus funciones son:

  - Soporte en actividades de administración en la gestión de nuevos proyectos.
  - Responsable de dar permisos de acceso a los equipos a los nuevos miembros de su grupo.
  - Responsable del laboratorio del grupo.
  - Mantenimiento básico de los equipos del grupo.
  - Actualización de la página web de la empresa con noticias relevantes sobre el grupo.
  - Responsable del servidor de repositorio de código desarrollado, del de copias de seguridad y de los ordenadores de simulación que utiliza el grupo.

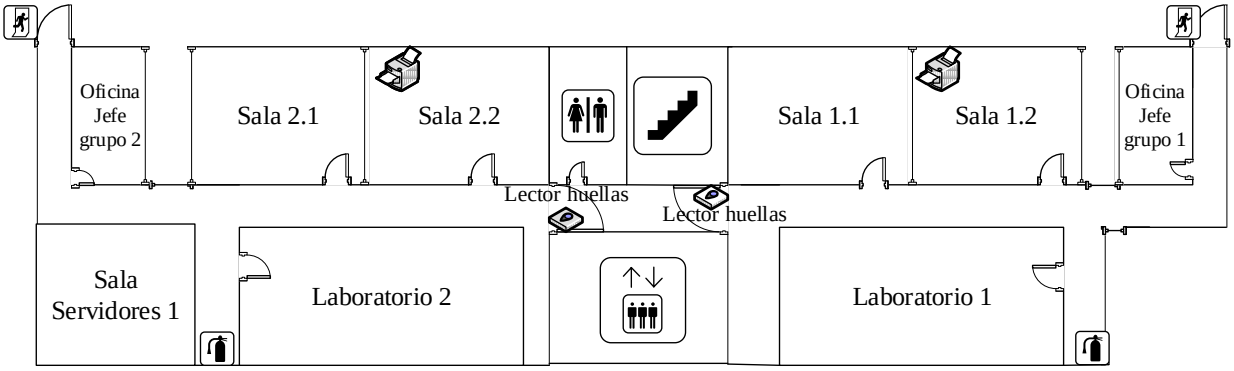
- Estudiantes doctorado. Son personas que se encuentran realizando sus tesis doctorales y cuyo tutor es el jefe de grupo y/o uno de los investigadores del grupo al que pertenecen.

Además de los técnicos de cada grupo, existe la figura del técnico del centro de investigación, que se encarga de las tareas generales de empresa. Algunas de sus funciones son:

  - Responsable del servidor de huellas, del servidor web y del servidor de correo de la organización.
  - Responsable de la gestión del suministro eléctrico, saneamiento, aire acondicionado, calefacción e infraestructura de red.
  - Encargado de la instalación del software básico necesario de los nuevos equipos.

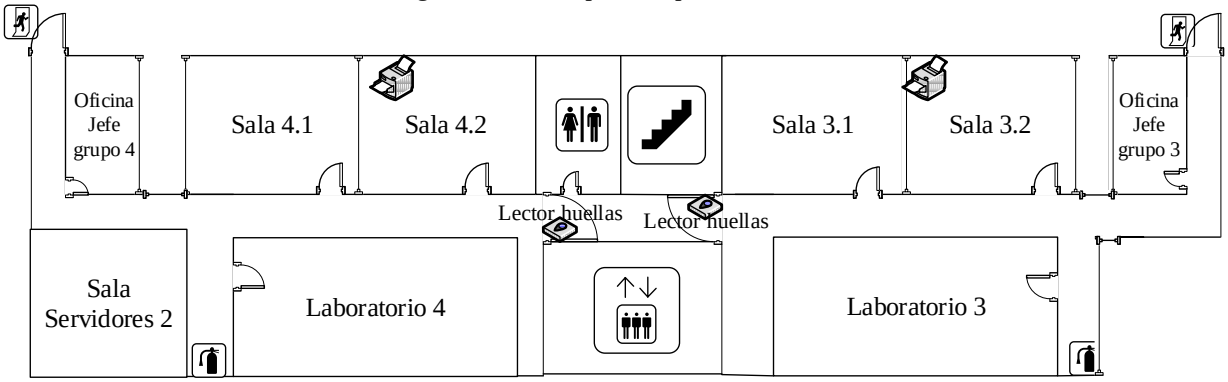
1.3.2. Instalaciones

En cuanto a las instalaciones, se adjuntan en la Imagen 7, Imagen 8 e Imagen 9 los planos orientativos de las tres plantas de oficinas de CEINTECO.



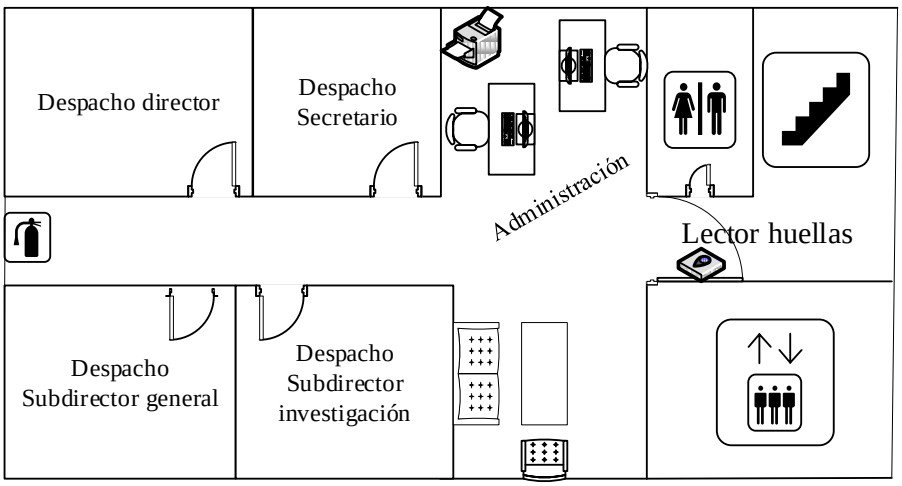
Oficinas primera planta

Imagen 7. Oficinas primera planta



Oficinas segunda planta

Imagen 8. Oficinas segunda planta de CEINTECO



Oficinas tercera planta

Imagen 9. Oficinas tercera planta de CEINTECO

1.3.3. Arquitectura de red

CEINTECO utiliza una arquitectura de red perimetral construida mediante encaminadores con filtrado de paquetes o cortafuegos. El cortafuegos interno (firewall B) protege la red interna de Internet y de la red perimetral, o DMZ. El cortafuegos externo (firewall A) protege la red interna y la perimetral del exterior.

En la DMZ se encuentran el servidor de correo, el servidor web y el servidor con la base de datos de las huellas. Cada grupo de investigación tiene su propia red de área local (LAN). Las salas de servidores también tienen una LAN cada una, así como la oficina de la tercera planta, formada por la administración y los despachos del equipo de dirección.

Además, CEINTECO dispone de un acceso WI-FI para que los trabajadores puedan conectarse a través de sus dispositivos móviles.

La organización tiene contratada una única conexión de red con uno de los proveedores de servicios de Internet más importantes del país.

En la Imagen 10 se detalla la arquitectura de red de la organización.

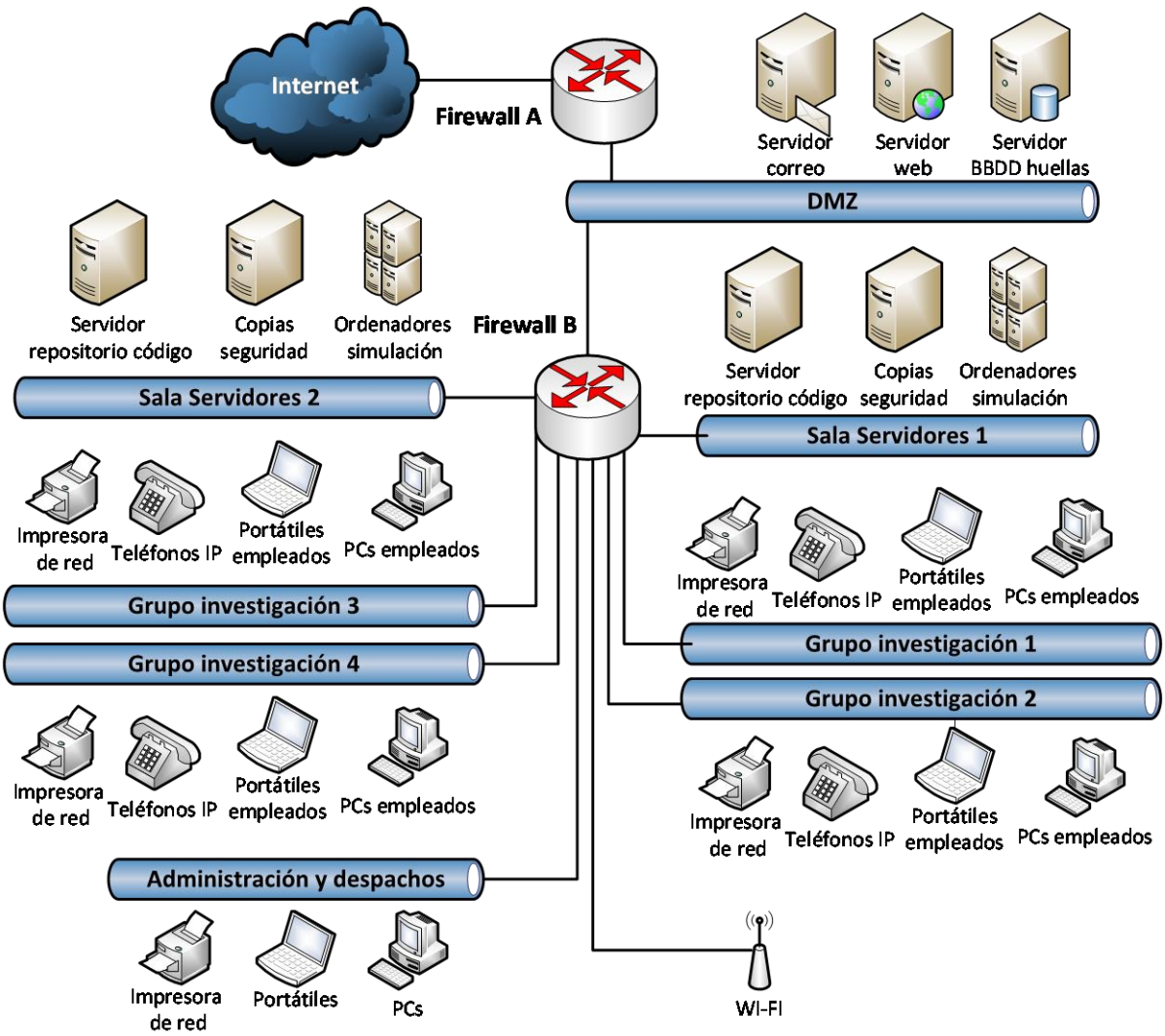


Imagen 10. Arquitectura de red de CEINTECO

1.3.4. Estado inicial de la seguridad de la información

CEINTECO tiene implantadas en sus oficinas algunas medidas de seguridad. Sin embargo, no cuenta con un departamento especializado en seguridad ni ha contratado a ninguna empresa externa para gestionar la seguridad. Son los técnicos, tanto el del centro de investigación como los de grupo, los encargados de controlar la seguridad de la organización y atender los problemas de seguridad que surjan. El técnico se encarga de la seguridad general de la empresa y los técnicos de cada grupo se encargan, a groso modo, de la seguridad de los procesos y sistemas del grupo al que pertenecen.

CEINTECO tiene conocimiento general de los equipos que posee pero no cuenta con un inventario de activos detallado ni ha realizado nunca un análisis de riesgos.

El acceso a los diferentes pasillos donde se encuentran las oficinas y laboratorios se realiza a través de huella digital, en total la organización tiene 5 escáneres de huella instalados. Junto al escáner de huella existe un timbre para que llamen las personas ajenas a la organización y así poder permitirles la entrada. No se dispone de tarjetas de visita ni se registran los visitantes que entran a las oficinas de CEINTECO.

Cada grupo de investigación dispone de una o varias salas donde trabajan los miembros de cada grupo. Para acceder a estas salas se necesita de una llave que abre la puerta. Cada trabajador tiene la llave de su sala. Las salas se abren por la mañana por primera vez y suelen permanecer abiertas hasta que el último empleado de la sala acaba su jornada laboral.

Todos los grupos disponen de un laboratorio propio en el que se encuentra disponible el equipamiento necesario para hacer los experimentos y medidas oportunas. Para acceder a cada laboratorio también es necesaria una llave.

Cada grupo dispone de una impresora de red ubicada en una de las salas del grupo a la que sólo se puede acceder si el empleado se encuentra en la misma LAN que la impresora, por lo que habitualmente sólo es utilizada por los miembros del grupo en el que se encuentra la impresora. Además, en la sala donde se encuentran ubicados los trabajadores de administración hay otra impresora que puede utilizar cualquier empleado siempre que se conecten a ella utilizando una contraseña. No existe ningún control de los documentos que se quedan en las impresoras sin recoger y nadie borra nunca la memoria de las impresoras.

Cada una de las salas de cada grupo dispone de una pequeña caja fuerte protegida con un candado de combinación numérica que contiene la llave de las otras salas del grupo y la del laboratorio. La combinación numérica no suele cambiarse a menudo y todos los trabajadores emplazados en la sala la conocen. Además, el técnico del centro de investigación dispone de todas las llaves del laboratorio.

Por otra parte, en cada planta donde están ubicados los grupos de investigación existe una sala que dispone de aire acondicionado donde se encuentran los ordenadores de simulación, el sistema de respaldo eléctrico, el servidor de copias de seguridad y el servidor con el repositorio de código. Para acceder a estas salas es necesaria una llave que únicamente poseen los técnicos de cada grupo y el técnico del centro. Por tanto, sólo está permitido el acceso a esta sala a los técnicos. El acceso a los servidores se realiza mediante un usuario y contraseña, no necesariamente robusta, que únicamente conocen los técnicos y que debe cambiarse cada año.

Los equipos que utilizan los empleados para trabajar pueden ser tanto ordenadores de sobremesa como ordenadores portátiles. En el caso de los ordenadores portátiles, no existe ningún sistema de seguridad físico para impedir que alguien se los pueda llevar.

Para el acceso a los ordenadores, cada trabajador dispone de un usuario y contraseña. No hay ningún sistema que obligue a utilizar una contraseña robusta ni a cambiar la contraseña cada cierto tiempo. Además, para acceder al sistema de gestión de nóminas de cada empleado, éstos necesitan de otra contraseña que sí debe ser robusta y deben cambiar cada año.

No existe ninguna política sobre el bloqueo de los equipos de cada trabajador, por lo que depende de cada empleado el bloquear su equipo cada vez que se aleja de él. Además, los trabajadores suelen tener los puestos de trabajo con papeles y documentos relacionados con el trabajo que están realizando.

El centro dispone de WI-FI protegida con WPA2 a la que los trabajadores pueden conectarse utilizando sus dispositivos móviles, tanto los de la empresa como los propios.

No existe una política de copias de seguridad general a toda la empresa ni existe un proceso automatizado que las realice. Los trabajadores son los encargados de realizar las copias de seguridad de sus equipos cuando ellos creen conveniente. Los técnicos de grupo son los encargados de realizar las copias de seguridad de los servidores que tienen a su cargo y las suelen realizar una vez por semana, si no se olvidan.

Todo trabajador firma un acuerdo de confidencialidad en el momento que es contratado. Por otra parte, cuando una persona deja la empresa o es despedida, no se revocan sus permisos de manera inmediata. Existe un proceso que se ejecuta cada tres meses que revisa los permisos de los trabajadores y, si encuentra alguna incoherencia lo da de baja de todas las bases de datos correspondientes.

1.3.5. Alcance SGSI

El alcance del Sistema de Gestión de Seguridad de la Información de CEINTECO va a abarcar todos los procesos y sistemas de la organización que permiten llevar a cabo las operaciones de negocio de ésta. Esto incluye todas las áreas físicas de la empresa, todos los sistemas de información que sean tratados en la organización, incluidos los sistemas de información que dan soporte al área de administración y dirección, y los procesos y sistemas de investigación y desarrollo de los distintos grupos de investigación. Todo esto de acuerdo con la Declaración de Aplicabilidad de CEINTECO.

1.4. Objetivos del Plan Director

El Plan Director, también conocido como Plan de Seguridad de la Información, consiste en la definición y priorización de un conjunto de proyectos en materia de seguridad de la información cuyo objetivo es reducir los riesgos a los que está expuesta la organización hasta unos niveles aceptables, a partir de un análisis de la situación inicial.

Para la realización de un buen Plan Director es necesario que éste recoja los objetivos estratégicos de la empresa, la definición del alcance y las obligaciones y buenas prácticas de seguridad que deberán cumplir los trabajadores.

Los objetivos del Plan Director de Seguridad son:

- ✓ Asegurar la protección de los activos y la información de organización.
- ✓ Cumplir con la legislación y regulaciones vigentes referentes al tratamiento de datos sensibles.

- ✓ Incrementar la confianza que las empresas privadas tienen en CEINTECO.
- ✓ Certificar el SGSI en la norma ISO 27001 para atraer a nuevas empresas externas.
- ✓ Lograr la concienciación y colaboración de todos los trabajadores de CEINTECO en materia de seguridad de la información.

Para lograr estos objetivos se deberá:

- ✓ Conocer el estado actual de la seguridad de la información de CEINTECO.
- ✓ Identificar los riesgos que puedan afectar a la empresa, consiguiendo con ello minimizar las posibles amenazas.
- ✓ Formar a los trabajadores para el uso seguro de los activos de la organización.
- ✓ Establecer de una manera clara los roles de los trabajadores en lo referente a la seguridad de la información.
- ✓ Definir los controles de seguridad a implementar.
- ✓ Establecer los indicadores y métricas para controlar el cumplimiento de las medidas seguridad de la información.
- ✓ Definir un plan de continuidad de negocio para evitar la interrupción de las actividades de negocio por ataques o fallos de seguridad.

En la Imagen 11 se muestran las fases que debe seguir todo Plan Director de Seguridad.

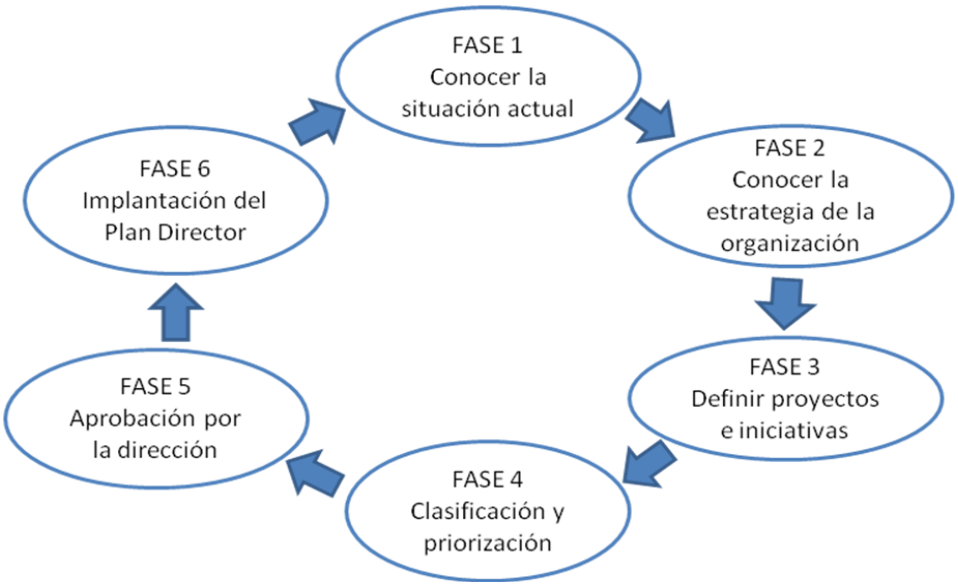


Imagen 11. Fases de un Plan Director de Seguridad

Una vez se haya implantado el Plan Director de Seguridad de CEINTECO, se deberá realizar un seguimiento periódico de los controles y proyectos establecidos para comprobar si los objetivos de seguridad fijados se están consiguiendo.

Para ello se establecerán distintos indicadores que facilitarán la generación de informes en los que se detalle el estado de la seguridad de la información de CEINTECO, así como procedimientos para detectar y notificar las incidencias o situaciones de seguridad deficiente.

Además de esto, también se realizarán auditorías internas que ayudarán a conocer si se están cumpliendo los objetivos de seguridad.

En capítulos posteriores se detallarán los distintos indicadores que se utilizarán para medir el cumplimiento de los objetivos del Plan Director así como el procedimiento que seguirá la organización para la realización de las auditorías internas.

1.5. Análisis diferencial

En el presente apartado se va a realizar un análisis de madurez de las medidas de seguridad ya implantadas en la organización en relación a la seguridad de la información. Este análisis se va a hacer en base a las normas ISO 27001:2013 e ISO 27002:2013.

Este análisis diferencial nos va a permitir conocer de manera global el estado actual de la empresa en relación a la seguridad de la información.

Se va a utilizar como modelo de evaluación de las medidas de seguridad ya implantadas en la organización el Modelo de Madurez de Capacidades (CCM) definido por el *Software Engineering Institute*. La aplicación de este modelo de madurez permite establecer criterios objetivos para la evaluación de la eficacia de los controles gracias a la repetitividad de la medida, permitiendo así analizar su evolución en el tiempo.

En la Tabla 1 se definen los niveles de capacidad que se van a utilizar.

Nivel	Efectividad	Significado	Descripción
L0	0%	Inexistente	• Ausencia total de proceso reconocible. • La organización no ha reconocido la existencia del problema.
L1	10%	Inicial	• La organización ha reconocido la existencia del problema y la necesidad de resolverlo. • No hay procesos estandarizados pero sí hay métodos ad hoc que tienden a ser aplicados de manera individual. • Resultados impredecibles y pobremente controlados.
L2	50%	Repetible	• Los procesos se han desarrollado y diferentes personas siguen procedimientos similares realizando la misma tarea. • No hay comunicación formal de procesos estándar y la responsabilidad recae en la persona. • Existe la posibilidad de que haya errores debido a la alta confianza en los conocimientos de las personas.
L3	90%	Definido	• Los procedimientos han sido estandarizados, documentados y comunicados. Son conocidos y bien entendidos. • El seguimiento de los procesos se ha dejado en mano de la persona y es complicado que se detecten desviaciones. • Los procedimientos no son sofisticados.
L4	95%	Administrado	• Es posible monitorear y medir el cumplimiento de los procedimientos y emprender acciones en aquellos que no estén funcionando correctamente. • Los procesos se encuentran en constante mejora y proveen buenas prácticas.
L5	100%	Optimizado	• Los procesos han sido refinados hasta un nivel de la mejor práctica, basados en los resultados de mejora continua y diseño de madurez de la organización.

Tabla 1. Niveles de capacidad del Modelo de Madurez de Capacidades (CCM)

La Tabla 2 muestra el análisis diferencial de las medidas de seguridad que CEINTECO tiene actualmente implantadas respecto las secciones que conforman la norma ISO 27001:2013.

ID	Sección ISO 27001:2013	Situación
4	**CONTEXTO DE LA ORGANIZACIÓN**	
4.1	Comprensión de la organización y de su contexto	L3 - Definido
4.2	Comprensión de las necesidades y expectativas de las partes interesadas	L1 - Inicial
4.3	Determinación del alcance del SGSI	L0 - Inexistente
4.4	SGSI	L0 - Inexistente
5	**LIDERAZGO**	
5.1	Liderazgo y compromiso	L1 - Inicial
5.2	Política	L0 - Inexistente
5.3	Roles, responsabilidades y autoridades en la organización	L1 - Inicial
6	**PLANIFICACIÓN**	
6.1	Acciones para hacer frente a los riesgos y oportunidades	
6.1.1	General	L0 - Inexistente
6.1.2	Valoración de los riesgos de seguridad de la información	L0 - Inexistente
6.1.3	Tratamiento de los riesgos de seguridad de la información	L0 - Inexistente
6.2	Objetivos de seguridad de la información y planificación para conseguirlos	L0 - Inexistente
7	**SOPORTE**	
7.1	Recursos	L1 - Inicial
7.2	Competencia	L2 - Repetible
7.3	Concienciación	L2 - Repetible
7.4	Comunicación	L2 - Repetible
7.5	Información documentada	
7.5.1	General	L0 - Inexistente
7.5.2	Creando y actualizando	L0 - Inexistente
7.5.3	Control de la información documentada	L0 - Inexistente
8	**OPERACIÓN**	
8.1	Planificación y control	L0 - Inexistente
8.2	Valoración de los riesgos de la seguridad de la información	L0 - Inexistente
8.3	Tratamiento de los riesgos de la seguridad de la información	L0 - Inexistente
9	**EVALUACIÓN**	
9.1	Seguimiento, medición, análisis y evaluación	L0 - Inexistente
9.2	Auditoría interna	L0 - Inexistente
9.3	Revisión por la dirección	L0 - Inexistente
10	**MEJORA**	
10.1	No conformidad y acciones correctivas	L0 - Inexistente
10.2	Mejora continua	L0 - Inexistente

Tabla 2. Análisis diferencial respecto a ISO 27001:2013

Si hacemos una media de la situación de los distintos puntos de cada sección y cambiamos la escala para verla en porcentaje, obtenemos una evaluación general de cada apartado de la ISO 27001. El estado actual de la implementación de la ISO 27001 en CEINTECO se muestra en la Tabla 3.

Sección ISO 27001:2013	% Efectividad
4. CONTEXTO DE LA ORGANIZACIÓN	92,5%
5. LIDERAZGO	6,66%
6. PLANIFICACION	0%
7. SOPORTE	22,85%
8. OPERACIÓN	0%
9. EVALUACION	0%
10. MEJORA	0%

Tabla 3. Estado actual implementación ISO 27001:2013

A continuación, en la Imagen 12, se muestra el estado actual de implementación de la ISO 27001 comparado con el estado al que se quiere llegar tras la implementación del SGSI y con el que sería el estado óptimo. En este caso, la línea azul representa el estado actual de cumplimiento de la norma, la línea roja un posible objetivo de cumplimiento a medio o largo plazo y, por último, la línea verde representa el nivel de cumplimiento óptimo. Los números que se muestran en la gráfica hacen referencia a las diferentes secciones contempladas en la ISO 27001:2013.

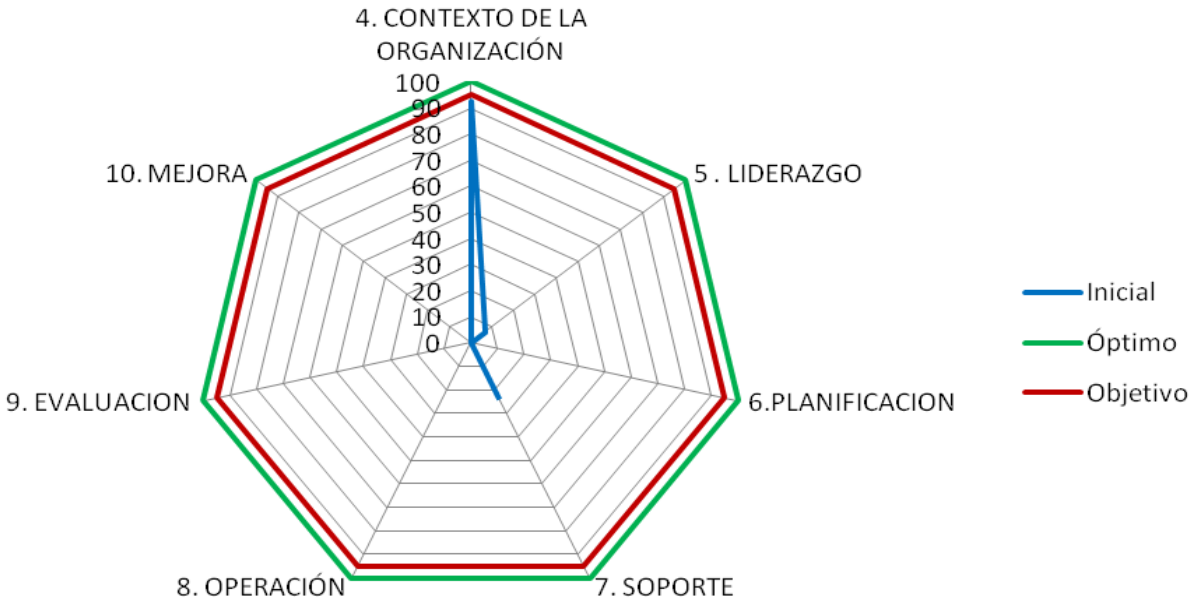


Imagen 12. Diagrama estado implementación ISO 27001:2013

La Tabla 4 muestra el análisis diferencial de las medidas de seguridad que CEINTECO tiene actualmente implantadas respecto a los controles que conforman la norma ISO 27002:2013.

ID	Control ISO 27002:2013	Situación
A.5	**POLÍTICAS DE SEGURIDAD**	
A.5.1	**Directrices de la Dirección en seguridad de la información**	
A.5.1.1	Conjunto de políticas para la seguridad de la información	L0 - Inexistente
A.5.1.2	Revisión de las políticas para la seguridad de la información	L0 - Inexistente
A.6	**ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMACIÓN**	
A.6.1	**Organización interna**	
A.6.1.1	Asignación de responsabilidades para la seguridad de la información	L2 - Repetible
A.6.1.2	Segregación de tareas	L2 - Repetible
A.6.1.3	Contacto con las autoridades	L0 - Inexistente
A.6.1.4	Contacto con grupos de interés especial	L0 - Inexistente
A.6.1.5	Seguridad de la información en la gestión de proyectos	L1 - Inicial
A.6.2	**Dispositivos para movilidad y teletrabajo**	
A.6.2.1	Política de uso de dispositivos para movilidad	L0 - Inexistente
A.6.2.2	Teletrabajo	L0 - Inexistente
A.7	**SEGURIDAD LIGADA A LOS RECURSOS HUMANOS**	
A.7.1	**Antes de la contratación**	
A.7.1.1	Investigación de antecedentes	L0 - Inexistente
A.7.1.2	Términos y condiciones de contratación	L3 - Definido
A.7.2	**Durante la contratación**	
A.7.2.1	Responsabilidades de gestión	L3 - Definido
A.7.2.2	Concienciación, educación y capacitación en seguridad de la información	L0 - Inexistente
A.7.2.3	Proceso disciplinario	L0 - Inexistente
A.7.3	**Cese o cambio de puesto de trabajo**	
A.7.3.1	Cese o cambio de puesto de trabajo	L3 - Definido
A.8	**GESTIÓN DE ACTIVOS**	
A.8.1	**Responsabilidad sobre los activos**	
A.8.1.1	Inventario de activos	L2 - Repetible
A.8.1.2	Propiedad de los activos	L0 - Inexistente
A.8.1.3	Uso aceptable de los activos	L2 - Repetible
A.8.1.4	Devolución de los activos	L5 - Optimizado
A.8.2	**Clasificación de la información**	
A.8.2.1	Directrices de clasificación	L0 - Inexistente
A.8.2.2	Etiquetado y manipulado de la información	L0 - Inexistente
A.8.2.3	Manipulación de activos	L3 - Definido

A.8.3	**Manejo de los soportes de almacenamiento**	
A.8.3.1	Gestión de los soportes extraíbles	L2 - Repetible
A.8.3.2	Eliminación de soportes	L0 - Inexistente
A.8.3.3	Soportes físicos en tránsito	L2 - Repetible
A.9	**CONTROL DE ACCESOS**	
A.9.1	**Requisitos de negocio para el control de accesos**	
A.9.1.1	Política de control de accesos	L3 - Definido
A.9.1.2	Control de acceso a las redes y servicios asociados	L3 - Definido
A.9.2	**Gestión de acceso de usuario**	
A.9.2.1	Gestión de altas/bajas en el registro de usuarios	L3 - Definido
A.9.2.2	Gestión de los derechos de acceso asignados a usuarios	L3 - Definido
A.9.2.3	Gestión de los derechos de acceso con privilegios especiales	L3 - Definido
A.9.2.4	Gestión de información confidencial de autenticación de usuarios	L0 - Inexistente
A.9.2.5	Revisión de los derechos de acceso de los usuarios	L0 - Inexistente
A.9.2.6	Retirada o adaptación de los derechos de acceso	L3 - Definido
A.9.3	**Responsabilidades del usuario**	
A.9.3.1	Uso de información confidencial para la autenticación	L1 - Inicial
A.9.4	**Control de acceso a sistemas y aplicaciones**	
A.9.4.1	Restricción del acceso a la información	L3 - Definido
A.9.4.2	Procedimientos seguros de inicio de sesión	L4 -Administrado
A.9.4.3	Gestión de contraseñas de usuario	L2 - Repetible
A.9.4.4	Uso de herramientas de administración de sistemas	L1 - Inicial
A.9.4.5	Control de acceso al código fuente de los programas	L3 - Definido
A.10	**CIFRADO**	
A.10.1	**Controles criptográficos**	
A.10.1.1	Política de uso de los controles criptográficos	L0 - Inexistente
A.10.1.2	Gestión de claves	L0 - Inexistente
A.11	**SEGURIDAD FÍSICA Y AMBIENTAL**	
A.11.1	**Áreas seguras**	
A.11.1.1	Perímetro de seguridad física	L3 - Definido
A.11.1.2	Controles físicos de entrada	L3 - Definido
A.11.1.3	Seguridad de oficinas, despachos y recursos	L3 - Definido
A.11.1.4	Protección contra las amenazas externas y ambientales	L3 - Definido
A.11.1.5	El trabajo en áreas seguras	L2 - Repetible
A.11.1.6	Áreas de acceso público, carga y descarga	L1 - Inicial
A.11.2	**Seguridad de los equipos**	
A.11.2.1	Emplazamiento y protección de equipos	L0 - Inexistente

A.11.2.2	Instalaciones de suministro	L3 - Definido
A.11.2.3	Seguridad del cableado	L2 - Repetible
A.11.2.4	Mantenimiento de los equipos	L2 - Repetible
A.11.2.5	Salida de activos fuera de las dependencias de la empresa	L3 - Definido
A.11.2.6	Seguridad de los equipos y activos fuera de las instalaciones	L2 - Repetible
A.11.2.7	Reutilización o retirada segura de dispositivos de almacenamiento	L2 - Repetible
A.11.2.8	Equipo informático de usuario desatendido	L1 - Inicial
A.11.2.9	Política de puesto de trabajo despejado y bloqueo de pantalla	L1 - Inicial
A.12	**SEGURIDAD EN LA OPERATIVA**	
A.12.1	**Responsabilidades y procedimientos de operación**	
A.12.1.1	Documentación de procedimientos de operación	L0 - Inexistente
A.12.1.2	Gestión de cambios	L2 - Repetible
A.12.1.3	Gestión de capacidades	L0 - Inexistente
A.12.1.4	Separación de entornos de desarrollo, prueba y producción	L0 - Inexistente
A.12.2	**Protección contra código malicioso**	
A.12.2.1	Controles contra el código malicioso	L4 - Administrado
A.12.3	**Copias de seguridad**	
A.12.3.1	Copias de seguridad de la información	L2 - Repetible
A.12.4	**Registro de actividad y supervisión**	
A.12.4.1	Registro y gestión de eventos de actividad	L0 - Inexistente
A.12.4.2	Protección de los registros de información	L0 - Inexistente
A.12.4.3	Registros de actividad del administrador y operador del sistema	L0 - Inexistente
A.12.4.4	Sincronización de relojes	L5 - Optimizado
A.12.5	**Control del software en explotación**	
A.12.5.1	Instalación del software en sistemas en producción	L3 - Definido
A.12.6	**Gestión de la vulnerabilidad técnica**	
A.12.6.1	Gestión de las vulnerabilidades técnicas	L0 - Inexistente
A.12.6.2	Restricciones en la instalación de software	L0 - Inexistente
A.12.7	**Consideraciones de las auditorías de los sistemas de información**	
A.12.7.1	Controles de auditoría de los sistemas de información	L0 - Inexistente
A.13	**SEGURIDAD EN LAS TELECOMUNICACIONES**	
A.13.1	**Gestión de la seguridad en las redes**	
A.13.1.1	Controles de red	L1 - Inicial
A.13.1.2	Mecanismos de seguridad asociados a servicios en red	L0 - Inexistente
A.13.1.3	Segregación de redes	L3 - Definido
A.13.2	**Intercambio de información con partes externas**	
A.13.2.1	Políticas y procedimientos de intercambio de información	L1 - Inicial

A.13.2.2	Acuerdos de intercambio	L0 - Inexistente
A.13.2.3	Mensajería electrónica	L0 - Inexistente
A.13.2.4	Acuerdos de confidencialidad y secreto	L1 - Inicial
A.14	**ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN**	
A.14.1	**Requisitos de seguridad de los sistemas de información**	
A.14.1.1	Análisis y especificación de los requisitos de seguridad	L0 - Inexistente
A.14.1.2	Seguridad de las comunicaciones en servicios accesibles por redes públicas	L0 - Inexistente
A.14.1.3	Protección de las transacciones por redes telemáticas	L0 - Inexistente
A.14.2	**Seguridad en los procesos de desarrollo y soporte**	
A.14.2.1	Política de desarrollo seguro de software	L0 - Inexistente
A.14.2.2	Procedimientos de control de cambios en los sistemas	L0 - Inexistente
A.14.2.3	Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo	L0 - Inexistente
A.14.2.4	Restricciones a los cambios en los paquetes de software	L0 - Inexistente
A.14.2.5	Uso de principios de ingeniería en protección de sistemas	L0 - Inexistente
A.14.2.6	Seguridad en entornos de desarrollo	L0 - Inexistente
A.14.2.7	Externalización del desarrollo software	L0 - Inexistente
A.14.2.8	Pruebas de funcionalidad durante el desarrollo de los sistemas	L0 - Inexistente
A.14.2.9	Pruebas de aceptación	L0 - Inexistente
A.14.3	**Datos de prueba**	
A.14.3.1	Protección de los datos utilizados en pruebas	L3 - Definido
A.15	**RELACIONES CON SUMINISTRADORES**	
A.15.1	**Seguridad de la información en las relaciones con suministradores**	
A.15.1.1	Política de seguridad de la información para suministradores	L0 - Inexistente
A.15.1.2	Tratamiento del riesgo dentro de acuerdos de suministradores	L0 - Inexistente
A.15.1.3	Cadena de suministro en tecnologías de la información y comunicaciones	L3 - Definido
A.15.2	**Gestión de la prestación del servicio por suministradores**	
A.15.2.1	Supervisión y revisión de los servicios prestados por terceros	L0 - Inexistente
A.15.2.2	Gestión de cambios en los servicios prestados por terceros	L0 - Inexistente
A.16	**GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN**	
A.16.1	**Gestión de incidentes de seguridad de la información y mejoras**	
A.16.1.1	Responsabilidades y procedimientos	L2 - Repetible
A.16.1.2	Notificación de los eventos de seguridad de la información	L2 - Repetible
A.16.1.3	Notificación de puntos débiles de la seguridad	L2 - Repetible
A.16.1.4	Valoración de eventos de seguridad de la información y toma de decisiones	L1 - Inicial
A.16.1.5	Respuesta a los incidentes de seguridad	L1 - Inicial

A.16.1.6	Aprendizaje de los incidentes de seguridad de la información	L1 - Inicial
A.16.1.7	Recopilación de las evidencias	L0 - Inexistente
A.17	**ASPECTOS DE LA SEGURIDAD DE LA INFORMACIÓN EN LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO**	
A.17.1	**Continuidad de la seguridad de la información**	
A.17.1.1	Planificación de la continuidad de la seguridad de la información	L0 - Inexistente
A.17.1.2	Implantación de la continuidad de la seguridad de la información	L0 - Inexistente
A.17.1.3	Verificación, revisión y evaluación de la continuidad de la seguridad de la información	L0 - Inexistente
A.17.2	**Redundancias**	
A.17.2.1	Disponibilidad de instalaciones para el procesamiento de la información	L0 - Inexistente
A.18	**CUMPLIMIENTO**	
A.18.1	**Cumplimiento de los requisitos legales y contractuales**	
A.18.1.1	Identificación de la legislación aplicable	L4 - Administrado
A.18.1.2	Derechos de propiedad intelectual (DPI)	L4 - Administrado
A.18.1.3	Protección de los registros de la organización	L3 - Definido
A.18.1.4	Protección de datos y privacidad de la información personal	L3 - Definido
A.18.1.5	Regulación de los controles criptográficos	L1 - Inicial
A.18.2	**Revisiones de la seguridad de la información**	
A.18.2.1	Revisión independiente de la seguridad de la información	L0 - Inexistente
A.18.2.2	Cumplimiento de las políticas y normas de seguridad	L0 - Inexistente
A.18.2.3	Comprobación del cumplimiento	L0 - Inexistente

Tabla 4. Análisis diferencial respecto a ISO 27002:2013

Si hacemos una media de la situación de los distintos controles de cada dimensión y cambiamos la escala para verla en porcentaje, obtenemos una evaluación general de cada dimensión de la ISO 27002. El estado actual de la implementación de la ISO 27002 en CEINTECO se muestra en la Tabla 5.

Control ISO 27002:2013	**% Efectividad**
A.5 POLÍTICAS SEGURIDAD	0%
A.6 ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMACIÓN	15,71%
A.7 SEGURIDAD LIGADA A LOS RECURSOS HUMANOS	36%
A.8 GESTIÓN DE ACTIVOS	39%
A.9 CONTROL DE ACCESOS	63,21%
A.10 CIFRADO	0%
A.11 SEGURIDAD FÍSICA Y AMBIENTAL	48,66%
A.12 SEGURIDAD EN LA OPERATIVA	27,5%
A.13 SEGURIDAD EN LAS TELECOMUNICACIONES	17,14%

A.14 ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN	7,5%
A.15 RELACIONES CON SUMINISTRADORES	18%
A.16 GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN	25,71%
A.17 ASPECTOS DE LA SEGURIDAD DE LA INFORMACIÓN EN LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO	0%
A.18 CUMPLIMIENTO	47,5%

Tabla 5. Estado actual implementación ISO 27002:2013

A continuación, en la Imagen 13, se muestra el estado actual de los controles de la ISO 27002:2013 comparado con el estado al que se quiere llegar tras la implementación del SGSI y con el que sería el estado óptimo. En este caso, la línea azul representa el estado actual del cumplimiento de los controles, la línea roja un posible objetivo de cumplimiento a medio o largo plazo y, por último, la línea verde representa el nivel de cumplimiento óptimo. Los números que se muestran en la gráfica hacen referencia a los diferentes dominios contemplados en la ISO 27002:2013.

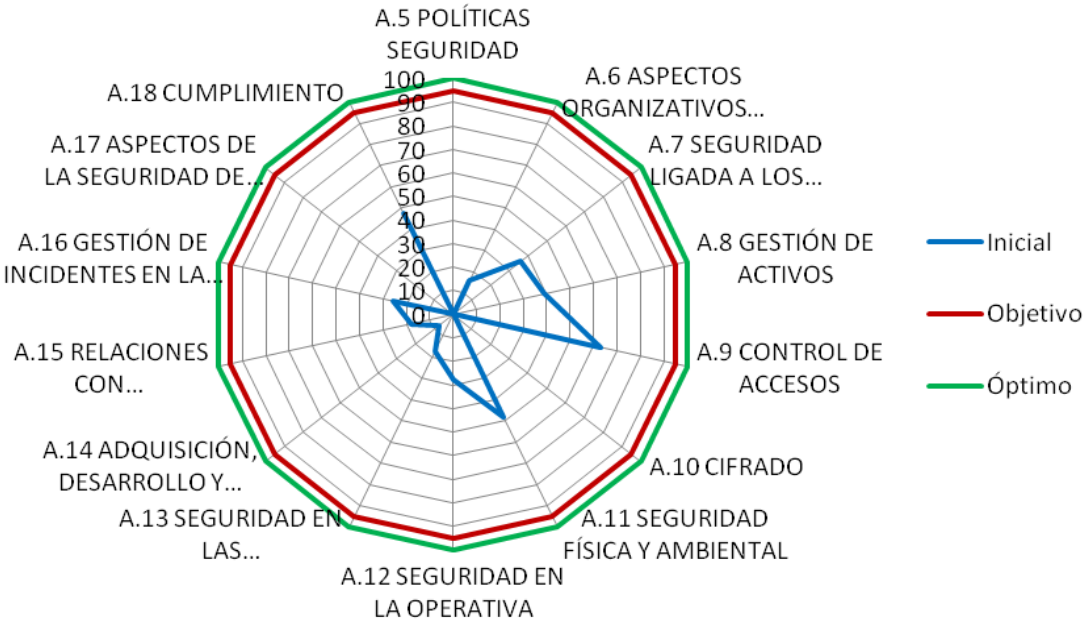


Imagen 13. Diagrama estado implementación ISO 27002:2013

2. Fase 2: Sistema de gestión documental

2.1. Introducción

La norma ISO/IEC 27001:2013 establece una serie de documentos que todo Sistema de Gestión de Seguridad de la Información tiene que tener para poder certificar el sistema.

En este apartado se van a definir los documentos más importantes que necesitará tener la empresa CEINTECO en su SGSI. Los documentos son:

- **Política de Seguridad**. Se trata de la normativa interna que debe conocer y cumplir todo el personal afectado por el alcance del SGSI. El contenido de este documento debe cubrir aspectos relativos al acceso de la información, uso de recursos de la organización, comportamiento en caso de incidentes de seguridad, etc.

- **Procedimiento de Auditorías Internas**. Este documento debe incluir una planificación de las auditorías que se realizarán durante la vigencia de la certificación, los requisitos que se establecerán a los auditores internos y se definirá también el modelo de informe de auditoría.

- **Gestión de Indicadores**. Es necesario definir las métricas e indicadores para medir la eficacia de los controles de seguridad implantados en la empresa. También se debe definir la sistemática para medir.

- **Procedimiento de Revisión por la Dirección**. La Dirección de la organización debe revisar anualmente las cuestiones más importantes relacionadas con el SGSI. Para ello, la ISO 27001 define tanto los puntos de entrada como los de salida que deben obtenerse de estas revisiones.

- **Gestión de Roles y Responsabilidades**. El SGSI tiene que estar compuesto por un equipo, conocido como Comité de Seguridad, que se encargue de crear, mantener, supervisar y mejorar el sistema. Este equipo debe estar compuesto, al menos, por una persona del equipo directivo para que las decisiones que se tomen estén respaldadas por alguien de la Dirección.

- **Metodología de Análisis de Riesgo**. Establece el sistema que se seguirá para calcular el riesgo. Este documento deberá incluir la identificación y valoración de los activos, amenazas y vulnerabilidades.

- **Declaración de Aplicabilidad**. Este documento incluye todos los controles de Seguridad establecidos en la organización y se incluye el detalle de su aplicabilidad, estado y documentación relacionada.

2.2. Esquema documental

2.2.1. Política de Seguridad

El objetivo de este documento es establecer las directrices en seguridad de la información de la empresa CEINTECO. Todas el personal que trabaja en la organización debe conocer todas las normas indicadas en el presente documento y velar por su cumplimiento.

2.2.1.1. Accesos físicos

1. El acceso físico de los trabajadores a las distintas oficinas de CEINTECO se permitirá a través de un sistema biométrico de huella dactilar situado en las puertas que dan acceso los pasillos donde se encuentran las salas y despachos de los distintos grupos de investigación y de administración.

2. Sólo estará permitido el acceso a las oficinas de la tercera planta utilizando la huella a los miembros del equipo de dirección, a administración, a los jefes de grupo y a todos los técnicos. El resto de empleados podrán acceder a estas oficinas siempre que haya una persona del equipo de administración en ella y, para ello, deberán tocar al timbre.

3. El personal ajeno a la empresa que desee acceder a las instalaciones deberá rellenar sus datos en una lista de visitas al entrar a las instalaciones del grupo al que visita, siendo el técnico del grupo el responsable de dicha lista. El jefe del grupo será el responsable del visitante durante el tiempo que dure su estancia en CEINTECO. Al salir de las instalaciones, el visitante deberá firmar en la lista de visitas cómo que se marcha de las instalaciones.

4. El acceso a los despachos de los jefes de grupo y dirección se realizará utilizando una llave que sólo tendrán los que trabajen en cada uno de los despachos. Además, el personal de administración dispone de una copia de cada llave de cada despacho de CEINTECO.

5. El acceso a las salas de los grupos de investigación se realizará utilizando una llave que poseerán todos los trabajadores de cada sala.

6. El acceso a los laboratorios de los grupos de investigación se realizará también utilizando una llave. Esta llave sólo la tendrán el jefe y el técnico de cada grupo. Para acceder al laboratorio los empleados deberán pedir permiso al técnico, que deberá apuntar la siguiente información: fecha y hora del acceso al laboratorio, persona que ha accedido y hora de salida del laboratorio.

7. Tanto el jefe como el técnico de cada grupo disponen de las llaves de todas las salas de su grupo. En caso de que ambos estén de vacaciones a la vez, se designará a una persona responsable de dichas llaves.

8. Los accesos a las salas de servidores se realizarán utilizando huella dactilar. Sólo tendrán acceso a estas salas el responsable de seguridad, el técnico del centro y los técnicos de los grupos de investigación.

2.2.1.2. Equipos y hardware

1. Cada trabajador es responsable de su equipo asignado y debe realizar un buen uso del mismo.

2. Todos los equipos deben estar protegidos por contraseña.

3. El equipo debe bloquearse cada vez que el trabajador se aleje de él.

4. Los sistemas de almacenamiento que se utilicen se extraerán siempre de manera segura.

5. Los ordenadores portátiles dispondrán de un sistema de seguridad para evitar que alguien se los pueda llevar.

6. Si algún trabajador necesita sacar algún equipo de CEINTECO de las instalaciones debe comunicárselo al técnico de su grupo junto a una justificación y éste lo debe aprobar.

7. El trabajador que saque equipos de las instalaciones de CEINTECO se hace responsable de lo que le suceda tanto al equipo como a la información que contenga dicho equipo.

8. Si se detecta algún comportamiento anómalo en algún equipo debe informarse de manera inmediata al técnico del grupo correspondiente.

9. Los dispositivos de almacenamiento que no se vayan a usar deberán ser entregados al técnico de cada grupo. Este decidirá si se reutiliza o se retira definitivamente. En cualquier caso, el técnico de grupo deberá realizar un formateo completo del dispositivo.

2.2.1.3. Acceso a Internet

1. Los trabajadores deben realizar un uso responsable de este recurso.

2. Está prohibido visitar páginas web con contenido ilícito.

3. Está prohibido el acceso, uso o instalación de servicios de mensajería instantánea que no sean los empleados por CEINTECO.

4. Está prohibida la descarga, uso o instalación de cualquier programa de descarga o intercambio P2P de música, películas, etc., así como juegos o software no aprobado por el equipo técnico de CEINTECO.

2.2.1.4. Correo electrónico

1. Todo el personal de CEINTECO dispone de una dirección de correo electrónica de la organización.

2. La cuenta de correo electrónico sólo podrá ser utilizada para temas relacionados con el trabajo que desempeñan en CEINTECO.

3. No está permitido utilizar el correo electrónico de la empresa como correo electrónico personal.

4. No está permitido realizar SPAM con el correo electrónico de CEINTECO.

5. Si se recibe un correo electrónico sospechoso debe seguirse el procedimiento definido por CEINTECO para comprobar si el correo es seguro o no.

2.2.1.5. Software

1. Todos los equipos deben de tener instalado el antivirus utilizado por CEINTECO y tenerlo habilitado en todo momento. El antivirus deberá de estar siempre actualizando con la última versión disponible.

2. Está prohibida la instalación de software no aprobado por CEINTECO.

3. Ningún equipo podrá tener instalado software que no disponga de licencia.

4. Para la instalación de nuevo software o actualización del existente es necesario comunicarlo primero al técnico de cada grupo que debe aprobar dicha instalación.

2.2.1.6. Copias de seguridad

1. Se deberán realizar copias de seguridad diarias de todos los servidores de CEINTECO. Los técnicos son los responsables de que las copias de los servidores que tienen a su cargo se realicen correctamente.

2. Los trabajadores deberán realizar copias de seguridad de sus equipos regularmente.

3. Las copias de seguridad se almacenarán en un edificio diferente al que alberga las oficinas de CEINTECO.

2.2.1.7. Información

1. No está permitido sacar fuera de las instalaciones de CEINTECO información restringida o confidencial sin haber obtenido un permiso previamente.

2. Los trabajadores deben mantener su puesto de trabajo limpio de información restringida o confidencial.

3. Los trabajadores deben recoger los documentos impresos de las impresoras en el momento de mandarlos a imprimir.

4. Los documentos con información restringida o confidencial no se tirarán en la papelera ordinaria sino que se utilizará el destructor de papeles situado en las oficinas de los grupos de investigación.

5. Está prohibido el uso de información confidencial para autenticarse en cualquiera de los sistemas de la organización.

2.2.1.8. Contraseñas

1. Las contraseñas que se utilicen en CEINTECO deben de tener entre 8 y 15 caracteres entre los que tienen que haber mayúsculas, minúsculas, números y símbolos.

2. Las contraseñas se cambiarán cada 3 meses y no se podrá utilizar como nueva contraseña ninguna de las tres últimas utilizadas.

3. Ningún trabajador puede comunicar a otro la contraseña de acceso a su equipo ni debe tenerla apuntada en ningún papel al alcance de la vista de otros.

2.2.2. Procedimiento de Auditorías Internas

2.2.2.1. Objetivo

Este documento tiene como objetivo establecer el procedimiento a seguir para la realización de las auditorías internas del Sistema de Gestión de Seguridad de la Información de la empresa CEINTECO con el fin de comprobar la eficacia del SGSI implantado y corregir las posibles no conformidades encontradas para mejorarlo.

2.2.2.2. Alcance

El alcance de las auditorías internas son los procesos implicados en el SGSI así como aquellos que tengan influencia en los procesos y procedimientos que se lleven a cabo dentro del SGSI de la organización.

2.2.2.3. Periodicidad

A excepción de la primera auditoría interna que se realizará a los 6 meses de haber implantado el SGSI, la periodicidad de realización de las auditorías internas será anual y su duración total será de 3 meses.

2.2.2.4. Responsabilidades

- Director General: Es la persona encargada de aprobar el programa de auditorías internas.
- Responsable seguridad de la información: Es la persona que colaborará con el equipo auditor y dará soporte en todo lo que sea necesario durante la auditoría.
- Equipo auditor: Es el encargado de la realización de las auditorías.

2.2.2.5. Equipo auditor

Puesto que todos los técnicos de la organización participarán de una manera u otra en la implantación del SGSI, el equipo auditor será subcontratado para garantizar la total independencia de la auditoría. El equipo auditor estará formado por dos personas: el auditor jefe, que será el responsable de la planificación y organización de la auditoría, y por otro auditor más.

Los requisitos mínimos que deben cumplir los miembros del equipo auditor son los siguientes:

- Ser independiente de la organización.
- Capacidad de comunicación.
- Conocimientos de informática y/o telecomunicaciones.
- Conocer tanto la norma ISO 27001:2013 como la ISO 27002:2013.
- Experiencia en la realización auditorías de seguridad de la información.
- Capacidad para elaborar informes.

2.2.2.6. Metodología

Las auditorías internas constarán de tres fases. Éstas se muestran en la Imagen 14.

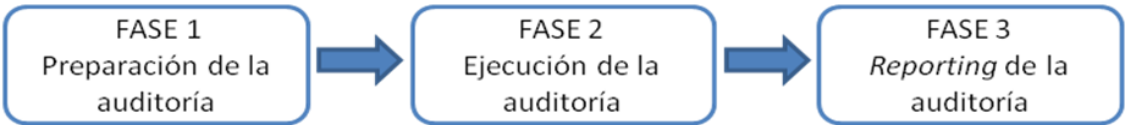


Imagen 14. Fases auditoría interna

Preparación de la auditoría

Se trata de la fase inicial de la auditoría y en ella se llevará a cabo una primera reunión entre el auditor jefe y el director general y el responsable de seguridad de CEINTECO para establecer de una manera clara cuales son los objetivos de la auditoría que se va a realizar y lo que se espera de ésta.

Tras la primera reunión se determinarán los procedimientos de comunicación entre el equipo auditor y los responsables de CEINTECO.

Se realizará a continuación el inventariado de las políticas de empresa que afecten a la auditoría y que serán comprobadas.

Por último, se definirán las pruebas que se van a realizar durante la auditoría.

Ejecución de la auditoría

En esta fase el equipo auditor llevará a cabo las diferentes tareas para la correcta realización de la auditoría interna.

Estas tareas serán:

1. Recolección de la información necesaria:
    - Documentación de la empresa con información sobre los requisitos del negocio.
    - Leyes y regulaciones.
    - Política de seguridad.
    - Documentación con los controles de seguridad implantados.
2. Ejecución de pruebas:
    - Se buscarán fallos en la documentación de la empresa.
    - Se realizarán entrevistas con los trabajadores.
    - Se ejecutarán las pruebas técnicas que se consideren oportunas.
3. Elaboración del informe de auditoría.

Reporting de la auditoría

En esta fase el auditor jefe comunicará a CEINTECO el informe de auditoría con los resultados y conclusiones obtenidas tras haber realizado todas las pruebas pertinentes.

2.2.2.7. Resultados: Informe de Auditoría

Como se ha mencionado anteriormente, una vez realizada la auditoría, el equipo auditor debe redactar el informe de auditoría en el que se establecerán las no conformidades detectadas y las recomendaciones pertinentes.

El informe de auditoría incluirá la siguiente información:

- Fecha de la auditoría.
- Nombre del auditor.
- Alcance de la auditoría.
- Controles auditados.
- Grado de adecuación del SGSI con la norma ISO 27001:2013.
- No conformidades detectadas.
- Recomendaciones de mejora.

2.2.3. Gestión de indicadores

En este documento se detallan los indicadores que va a utilizar CEINTECO para controlar el funcionamiento de las medidas de seguridad de la información que se van a implantar, así como su eficacia y eficiencia. También se definen los mecanismos y periodicidad de medida de cada uno de los indicadores que se van a utilizar.

A continuación, en la Tabla 6, se muestran los indicadores establecidos para evaluar el SGSI de CEINTECO.

ID	Indicador	Descripción	Control	Fórmula	Frecuencia	Valor objetivo/ umbral
IN1	Política de seguridad	Verificar que se realiza la revisión de las políticas de seguridad por parte de la Dirección	A.5.1.2	Nº revisiones /año	Anual	2/1
IN2	Responsabilidades	Verificar si los roles y responsabilidades en cuanto a seguridad de la información están definidos	A.6.1.1	(Nº tareas seguridad con responsable asignado / Nº tareas seguridad totales)*100	Anual	100% / 90%
IN3	Dispositivos móviles	Medida del cumplimiento de las políticas respecto a los dispositivos móviles	A.6.2.1	(Nº veces uso no por trabajo)/(Nº veces uso total)*100	Semestral	0% / 10%
IN4	Formación	Medida de la eficacia de los cursos de formación	A.7.2.2	(Suma valoraciones cursos)*10/Nº encuestas	Anual	80 / 70
IN5	Disciplina	Medida de cantidad de violaciones de seguridad de la información por parte de los trabajadores	A.7.2.3	Nº sanciones/semestre	Semestral	0 / 5
IN6	Inventario activos	Comprobar el número de activos inventariados	A.8.1.1	(Nº activos en inventario/Nº activos totales)*100	Trimestral	100% / 90%
IN7	Mal uso de activos	Medida de la calidad de uso de los activos de la organización ya sea en la oficina o fuera de ella	A.8.1.3, A.8.3.3, A.6.2.1	(Nº activos rotos por mal uso/accidentes/Nº activos totales)*100	Semestral	0% / 5%
IN8	Extravío activos	Medida de la cantidad de activos extraviados	A.8.1.4, A.11.2.6	(Nº activos totales/Nº activos en inventario)*100	Trimestral	100% / 90%
IN9	Control accesos red	Medida de la cantidad de accesos no autorizados a la red de la organización	A.9.1.2	(Nº accesos no autorizados / Nº total accesos realizados)*100	Mensual	0% / 5%
IN10	Derechos de acceso de usuario	Medida de la eficacia del proceso de otorgar/quitar los permisos a los usuarios	A.9.2.1, A.9.2.2, A.9.2.5, A.9.2.6	(Nº de personas con derecho acceso / Nº total trabajadores)*100	Mensual	100% / 95%

IN11	Controles criptográficos	Medida de la eficacia de la política de encriptación de datos sensibles	A.10.1.1	(Nº sistemas con datos sensible encriptados/Nº de sistemas con datos sensibles totales) *100	Semestral	100% / 95%
IN12	Control accesos oficinas	Medida de la eficacia de las medidas de seguridad físicas	A.11.1.2, A.11.1.3, A.11.1.6	(Accesos fallidos/Accesos totales)*100	Mensual	0% / 10%
IN13	Control accesos laboratorios	Medida de la eficacia de las medidas de seguridad de acceso a los laboratorios	A.11.1.2, A.11.1.3	(Nº de accesos autorizados / Nº accesos totales)*100	Trimestral	100% / 85%
IN14	Revisión anti-incendios	Verificar que se realizan las revisiones a los sistemas contra incendios	A.11.1.4	Nº revisiones/año	Anual	2/2
IN15	Fallas de energía	Medida de la eficacia de los equipos UPS de la organización	A.11.2.2	(Nº de equipos apagados tras apagón controlado/Nº de equipos totales)*100	Semestral	0% / 10%
IN16	Cableado	Medida de la seguridad del cableado de la organización	A.11.2.3	(Nº cables luz/telecom a la vista/Nº cables luz/telecom totales)*100	Semestral	0% / 15%
IN17	Mantenimiento equipos	Medida de la cantidad de equipos que se encuentran en un estado óptimo	A.11.2.4	(Nº equipos con últimas actualizaciones / Nº equipos totales)*100	Mensual	100% / 95%
IN18	Copias de seguridad de los equipos de trabajo	Medida de la eficacia de las copias de seguridad de los equipos de los trabajadores	A.12.3.1	(Copias fallidas/Copias totales)*100	Trimestral	0% / 10%
IN19	Copias de seguridad servidores	Medida de la eficacia de las copias de seguridad de los servidores	A.12.3.1	(Copias fallidas/Copias totales)*100	Mensual	0% / 5%
IN20	Malware/virus detectados	Medida de la cantidad de programas maliciosos detectados en los equipos de la organización	A.12.2.1	Nº programas maliciosos detectados/trimestre	Trimestral	0 / 10
IN21	Antivirus	Medida de la cantidad de equipos que no disponen de antivirus instalados	A.12.2.1	(Nº equipos con antivirus/ Nº equipos totales)*100	Mensual	100% / 95%
IN22	Licencias de software	Medida de la cantidad de software con licencia instalado en los equipos de trabajo	A.12.5.1, A.18.1.2	(Nº licencias compradas / Nº aplicaciones totales instaladas)*100	Anual	100% / 90%
IN23	Software no autorizado instalado	Medida de la cantidad de software instalado sin autorización	A.12.6.2	(Nº de software no autorizado instalado/Nº de software total instalado)*100	Semestral	0% / 10%
IN24	Comunicaciones externas	Verificar el correcto cumplimiento de las políticas de intercambio de información con el exterior	A.13.2.2, A.13.2.3	(Nº comunicaciones externas protegidas/Nº comunicaciones externas totales)*100	Semestral	100% / 90%

IN25	Revisión prestación servicios proveedores	Medidas del cumplimiento de los servicios contratados por parte de los proveedores	A.15.2.1	(Nº incumplimientos de proveedores/Nº contratos con proveedores)*100	Trimestral	0% / 10%
IN26	Puntos débiles seguridad	Medida de la eficacia del procedimiento de notificación de debilidades en el SGSI	A.16.1.2, A.16.1.3	Nº notificaciones de debilidades por los trabajadores/mes	Mensual	-
IN27	Incidentes	Medida del número de incidentes de seguridad que ocurren en la organización	A.16.1.4	Nº incidentes/mes	Mensual	0 / 3
IN28	Continuidad de negocio	Medida de la operatividad de los procesos que forman parte del plan de continuidad de negocio	A.17.1.2	(Nº procesos del plan de continuidad funcionando correctamente / Nº procesos del plan de continuidad totales)*100	Semestral	100% / 90%
IN29	Auditorías internas	Verificar que se realizan las auditorías internas	A.18.2.1	Nº auditorias/año	Anual	2/1
IN30	Nuevos clientes	Medida del incremento nº de empresas externas para las que se trabaja	-	(Nº empresas externas año actual) - (Nº empresas externas año anterior)	Anual	Número positivo
IN31	Filtraciones información	Medida de la cantidad de filtraciones de información de la organización	-	Nº de filtraciones de información de la empresa/semestre	Semestral	0/1
IN32	Confianza en la empresa	Medida de la confianza en la organización	-	Encuesta sobre la confianza que tienen en CEINTECO a los clientes Medida: escala entre 1 y 10	Anual/Al terminar un proyecto con el cliente	10/8

Tabla 6. Indicadores

2.2.4. Procedimiento de Revisión por la Dirección

La Dirección de CEINTECO deberá revisar periódicamente el Sistema de Gestión de Seguridad de la Información para comprobar si el SGSI está funcionando como se esperaba o si, en cambio, se deben introducir cambios y mejoras en el SGSI de la organización.

La primera revisión de la Dirección se realizará a los 6 meses de haber implantado el SGSI y, posteriormente, las revisiones se llevarán a cabo anualmente.

En estas revisiones la Dirección realizará las siguientes acciones:

- ✓ Identificar cambios en los niveles de riesgos, nuevas amenazas y vulnerabilidades.
- ✓ Identificar cambios en la legislación y regulación.
- ✓ Revisar el estado del SGSI.
- ✓ Analizar el cumplimiento de los objetivos del SGSI.
- ✓ Analizar la efectividad de los controles implantados.
- ✓ Establecer nuevas acciones preventivas, correctivas y de mejora o cambiar las existentes.
- ✓ Documentar los resultados de la revisión llevada a cabo.

Para ello, los puntos de entrada de estas revisiones serán los siguientes:

- Resultados de revisiones anteriores del SGSI.
- Resultados de los indicadores definidos en el SGSI.
- Resultados de las auditorías internas.
- No conformidades surgidas desde la última revisión.
- Estado de las medidas preventivas y correctivas.
- Cambios en la organización, ya sean internos o externos.
- Sugerencias del personal de CEINTECO referentes a la mejora de la seguridad de la información.
- Retroalimentación de los clientes.

Las salidas que se obtendrán de estas revisiones serán:

- Mejora de la efectividad del SGSI.
- Actualización de la evaluación y tratamiento de los riesgos.
- Modificación de controles existentes o inclusión de nuevos controles.
- Modificación de procedimientos.

2.2.5. Gestión de Roles y Responsabilidades

Para gestionar de manera adecuada el Sistema de Gestión de Seguridad de la Información de CEINTECO es necesario crear un Comité de Seguridad que tenga responsabilidad directa sobre la seguridad de la información de la empresa. Este comité debe estar formado por varios miembros de la organización entre los que debe haber, al menos, una persona del equipo directivo.

Para tener un mayor conocimiento en temas de seguridad de la información, CEINTECO ha decidido contratar a un experto en seguridad de la información como responsable de la seguridad de la información de la organización.

A continuación se van a detallar los roles y responsabilidades de la estructura organizativa en seguridad de la información de CEINTECO.

2.2.5.1. Comité de Seguridad

El Comité de Seguridad de CEINTECO estará formado por las siguientes personas:

- Subdirector general.
- Responsable de seguridad (recién contratado).
- Técnico del centro de investigación.
- Jefes de los grupos de investigación.

Las funciones y responsabilidades del Comité de Seguridad serán las siguientes:

- ✓ Implantar las directrices de la Dirección.
- ✓ Asignar los distintos roles y funciones en materia de seguridad.
- ✓ Presentar las políticas, normas y responsabilidades en materia de seguridad de la información a la Dirección para que sean aprobadas.
- ✓ Validar el mapa de riesgos y las acciones de mitigación propuestas.
- ✓ Validar el Plan de Seguridad y presentarlo a la Dirección para que sea aprobado.
- ✓ Supervisar el desarrollo y mantenimiento del Plan de Continuidad de negocio.
- ✓ Velar por el cumplimiento de la legislación y regulación vigente.
- ✓ Promover la concienciación y formación de los empleados en materia de seguridad de la información.
- ✓ Aprobar y revisar periódicamente el cuadro de mando de la seguridad de la información y de la evolución del SGSI.

Este comité se reunirá cada 2 semanas durante las 2 primeras fases de implantación del SGSI (fases *Plan* y *Do* del Ciclo de *Deming*). Una vez superadas estas fases, se reunirá de manera regular cada 3 meses. También se podrá reunir en caso de crisis.

2.2.5.2. Responsable de Seguridad

El Responsable de Seguridad es otra figura importante en el desarrollo de la seguridad de la información de CEINTECO. Sus responsabilidades en materia de seguridad de la información serán las siguientes:

- ✓ Elaborar, promover y mantener la política de seguridad de la información.
- ✓ Elaborar el plan de riesgos y las posibles soluciones para mitigar las amenazas.
- ✓ Proponer nuevos objetivos en materia de seguridad de la información.
- ✓ Desarrollar y mantener el marco normativo de seguridad y controlar su cumplimiento.
- ✓ Liderar la implantación del SGSI.
- ✓ Gestionar la seguridad de la información de la organización de manera global.
- ✓ Revisar periódicamente el estado de la seguridad de la información.
- ✓ Realizar el seguimiento de los incidentes de seguridad.
- ✓ Controlar y revisar los indicadores definidos.
- ✓ Revisar los informes de auditoría.
- ✓ Reportar al Comité de Seguridad las cuestiones relevantes en materia de seguridad de la información.

2.2.5.3. Técnico de centro de investigación

En el técnico del centro de investigación recaerán las siguientes responsabilidades en materia de seguridad de la información:

- ✓ Realizar la implantación de los controles del SGSI.
- ✓ Resolver los incidentes de seguridad que estén a su alcance.
- ✓ Reportar al responsable de seguridad los incidentes de seguridad.
- ✓ Colaborar con el responsable de seguridad en la identificación de riesgos y propuesta de soluciones.
- ✓ Revisar la correcta realización de las copias de seguridad de los servidores globales de la organización.
- ✓ Instalar el software básico de los equipos nuevos, incluyendo el software antivirus.

2.2.5.4. Técnicos de grupo

Los técnicos de grupo tienen las siguientes responsabilidades en materia de seguridad:

- ✓ Notificar al técnico del centro de investigación de los incidentes de seguridad detectados en el grupo de investigación.
- ✓ Administrar los equipos del grupo.
- ✓ Realizar el mantenimiento de los equipos del grupo.
- ✓ Dar permisos de acceso a los miembros del grupo a equipos, red, etc.

- ✓ Controlar el cumplimiento de las normas definidas en la política de seguridad dentro de su grupo.
- ✓ Revisar la correcta realización de las copias de seguridad de los servidores del grupo.
- ✓ Autorizar y controlar el acceso al laboratorio del grupo.
- ✓ Apuntar y supervisar los accesos a las instalaciones de personal ajeno a la empresa.

2.2.5.5. Personal en general

El personal de CEINTECO tiene las siguientes obligaciones y responsabilidades:

- ✓ Respetar y seguir las normas y procedimientos definidos en la política de seguridad de la empresa.
- ✓ Mantener la confidencialidad de la información.
- ✓ Hacer un buen uso de los activos de la organización.
- ✓ Respetar la legislación y regulación vigentes.
- ✓ Notificar al técnico de grupo correspondiente las anomalías o incidentes de seguridad así como las situaciones sospechosas.

2.2.5.6. Organigrama funcional de la seguridad

Por último en la Imagen 15 se muestra el organigrama funcional de CEITENCO en cuanto a seguridad de la información se refiere con los actores más relevantes así como sus principales funciones.

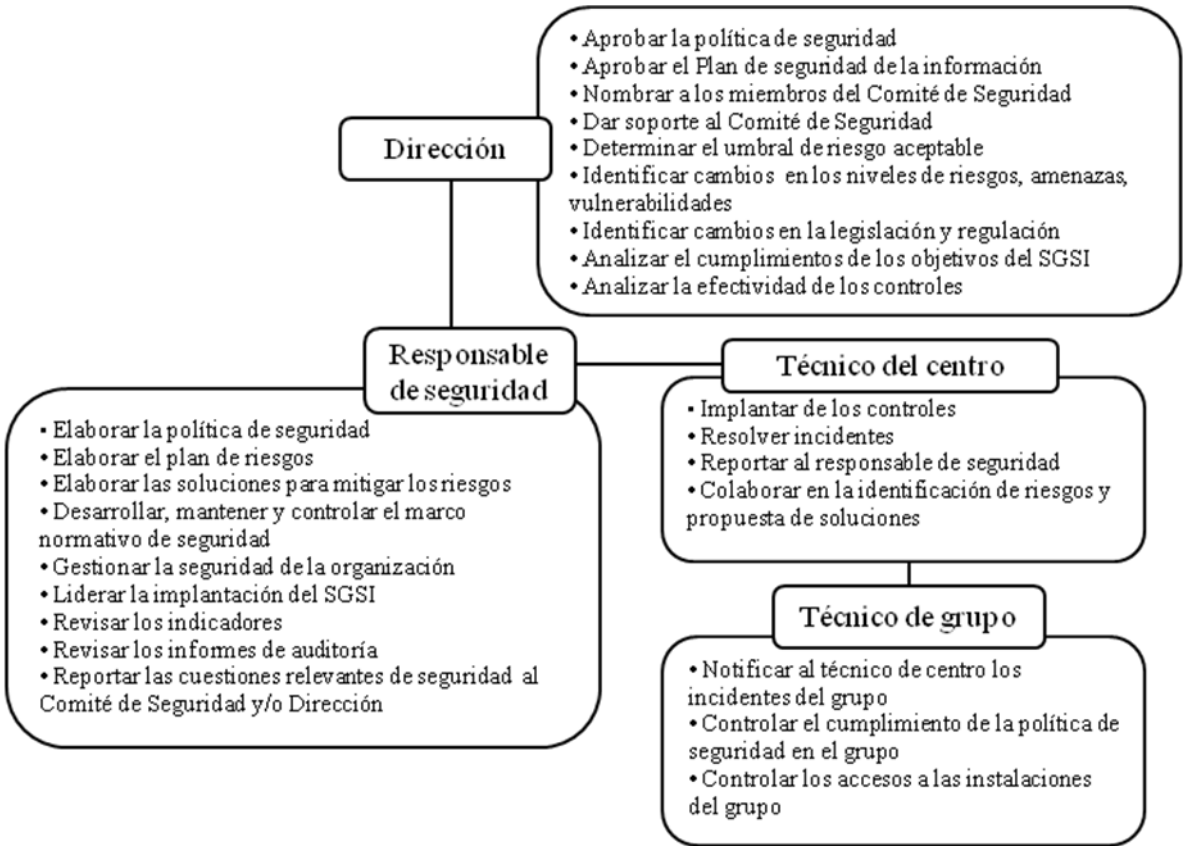


Imagen 15. Organigrama funcional de la seguridad de la información de CEINTECO

2.2.6. Declaración de Aplicabilidad

En la Tabla 7 que aparece en este documento se recoge la relación de controles de la ISO/IEC 27002:2013 y se especifica, para cada uno de ellos, si se va a aplicar o no al SGSI de CEINTECO. Además, se detalla la justificación de exclusión del control en caso de no aplicarse o la descripción de cómo se implementa en caso de que se vaya a aplicar.

ID	Control ISO 27002:2013	Aplica	Justificación / Descripción
A.5	**POLÍTICAS DE SEGURIDAD**		
A.5.1	**Directrices de la Dirección en seguridad de la información**		
A.5.1.1	Conjunto de políticas para la seguridad de la información	SI	Se debe definir un conjunto de políticas de seguridad de la información que sean aprobadas por la dirección y comunicadas a todos los trabajadores.
A.5.1.2	Revisión de las políticas para la seguridad de la información	SI	La política de seguridad deben ser revisadas periódicamente o cuando ocurran cambios significativos.
A.6	**ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMACIÓN**		
A.6.1	**Organización interna**		
A.6.1.1	Asignación de responsabilidades para la seguridad de la información	SI	Se deben asignar los distintos roles y responsabilidades en cuanto a seguridad de la información.
A.6.1.2	Segregación de tareas	SI	Se deben separar las responsabilidades para reducir las posibilidades de uso indebido de activos, de accesos no autorizados de modificaciones no autorizadas.
A.6.1.3	Contacto con las autoridades	SI	Se deben mantener los contactos apropiados con las autoridades pertinentes.
A.6.1.4	Contacto con grupos de interés especial	SI	Se debe mantener contacto con asociaciones o grupos especializados en seguridad.
A.6.1.5	Seguridad de la información en la gestión de proyectos	SI	Se debe tatar la seguridad de la información en la gestión de cualquier proyecto.
A.6.2	**Dispositivos para movilidad y teletrabajo**		
A.6.2.1	Política de uso de dispositivos para movilidad	SI	Se deben adoptar una política y medidas de seguridad para gestionar los riesgos del uso de dispositivos móviles.
A.6.2.2	Teletrabajo	SI	Se deben implementar medidas de seguridad para proteger la información tratada en los lugares desde los que se teletrabaja.
A.7	**SEGURIDAD LIGADA A LOS RECURSOS HUMANOS**		
A.7.1	**Antes de la contratación**		
A.7.1.1	Investigación de antecedentes	SI	Se deben verificar los antecedentes de todos los candidatos a un empleo en la organización. Esta investigación se hará de acuerdo con la legislación y regulación vigente.
A.7.1.2	Términos y condiciones de contratación	SI	Los contratos con los empleados y terceros deben establecer las responsabilidades y condiciones en materia de seguridad de la información.
A.7.2	**Durante la contratación**		

A.7.2.1	Responsabilidades de gestión	SI	La Dirección debe exigir a los empleados la aplicación de la seguridad de la información de acuerdo a las políticas y procedimientos de la empresa.
A.7.2.2	Concienciación, educación y capacitación en seguridad de la información	SI	Todos los empleados deben recibir formación para tomar conciencia de la seguridad de la información de la empresa.
A.7.2.3	Proceso disciplinario	SI	Debe existir un proceso disciplinario para los trabajadores que hayan realizado alguna violación de seguridad.
A.7.3	**Cese o cambio de puesto de trabajo**		
A.7.3.1	Cese o cambio de puesto de trabajo	SI	Se deben definir las responsabilidades y deberes que tienen los empleados al cambiar de contrato o terminar con él.
A.8	**GESTIÓN DE ACTIVOS**		
A.8.1	**Responsabilidad sobre los activos**		
A.8.1.1	Inventario de activos	SI	Se deben identificar los activos y realizar y mantener un inventario de éstos.
A.8.1.2	Propiedad de los activos	SI	Todo activo del inventario debe tener un propietario que será el responsable de dicho activo.
A.8.1.3	Uso aceptable de los activos	SI	Se deben definir las reglas de uso de los activos.
A.8.1.4	Devolución de los activos	SI	Todos los empleados deben devolver los activos que tengan a su cargo al terminar el contrato con la organización.
A.8.2	**Clasificación de la información**		
A.8.2.1	Directrices de clasificación	SI	La información debe ser clasificada en base a los requisitos legales, valor, criticidad, susceptibilidad a divulgación o modificación no autorizada.
A.8.2.2	Etiquetado y manipulado de la información	SI	Se debe definir el procedimiento para el etiquetado de la información.
A.8.2.3	Manipulación de activos	SI	Se deben definir el procedimiento para el manejo de activos.
A.8.3	**Manejo de los soportes de almacenamiento**		
A.8.3.1	Gestión de los soportes extraíbles	SI	Se deben definir el procedimiento para la gestión de soportes extraíbles.
A.8.3.2	Eliminación de soportes	SI	Se debe definir un procedimiento seguro para eliminar los soportes de almacenamiento que ya no se requieran.
A.8.3.3	Soportes físicos en tránsito	SI	Se deben proteger los soportes físicos que contienen información cuando se transportan para evitar accesos no autorizados, usos indebidos o corrupción.
A.9	**CONTROL DE ACCESOS**		
A.9.1	**Requisitos de negocio para el control de accesos**		
A.9.1.1	Política de control de accesos	SI	Se debe establecer una política de control de accesos.
A.9.1.2	Control de acceso a las redes y servicios asociados	SI	Sólo se debe permitir el acceso de los trabajadores a la red y a los servicios de la red para los que estén autorizados.
A.9.2	**Gestión de acceso de usuario**		

A.9.2.1	Gestión de altas/bajas en el registro de usuarios	SI	Se debe implementar un proceso de altas y bajas en el registro de usuarios.
A.9.2.2	Gestión de los derechos de acceso asignados a usuarios	SI	Se debe implementar un proceso de asignación de derechos de acceso para los trabajadores.
A.9.2.3	Gestión de los derechos de acceso con privilegios especiales	SI	Se debe restringir y controlar la asignación y uso de los derechos de acceso privilegiado.
A.9.2.4	Gestión de información confidencial de autenticación de usuarios	SI	Se debe controlar mediante un proceso la asignación de la información confidencial.
A.9.2.5	Revisión de los derechos de acceso de los usuarios	SI	Se deben revisar periódicamente los derechos de acceso de los usuarios a los activos y sistemas de la empresa.
A.9.2.6	Retirada o adaptación de los derechos de acceso	SI	Al finalizar el contrato de un trabajador se le deben retirar sus derechos de acceso a la información e instalaciones de la empresa.
A.9.3	**Responsabilidades del usuario**		
A.9.3.1	Uso de información confidencial para la autenticación	SI	Se debe exigir a los trabajadores que cumplan con las prácticas de la organización para el uso de información de autenticación secreta.
A.9.4	**Control de acceso a sistemas y aplicaciones**		
A.9.4.1	Restricción del acceso a la información	SI	Se debe restringir el acceso a la información de acuerdo con la política de acceso.
A.9.4.2	Procedimientos seguros de inicio de sesión	SI	Se debe utilizar un proceso de inicio de sesión seguro para acceder a sistemas y aplicaciones.
A.9.4.3	Gestión de contraseñas de usuario	SI	Los sistemas de gestión de contraseñas deben asegurar la calidad de las contraseñas.
A.9.4.4	Uso de herramientas de administración de sistemas	SI	Se debe controlar el uso de programas que puedan anular el sistema y los controles de las aplicaciones.
A.9.4.5	Control de acceso al código fuente de los programas	SI	Se debe restringir el acceso a los códigos fuente de los programas.
A.10	**CIFRADO**		
A.10.1	**Controles criptográficos**		
A.10.1.1	Política de uso de los controles criptográficos	SI	Se debe establecer una política sobre el uso de controles criptográficos para la protección de la información de la empresa.
A.10.1.2	Gestión de claves	SI	Se debe establecer una política sobre el uso, protección y tiempo de vida de las llaves criptográficas.
A.11	**SEGURIDAD FÍSICA Y AMBIENTAL**		
A.11.1	**Áreas seguras**		
A.11.1.1	Perímetro de seguridad física	SI	Se debe definir el perímetro de seguridad y usarlo para proteger las áreas que contengan información sensible e instalaciones de manejo de información.
A.11.1.2	Controles físicos de entrada	SI	Las áreas seguras deben de estar protegidas mediantes controles apropiados que sólo permitan la entrada al personal de la organización.
A.11.1.3	Seguridad de oficinas, despachos y recursos	SI	Se debe aplicar seguridad física a todas las instalaciones de la empresa.
A.11.1.4	Protección contra las amenazas externas y ambientales	SI	Se debe aplicar seguridad contra desastres naturales, ataques externos o accidentes.
A.11.1.5	El trabajo en áreas seguras	SI	Se deben definir procedimientos para el trabajo en áreas seguras.

A.11.1.6	Áreas de acceso público, carga y descarga	SI	Se debe controlar el acceso a las áreas donde puede entrar personal ajeno a la empresa.
A.11.2	**Seguridad de los equipos**		
A.11.2.1	Emplazamiento y protección de equipos	SI	Los equipos deben estar ubicados y protegidos de tal manera que se reduzcan las amenazas y peligros del entorno y las oportunidades para el acceso no autorizado.
A.11.2.2	Instalaciones de suministro	SI	Los equipos se deben proteger contra fallas de energía.
A.11.2.3	Seguridad del cableado	SI	El cableado de potencia y el de telecomunicaciones debe estar protegido para evitar ser interceptado o dañado.
A.11.2.4	Mantenimiento de los equipos	SI	Los equipos deben de ser mantenidos correctamente para asegurar siempre su integridad y disponibilidad.
A.11.2.5	Salida de activos fuera de las dependencias de la empresa	SI	Se debe definir un procedimiento para sacar los activos fuera de la empresa.
A.11.2.6	Seguridad de los equipos y activos fuera de las instalaciones	SI	Se deben aplicar medidas de seguridad a los activos que salgan de la organización.
A.11.2.7	Reutilización o retirada segura de dispositivos de almacenamiento	SI	Se debe verificar que los equipos que contengan información sensible y vayan a ser retirados o reutilizados son limpiados antes de su retirada o reutilización.
A.11.2.8	Equipo informático de usuario desatendido	SI	Los trabajadores deben asegurarse de que los equipos desentendidos estén siempre protegidos.
A.11.2.9	Política de puesto de trabajo despejado y bloqueo de pantalla	SI	Los trabajadores deben tener sus puestos de trabajo limpios de información confidencial así como de bloquear la pantalla de su ordenador siempre que no lo estén utilizando.
A.12	**SEGURIDAD EN LA OPERATIVA**		
A.12.1	**Responsabilidades y procedimientos de operación**		
A.12.1.1	Documentación de procedimientos de operación	SI	Se deben documentar los procedimientos de operación y poner a disposición de todo el personal de la empresa.
A.12.1.2	Gestión de cambios	SI	Se deben controlar los cambios en la organización que afectan a la seguridad de la información.
A.12.1.3	Gestión de capacidades	SI	Se debe hacer un seguimiento al uso de los recursos y hacer los ajustes y proyecciones de requisitos sobre la capacidad futura.
A.12.1.4	Separación de entornos de desarrollo, prueba y producción	NO	No existen diferentes entornos.
A.12.2	**Protección contra código malicioso**		
A.12.2.1	Controles contra el código malicioso	SI	Se deben implementar controles de detección, prevención y de recuperación contra códigos maliciosos.
A.12.3	**Copias de seguridad**		
A.12.3.1	Copias de seguridad de la información	SI	Se deben hacer copias de seguridad de la información y del software realizado y ponerlas a prueba regularmente.
A.12.4	**Registro de actividad y supervisión**		
A.12.4.1	Registro y gestión de eventos de	SI	Se deben registrar y revisar cada cierto tiempo los

	actividad		registros sobre las actividades de los trabajadores, excepciones, fallas y eventos de seguridad de la información.
A.12.4.2	Protección de los registros de información	SI	Se deben proteger las instalaciones e información de registro contra la alteración y el acceso no autorizado.
A.12.4.3	Registros de actividad del administrador y operador del sistema	SI	Se deben registrar las actividades del administrador del sistema así como proteger y revisar regularmente dichos registros.
A.12.4.4	Sincronización de relojes	SI	Todos los relojes de la organización deben de estar sincronizados.
A.12.5	**Control del software en explotación**		
A.12.5.1	Instalación del software en sistemas en producción	SI	Se deben establecer procedimientos para controlar la instalación de software en los sistemas operativos.
A.12.6	**Gestión de la vulnerabilidad técnica**		
A.12.6.1	Gestión de las vulnerabilidades técnicas	SI	Se debe obtener información sobre vulnerabilidades técnicas de los sistemas de información utilizados, evaluar la exposición frente a estas vulnerabilidades y tomar las medidas oportunas.
A.12.6.2	Restricciones en la instalación de software	SI	Se deben establecer reglas para la instalación de software en los equipos.
A.12.7	**Consideraciones de las auditorías de los sistemas de información**		
A.12.7.1	Controles de auditoría de los sistemas de información	SI	Las actividades de auditoría se deben acordar con los trabajadores para minimizar las interrupciones en el trabajo diario.
A.13	**SEGURIDAD EN LAS TELECOMUNICACIONES**		
A.13.1	**Gestión de la seguridad en las redes**		
A.13.1.1	Controles de red	SI	Se deben gestionar y controlar las redes para proteger la información en los sistemas.
A.13.1.2	Mecanismos de seguridad asociados a servicios en red	SI	Se deben identificar los mecanismos de seguridad, los niveles de servicio y los requisitos de gestión de los servicios de red e incluirlos en los acuerdos de servicios de red.
A.13.1.3	Segregación de redes	SI	Los distintos grupos dentro de la organización deben separarse en redes.
A.13.2	**Intercambio de información con partes externas**		
A.13.2.1	Políticas y procedimientos de intercambio de información	SI	Se deben definir políticas para proteger la transferencia de información mediante el uso de todo tipo de instalaciones de comunicación.
A.13.2.2	Acuerdos de intercambio	SI	Los acuerdos deben tener en cuenta la transferencia segura de la información entre la empresa y las partes externas.
A.13.2.3	Mensajería electrónica	SI	Se debe proteger adecuadamente la información incluida en mensajería electrónica.
A.13.2.4	Acuerdos de confidencialidad y secreto	SI	Se deben identificar, revisar y documentar los requisitos para los acuerdos de confidencialidad que reflejen las necesidades de la organización para la protección de la información.
A.14	**ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN**		

A.14.1	**Requisitos de seguridad de los sistemas de información**		
A.14.1.1	Análisis y especificación de los requisitos de seguridad	SI	Se deben incluir los requisitos relacionados con la seguridad de la información en los requisitos para los nuevos sistemas de información o para las mejoras de los sistemas existentes.
A.14.1.2	Seguridad de las comunicaciones en servicios accesibles por redes públicas	SI	La información que pasa por redes públicas debe protegerse de actividades fraudulentas, modificación no autorizada, divulgación, etc.
A.14.1.3	Protección de las transacciones por redes telemáticas	SI	Se debe proteger la información en las transacciones de los servicios de las aplicaciones para evitar alteración, divulgación, modificación no autorizada, etc.
A.14.2	**Seguridad en los procesos de desarrollo y soporte**		
A.14.2.1	Política de desarrollo seguro de software	SI	Se deben establecer reglas para el desarrollo de software que se realiza en la empresa.
A.14.2.2	Procedimientos de control de cambios en los sistemas	SI	Los cambios a los sistemas se deben controlar mediante procedimientos de control de cambios.
A.14.2.3	Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo	SI	Se deben revisar las aplicaciones críticas cuando se cambian las plataformas de operación y ponerlas a prueba para asegurar que no hay impacto adverso.
A.14.2.4	Restricciones a los cambios en los paquetes de software	SI	Se deben controlar todos los cambios de paquetes de software
A.14.2.5	Uso de principios de ingeniería en protección de sistemas	SI	Se deben establecer principios para la construcción de sistemas seguros.
A.14.2.6	Seguridad en entornos de desarrollo	SI	Se debe establecer un ambiente de desarrollo seguro.
A.14.2.7	Externalización del desarrollo software	NO	No se externaliza ningún tipo de desarrollo en la organización.
A.14.2.8	Pruebas de funcionalidad durante el desarrollo de los sistemas	SI	Se deben llevar a cabo pruebas de funcionalidad de la seguridad de los sistemas.
A.14.2.9	Pruebas de aceptación	SI	Se deben establecer programas de prueba para aceptación para los sistemas de información nuevos y actualizaciones de los existentes.
A.14.3	**Datos de prueba**		
A.14.3.1	Protección de los datos utilizados en pruebas	SI	Los datos de prueba deben estar adecuadamente protegidos y controlados.
A.15	**RELACIONES CON SUMINISTRADORES**		
A.15.1	**Seguridad de la información en las relaciones con suministradores**		
A.15.1.1	Política de seguridad de la información para suministradores	SI	Se deben acordar los requisitos de seguridad de la información con los suministradores para reducir los riesgos asociados con el acceso de éstos a los activos de la empresa.
A.15.1.2	Tratamiento del riesgo dentro de acuerdos de suministradores	SI	Se deben determinar los requisitos de seguridad de la información con cada proveedor que pueda tener acceso a activos de infraestructura TIC para la información de la comunicación.
A.15.1.3	Cadena de suministro en tecnologías de la información y comunicaciones	SI	Se deben definir los requisitos para tratar los riesgos de seguridad de la información asociados con la cadena de suministro de productos y servicios de las TIC.
A.15.2	**Gestión de la prestación del servicio por suministradores**		

A.15.2.1	Supervisión y revisión de los servicios prestados por terceros	SI	Se debe realizar un seguimiento de la prestación de servicios de los suministradores.
A.15.2.2	Gestión de cambios en los servicios prestados por terceros	SI	Se deben gestionar los cambios en el suministro de servicios por parte de los proveedores (mantenimiento, mejora de políticas, procedimientos, controles de seguridad existentes).
A.16	**GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN**		
A.16.1	**Gestión de incidentes de seguridad de la información y mejoras**		
A.16.1.1	Responsabilidades y procedimientos	SI	Se deben definir las responsabilidades y procedimientos de gestión de incidentes de seguridad para asegurar una respuesta rápida, eficaz y ordenada.
A.16.1.2	Notificación de los eventos de seguridad de la información	SI	Se deben establecer los canales adecuados para notificar los eventos de seguridad de la información.
A.16.1.3	Notificación de puntos débiles de la seguridad	SI	Se debe exigir a los trabajadores que observen e informen de cualquier debilidad en la seguridad que puedan encontrar.
A.16.1.4	Valoración de eventos de seguridad de la información y toma de decisiones	SI	Se deben evaluar los eventos de seguridad de la información y decidir si se van a clasificar como incidentes de seguridad de la información.
A.16.1.5	Respuesta a los incidentes de seguridad	SI	Se debe dar respuesta a los incidentes de seguridad de acuerdo a los procedimientos establecidos.
A.16.1.6	Aprendizaje de los incidentes de seguridad de la información	SI	Se debe usar el conocimiento adquirido al analizar y resolver los incidentes para reducir su probabilidad de aparición e impacto futuros.
A.16.1.7	Recopilación de las evidencias	SI	Se debe establecer un procedimiento de identificación, recolección, adquisición y preservación de información que pueda servir como evidencia.
A.17	**ASPECTOS DE LA SEGURIDAD DE LA INFORMACIÓN EN LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO**		
A.17.1	**Continuidad de la seguridad de la información**		
A.17.1.1	Planificación de la continuidad de la seguridad de la información	SI	Se deben determinar los requisitos de seguridad de la información y la continuidad de la gestión de ésta en situaciones adversas.
A.17.1.2	Implantación de la continuidad de la seguridad de la información	SI	Se deben implementar procesos y controles para asegurar el nivel de continuidad requerido de seguridad.
A.17.1.3	Verificación, revisión y evaluación de la continuidad de la seguridad de la información	SI	Se deben verificar periódicamente los controles de continuidad de seguridad implementados.
A.17.2	**Redundancias**		
A.17.2.1	Disponibilidad de instalaciones para el procesamiento de la información	NO	De momento no se va a aplicar este control
A.18	**CUMPLIMIENTO**		
A.18.1	**Cumplimiento de los requisitos legales y contractuales**		
A.18.1.1	Identificación de la legislación aplicable	SI	Se debe identificar la legislación y regulación pertinente para cumplirlas.
A.18.1.2	Derechos de propiedad intelectual (DPI)	SI	Se deben implementar los procedimientos apropiados para asegurar el cumplimiento de la legislación y regulación relacionadas con los

			derechos de propiedad intelectual y uso de software patentado.
A.18.1.3	Protección de los registros de la organización	SI	Los registros deben protegerse contra pérdida, destrucción, acceso no autorizado, falsificación y liberación no autorizada de acuerdo con los requisitos legislativos.
A.18.1.4	Protección de datos y privacidad de la información personal	SI	Se debe asegurar la privacidad y protección de la información de carácter personal de acuerdo a como dicta la ley.
A.18.1.5	Regulación de los controles criptográficos	SI	Se deben usar controles criptográficos de acuerdo a la legislación pertinente.
A.18.2	**Revisiones de la seguridad de la información**		
A.18.2.1	Revisión independiente de la seguridad de la información	SI	La seguridad de la información de la organización debe revisarse de manera independiente periódicamente o cuando ocurran cambios significativos.
A.18.2.2	Cumplimiento de las políticas y normas de seguridad	SI	La Dirección debe revisar regularmente el cumplimiento del procesamiento y procedimientos de información.
A.18.2.3	Comprobación del cumplimiento	SI	Los sistemas de información se deben revisar periódicamente para determinar el cumplimiento de las políticas de seguridad de la información.

Tabla 7. Declaración de Aplicabilidad

2.2.7. Metodología de Análisis de Riesgos

La metodología de análisis de riesgos elegida por CEINTECO es MAGERIT que tiene como característica fundamental que los riesgos que se plantean para una organización se expresan directamente en valores económicos, lo que ayudará a la toma de decisiones por parte de la Dirección de la empresa.

MAGERIT sigue una serie de fases antes de llegar a la elaboración e identificación de todos los riesgos de una organización. El proceso que sigue se muestra en la Imagen 16.

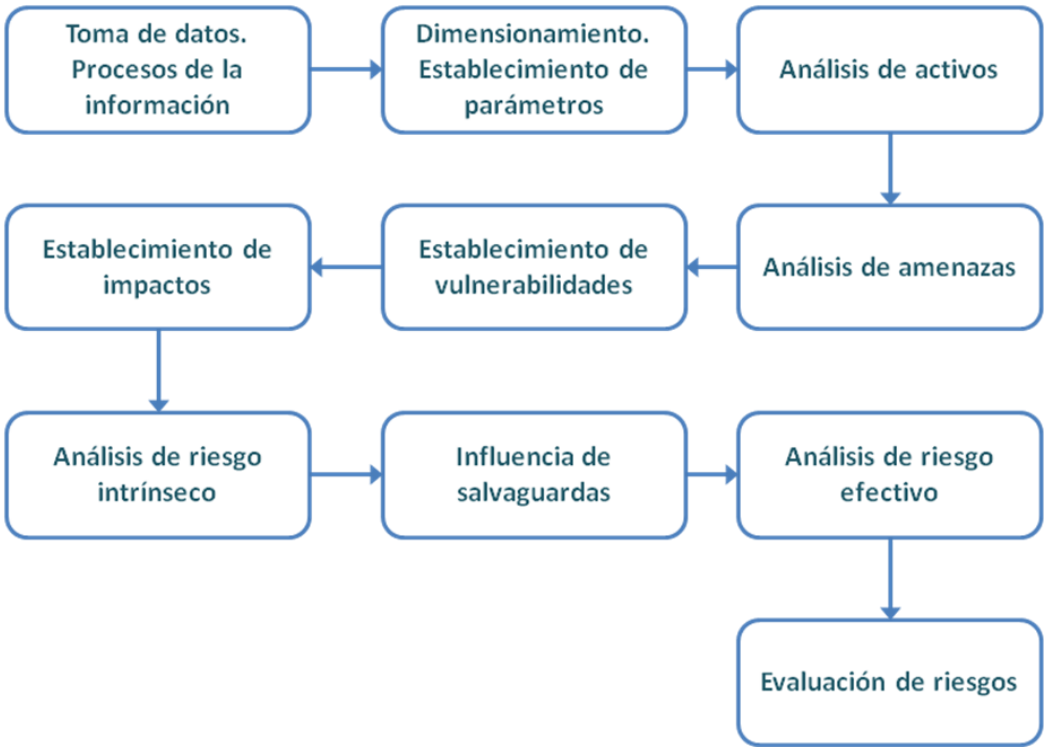


Imagen 16. Fases análisis de riesgos

A continuación se va a explicar en qué consiste cada una de estas fases.

Fase 1. Toma de datos y procesos de información

En la fase de toma de datos y procesos de información debe definirse el alcance que se va a analizar. Se debe tener en cuenta que cuanto mayor sea el alcance, mayor va a ser el número de riesgos analizables.

En esta fase se van a analizar los procesos que realiza CEINTECO, para determinar aquellos que son más críticos.

También se deben definir en esta fase las unidades que se pretende analizar, es decir, se debe determinar el nivel de detalle al que se quiere llegar. Una vez más, se debe tener en cuenta que cuanto más detalle, tendrán que analizarse más elementos y, por tanto, el análisis de riesgos será más costoso.

Fase 2. Establecimiento de parámetros

En esta fase se van a establecer los parámetros que se utilizarán durante todo el proceso de análisis de riesgos de CEINTECO.

Los parámetros que deben identificarse son los siguientes:

- Valor de los activos: Este parámetro se utiliza para asignar una valoración económica a todos los activos que la organización requiere para llevar a cabo sus procesos.

  En el momento de asignar las valoraciones hay que tener presente los siguientes puntos:

  - Valor de reposición: Se trata del valor que tiene para la organización reponer ese activo en caso de pérdida o que éste no pueda ser utilizado.
  - Valor de configuración: Se trata del tiempo necesario desde que se adquiere el nuevo activo hasta que se pone a punto para que pueda utilizarse.
  - Valor de uso del activo: Se trata del valor que pierde la organización durante el tiempo que no puede utilizar el activo para la función que desarrolla.
  - Valor de pérdida de oportunidad: Se trata del valor que pierde potencialmente la organización por no poder dispone del activo durante un tiempo.

  El procedimiento de valoración de activos que va se va a utilizar para el SGSI de CEINTECO se muestra en la Tabla 8.

Valoración	Rango	Valor
Muy alta	valor > 200.000€	300.000 €
Alta	100.000€ < valor >200.000€	150.000 €
Media	50.000€ < valor > 100.000 €	75.000 €
Baja	10.000€ < valor > 50.000 €	30.000€
Muy baja	valor < 10.000 €	10.000 €

Tabla 8. Procedimiento de valoración

- Vulnerabilidad: Se trata de la frecuencia de ocurrencia de una amenaza, es decir, la frecuencia con la que la organización puede sufrir alguna amenaza en concreto.

  Esta frecuencia también se debe de plasmar en una escala de valores. Una vez se tenga clara la escala de valores, hay que traducir estas vulnerabilidades a números. Esta valoración numérica se realiza mediante estimaciones anuales, de tal forma que:

  Vulnerabilidad = Frecuencia estimada / Días del año

  La escala de valores que se va a utilizar en el SGSI de CEINTECO se muestra a continuación en la Tabla 9.

Vulnerabilidad	Rango	Valor
Frecuencia extrema	1 vez al día	1
Frecuencia alta	1 vez cada 2 semanas	26/365 = 0.071233
Frecuencia media	1 vez cada 2 meses	6/365 = 0.016438
Frecuencia baja	1 vez cada 6 meses	2/365 = 0.005479
Frecuencia muy baja	1 vez al año	1/365 = 0.002739

Tabla 9. Clasificación de la vulnerabilidad

- Impacto: Se trata del tanto por ciento del valor del activo que se pierde en el caso de que suceda un incidente sobre él. Para realizar este análisis, hay que pensar, a priori, en los diferentes niveles de impacto que se quieren utilizar y a partir de ahí asignar el porcentaje de valor que se estima que puede perderse en cada caso.

  La valoración de los impactos que va a utilizar CEINTECO para su SGSI se muestra en la Tabla 10.

Impacto	Valor
Muy alto	100%
Alto	75%
Medio	50%
Bajo	20%
Muy bajo	5%

Tabla 10. Valoración de impactos

- Efectividad del control de seguridad: Este parámetro consiste en pensar cómo las diferentes medidas de seguridad que se van a implantar pueden reducir el riesgo detectado. Para esto, hay que tener en cuenta que las medidas de seguridad tienen dos modos de actuar con el riesgo: o reducen la vulnerabilidad o reducen el impacto que provoca el riesgo.

  La clasificación de niveles que se va a utilizar en el SGSI de CEINTECO se muestra en la Tabla 11.

Variación impacto/vulnerabilidad	Valor
Muy alto	100%
Alto	75%
Medio	50%
Bajo	30%
Muy bajo	10%

Tabla 11. Clasificación de niveles

Fase 3. Análisis de activos

En esta fase se deben identificar qué activos posee y necesita CEINTECO para llevar a cabo sus actividades, teniendo en cuenta que sólo se deben analizar los activos que están dentro del alcance del SGSI.

Los activos se clasificarán teniendo en cuenta los siguientes tipos:

- Activos físicos. Son los elementos de tipo *hardware* que se utilizan en la organización.
- Activos lógicos. Son los elementos de *software* que se utilizan en la empresa.
- Activos de personal. Son las personas que trabajan en la empresa.
- Activos de entorno e infraestructura. Son los elementos que posee la organización y que necesita para que el resto pueda funcionar correctamente.
- Activos intangibles. Son los elementos que no posee la empresa directamente pero que son importantes para ella.

Fase 4. Análisis de amenazas

Las amenazas son aquellas situaciones que podrían llegar a darse en una empresa y que desembocarían en un problema de seguridad.

Se clasifican en cuatro grupos:

- Accidentes. Se trata de situaciones provocadas involuntariamente y que la mayoría de veces no pueden evitarse, ya que pueden provocarse, por ejemplo, por efectos naturales.
- Errores. Se trata de situaciones cometidas de manera involuntaria por el propio desarrollo de las actividades diarias.
- Amenazas intencionales presenciales. Se trata de situaciones provocadas de manera voluntaria por el personal de la organización.
- Amenazas intencionales remotas. Se trata de situaciones provocadas voluntariamente por personas ajenas a la empresa.

Fase 5. Establecimiento de vulnerabilidades

Una vulnerabilidad es un agujero que existe en la empresa y que permite que una amenaza pueda dañar un activo.

En esta fase se tendrán en cuenta las vulnerabilidades existentes en CEINTECO para poder estimar la frecuencia de ocurrencia de una amenaza sobre un activo.

Fase 6. Establecimiento de impactos

Los impactos son las consecuencias que provoca en la organización el hecho de que una amenaza afecte a un activo.

En esta fase se analizarán los posibles impactos en los activos de CEINTECO. Para ello se tendrán en cuenta los siguientes puntos:

- El resultado de la agresión de una amenaza sobre un activo.
- El efecto sobre cada activo para poder agrupar los impactos según la relación de activos.
- El valor económico de las pérdidas producidas.
- Las pérdidas cuantitativas o cualitativas.

Fase 7. Análisis del riesgo intrínseco

En esta fase se obtendrá el riesgo intrínseco de CEINTECO.

Los riesgos intrínsecos son aquellos a los que la empresa está expuesta sin tener en cuenta las medidas de seguridad que se puedan implantar, es decir, las situaciones que puedan darse teniendo en cuenta todos los elementos que posee la organización.

Para calcular el riesgo intrínseco se aplicará la siguiente fórmula:

Riesgo = Valor del activo * Vulnerabilidad * Impacto

Fase 8. Influencia de salvaguardas

En esta fase se decidirá cuál es la mejor solución de seguridad que permita reducir los riesgos identificados.

Para ello se utilizarán medidas de salvaguarda tanto preventivas como correctivas.

Las salvaguardas preventivas son aquellas medidas de seguridad que reducen las vulnerabilidades, por lo que la frecuencia de ocurrencia de la vulnerabilidad quedaría disminuida:

Nueva vulnerabilidad = Vulnerabilidad * Porcentaje de disminución de la vulnerabilidad

Las salvaguardas correctivas son aquellas que reducen el impacto de las amenazas, por lo que el impacto de las amenazas quedaría reducido:

Nuevo impacto = Impacto * Porcentaje de disminución de impacto

Fase 9. Análisis de riesgo efectivo

En esta fase se obtendrá el riesgo efectivo que tendrá CEINTECO para cada una de las amenazas detectadas.

La fórmula que se va a utilizar para obtener este riesgo es la siguiente.

Riesgo efectivo = Valor efectivo * Nueva vulnerabilidad * Nuevo impacto

= Valor activo * (Vulnerabilidad * Porcentaje de disminución de vulnerabilidad) * (Impacto * Porcentaje de disminución de impacto)

= Riesgo intrínseco * Porcentaje de disminución de vulnerabilidad * Porcentaje de disminución de impacto

Fase 10. Evaluación de riesgos

En esta fase se llevará a cabo la toma de decisiones por parte de CEINTECO sobre las medidas de seguridad a escoger entre el listado de salvaguardas que permiten reducir los riesgos.
Se va a intentar disminuir todos los riesgos encontrados hasta situarlos por debajo del "umbral de riesgos", es decir, el punto en el que CEINTECO considera que los riesgos a los que se encuentra expuesta no son aceptables.

Además, se elaborará un plan de acción que contendrá la siguiente información:

- Establecimiento de prioridades. Se trata de identificar los riesgos, que tendrán que ser reducidos en primer lugar.
- Planteamiento de análisis de coste/beneficio. Se trata de analizar, para cada una de las medidas, el coste que supondría implantarlas y en qué porcentaje reduciría los riesgos.
- Selección de controles definitivos. Se trata de seleccionar los controles definitivos que CEINTECO implantará para reducir los riesgos por debajo del umbral.
- Asignación de responsabilidades. Se trata de asignar a los responsables de llevar a cabo la implantación de los controles.
- Implantación de los controles. Se trata de realizar la implantación de los controles de seguridad elegidos.

3. Fase 3: Análisis de riesgos

3.1. Introducción

El análisis de riesgos es la fase más importante en el ciclo de vida de la seguridad de la información de una organización. Este análisis servirá para descubrir qué necesidades de seguridad tiene la empresa tras detectar cuáles son los puntos débiles en seguridad y las amenazas a las que se encuentra expuesta.

En primer lugar se identificarán y clasificarán todos los activos de la organización vinculados a la información, obteniendo el inventario de activos de CEINTECO. A continuación se determinará el valor de cada uno de los activos identificados. Una vez identificados y valorados los activos, se llevará a cabo el análisis de las amenazas a las que están expuestos los activos identificados, es decir, se listarán las distintas amenazas y se analizará, para cada uno de los activos identificado, con qué frecuencia puede producirse cada una de las amenazas y el impacto que tendría en la distintas dimensiones de seguridad del activo. Posteriormente, se determinará el impacto potencial que supondría para CEINTECO la materialización de las amenazas encontradas. Por último, se calculará el nivel del riego aceptable y el riesgo residual.

3.2. Inventario de activos

El primer paso para realizar un análisis de riesgos es la identificación de los activos que están dentro del alcance del SGSI de la organización y que son necesarios para llevar a cabo sus actividades.

Los activos se van clasificar en distintos ámbitos acorde con la metodología MAGERIT. Los ámbitos que se van a utilizar son los siguientes:

- Instalaciones [L]: Lugares donde se hospedan los sistemas de información y comunicaciones.
- Hardware [HW]: Los medios materiales, físicos, destinados a soportar directa o indirectamente los servicios que presta la organización.
- Aplicación [SW]: Tareas que han sido automatizadas para su desempeño por un equipo informático. Las aplicaciones gestionan, analizan y transforman los datos permitiendo la explotación de la información para la prestación de servicios.
- Datos [D]: La información que permite a la organización prestar sus servicios.
- Red [COM]: Son los medios de transporte que llevan datos de un sitio a otro. Se incluyen tanto instalaciones dedicadas como servicios de comunicaciones contratados a terceros.
- Servicios [S]: Servicios prestados por el sistema.
- Equipamiento auxiliar [AUX]: Otros equipos que sirven de soporte a los sistemas de información, sin estar directamente relacionados con éstos.
- Personal [P]: Personas relacionadas con los sistemas de información.

En la Tabla 12 muestra el inventario de activos de CEINTECO.

Ámbito	ID	Activo
Instalaciones [L]	L1	Pasillo administración y despachos dirección
	L2	Pasillo grupo investigación 1
	L3	Pasillo grupo investigación 2
	L4	Pasillo grupo investigación 3
	L5	Pasillo grupo investigación 4
	L6	Sala 1.1
	L7	Sala 1.2
	L8	Sala 2.1
	L9	Sala 2.2
	L10	Sala 3.1
	L11	Sala 3.2
	L12	Sala 4.1
	L13	Sala 4.2
	L14	Oficina jefe grupo 1
	L15	Oficina jefe grupo 2
	L16	Oficina jefe grupo 3
	L17	Oficina jefe grupo 4
	L18	Laboratorio 1
	L19	Laboratorio 2
	L20	Laboratorio 3
	L21	Laboratorio 4
	L22	Sala Servidores 1
	L23	Sala Servidores 2
	L24	Despacho director
	L25	Despacho subdirector general
	L26	Despacho subdirector investigación
	L27	Despacho secretario
	L28	Sala copias de seguridad

	L29	Sala servidores globales
Hardware [HW]	HW1	Servidor correo
	HW2	Servidor web
	HW3	Servidor BBDD huellas
	HW4	Servidores repositorio código (2)
	HW5	Equipos copias seguridad (2)
	HW6	Ordenadores simulación (10)
	HW7	Firewall (2)
	HW8	Impresoras de red (5)
	HW9	Teléfonos IP (85)
	HW10	Portátiles
	HW11	PCs personal investigación
	HW12	PCs administración
	HW13	Punto acceso Wi-Fi
	HW14	Escáner huellas (7)
Aplicación [SW]	SW1	S.O. Windows 7 Professional
	SW2	S.O. Ubuntu
	SW3	Microsoft Windows Server 2008
	SW4	Microsoft Office 2013
	SW5	Microsoft Visual Studio
	SW6	Matlab
	SW7	Adobe Acrobat Professional
	SW8	LaTeX
	SW9	Antivirus
	SW10	Aplicaciones internas administración
	SW11	Aplicación gestión copias de seguridad
Datos [D]	D1	Base de datos de huellas
	D2	Datos de los trabajadores
	D3	Datos de los clientes
	D4	Información del acceso de visitas
	D5	Copias seguridad servidores

	D6	Código fuente desarrollos
	D7	Datos de investigaciones y experimentos
Red [COM]	COM1	Cableado eléctrico
	COM2	Cableado telecomunicaciones
	COM3	Servicio VoIP
	COM4	Servicio Internet
	COM5	Red inalámbrica
Servicios [S]	S1	Correo electrónico
	S2	Acceso remoto
	S3	Página web
Equipamiento auxiliar [AUX]	AUX1	Sistema de climatización
	AUX2	Sistema detección incendios
	AUX3	Sistema de alimentación ininterrumpido (SAI)
	AUX4	Extintores (5)
	AUX5	Televisión
	AUX6	Generador de señales IQ (2)
	AUX7	Analizador de espectro
	AUX8	Femtocelda LTE
	AUX9	Receptor de señales IQ (2)
	AUX10	Analizador de red vectorial (2)
	AUX11	Conversor de frecuencia
	AUX12	Fuente de radiofrecuencia
	AUX13	Analizador de espectro óptico
	AUX14	Osciloscopio (3)
	AUX15	Equipamiento radiodifusión
	AUX16	Terminales móviles (3)
	AUX17	Altavoces (10)
	AUX18	Micrófonos (10)
	AUX19	Analizador de audio
	AUX20	Destructor papeles
Personal [P]	P1	Director general

	P2	Subdirector general
	P3	Subdirector investigación
	P4	Secretario
	P5	Personal administración
	P6	Responsable Seguridad
	P7	Técnico centro investigación
	P8	Técnicos de grupo
	P9	Jefes de grupo
	P10	Personal de investigación

Tabla 12. Inventario de activos

3.3. Valoración de los activos

Una vez realizada la identificación de los activos, se debe valorar cada uno de los activos identificados. Para ello, se debe tener en cuenta no sólo el valor de cada activo por separado sino también las dependencias entre los activos, ya que éstos se encuentran jerarquizados dentro de la organización.

En primer lugar se van a analizar las dependencias entre activos. Se dice que un "activo superior" depende de otro "activo inferior" cuando las necesidades de seguridad del superior se reflejan en las necesidades de seguridad del inferior, es decir, cuando la materialización de una amenaza en el activo inferior tiene como consecuencia un perjuicio sobre el activo superior.

En las siguientes imágenes se muestran las dependencias de algunos de los activos pertenecientes al ámbito Datos [D] y Servicios [S].

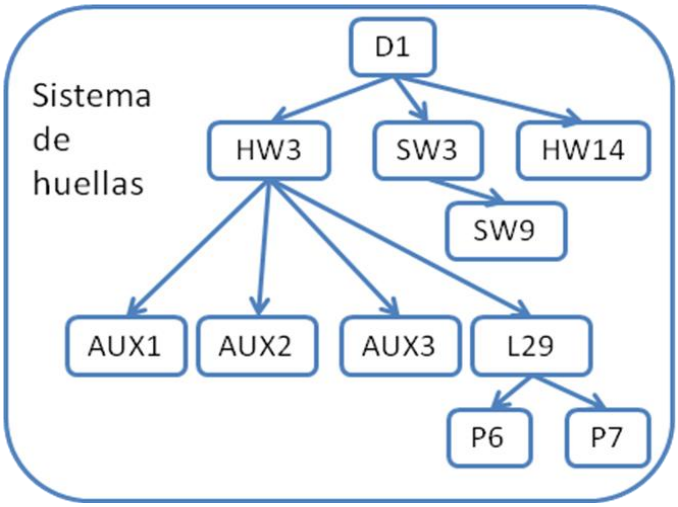


Imagen 17. Dependencias del activo D1 - Base de datos de huellas

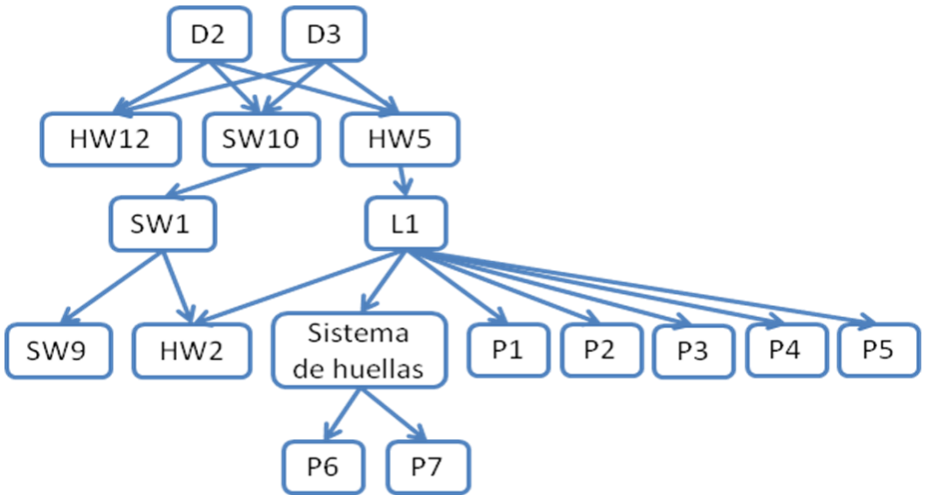


Imagen 18. Dependencias de los activos D2 - Datos de los trabajadores y D3 - Datos de los clientes

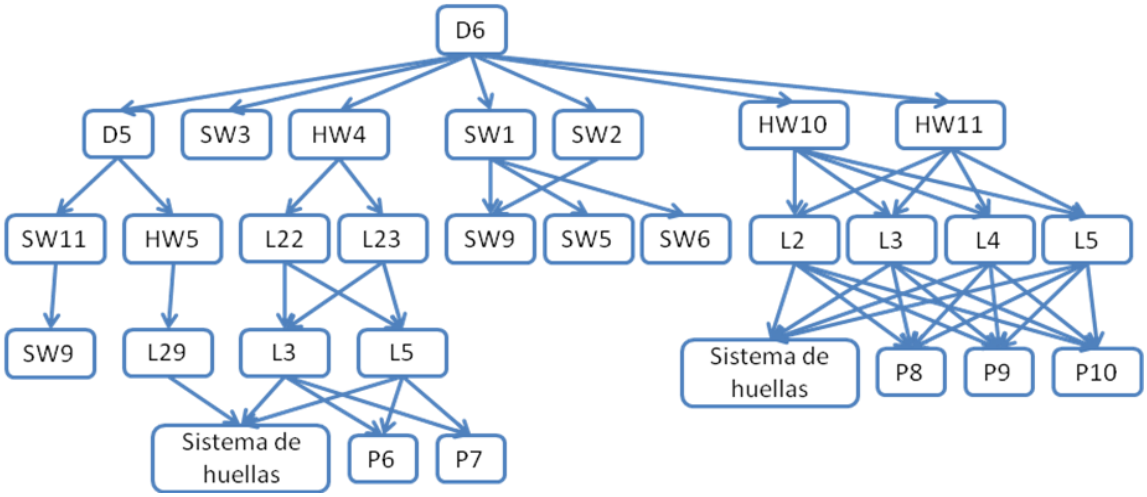


Imagen 19. Dependencias del activo D6 - Código fuente desarrollos

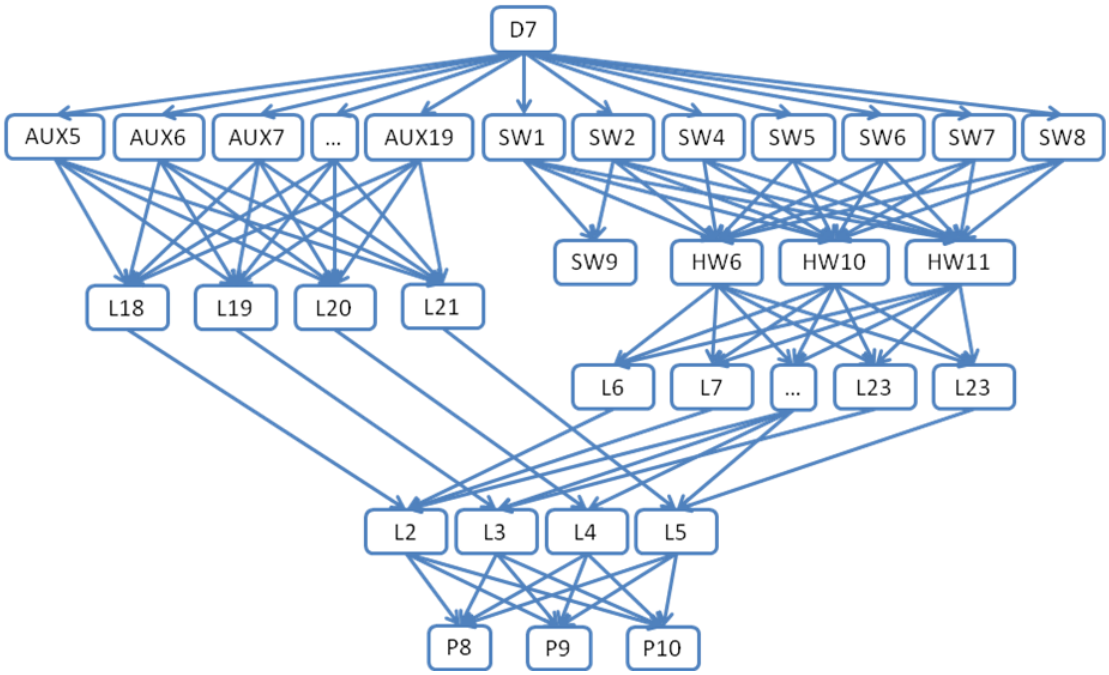


Imagen 20. Dependencias del activo D7 - Datos de investigaciones y experimentos

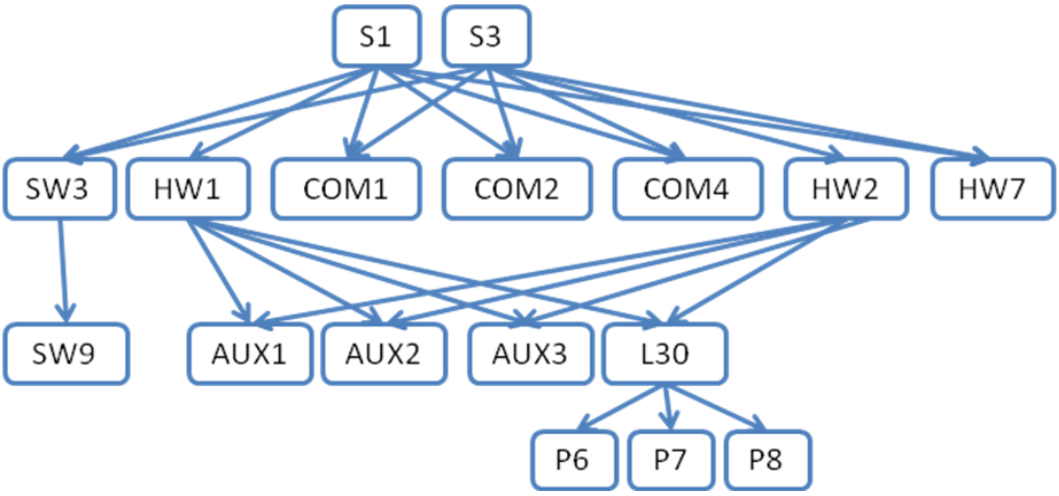


Imagen 21. Dependencias de los activos S1 - Correo electrónico y S3 - Página web

A continuación se va a realizar la valoración de cada uno de los activos inventariados. A la hora de asignar un valor a cada activo se van a tener en cuenta las siguientes consideraciones:

El valor de reposición del activo en caso de que éste se pierda o no pueda ser utilizado.

El tiempo que se necesita desde que se adquiere el nuevo activo hasta que se pone a punto para que pueda utilizarse.

El valor que pierde la organización durante el tiempo en el que no se puede utilizar el activo.

El valor que pierde potencialmente la organización por no poder disponer del activo durante un tiempo.

En la Tabla 13 se muestra la escala de la valoración de activos que se va a utilizar. Ésta está basada en la propuesta de MAGERIT en su Libro III.

Valoración	ID	Rango	Valor
Muy alta	MA	valor > 200.000€	300.000 €
Alta	A	100.000€ < valor >200.000€	150.000 €
Media	M	50.000€ < valor > 100.000 €	75.000 €
Baja	B	10.000€ < valor > 50.000 €	30.000€
Muy baja	MB	valor < 10.000 €	10.000 €

Tabla 13. Escala valoración activos

Este procedimiento de valoración de activos va a permitir realizar la asignación de un valor tanto cualitativo como cuantitativo a cada uno de los activos identificados.

Más adelante, en la Tabla 15 se muestran los valores asignados a los activos que forman parte de la empresa CEINTECO.

3.4. Dimensiones de seguridad

Además de la valoración de los activos debe indicarse el aspecto de la seguridad más crítico de cada activo. Por esto, tras haber obtenido la valoración de cada uno de los activos, se va a realizar la valoración ACIDT de dichos activos, es decir, se va a medir la criticidad en las cinco dimensiones de la seguridad de la información.

Las dimensiones se utilizan para valorar las consecuencias de la materialización de una amenaza. La valoración que recibe un activo en una cierta dimensión es la medida de perjuicio para la organización si el activo se ve dañado en dicha dimensión.

Las cinco dimensiones que se van a analizar para cada uno de los activos de CEINTECO son las siguientes:

Autenticidad [A]: Propiedad o característica consistente en que una entidad es quien dice ser o bien que garantiza la fuente de la que proceden los datos. Para valorar un activo en esta dimensión hay que realizarse la siguiente pregunta: ¿Qué importancia tendría que quien accede al servicio no sea realmente quien se cree?

Confidencialidad [C]: Propiedad o característica consistente en que la información ni se pone a disposición, ni se revela a individuos, entidades o procesos no autorizados. Para valorar un activo en esta dimensión hay que realizarse la siguiente pregunta: ¿Qué importancia tendría que el dato fuera conocido por personas no autorizadas?

Integridad [I]: Propiedad o característica consistente en que el activo de información no ha sido alterado de manera no autorizada. Para valorar un activo en esta dimensión hay que realizarse la siguiente pregunta: ¿Qué importancia tendría que los datos fueran modificados fuera de control?

Disponibilidad [D]: Propiedad o característica de los activos consistente en que las entidades o procesos autorizados tienen acceso a los mismos cuando lo requieren. Para valorar un activo en esta dimensión hay que realizarse la siguiente pregunta: ¿Qué importancia tendría el activo si no estuviera disponible?

Trazabilidad [T]: Propiedad o característica consistente en que las actuaciones de una entidad pueden ser imputadas exclusivamente a dicha entidad. Para valorar un activo en esta dimensión hay que realizarse la siguiente pregunta: ¿Qué importancia tendría que no quedara constancia fehaciente del uso del servicio?

Para valorar los activos en las cinco dimensiones se necesita tener clara qué escala de valoración se va a utilizar. En este caso se va a utilizar la escala propuesta en la Tabla 14.

Valor		Criterio
10	Muy alto	Daño muy grave para la organización
7-9	Alto	Daño grave para la organización
4-6	Medio	Daño importante para la organización
1-3	Bajo	Daño menor para la organización
0	Muy bajo	Irrelevante para la organización

Tabla 14. Valoración dimensiones de seguridad

3.5. Tabla resumen de valoración

En este apartado se muestra la Tabla 15, donde se han especificado los valores de cada uno de los activos de CEINTECO tanto de manera general como respecto a las cinco dimensiones de la seguridad de la información.

Ámbito	ID	Activo	Valor	Aspectos críticos				
				A	C	I	D	T
Instalaciones [L]	L1	Pasillo administración y despachos dirección	MA	8	0	0	8	5
	L2	Pasillo grupo investigación 1	B	8	0	0	8	0
	L3	Pasillo grupo investigación 2	B	8	0	0	8	0
	L4	Pasillo grupo investigación 3	B	8	0	0	8	0
	L5	Pasillo grupo investigación 4	B	8	0	0	8	0
	L6	Sala 1.1	M	8	1	0	8	2
	L7	Sala 1.2	M	8	1	0	8	2
	L8	Sala 2.1	M	8	1	0	8	2
	L9	Sala 2.2	M	8	1	0	8	2
	L10	Sala 3.1	M	8	1	0	8	2
	L11	Sala 3.2	M	8	1	0	8	2
	L12	Sala 4.1	M	8	1	0	8	2
	L13	Sala 4.2	M	8	1	0	8	2
	L14	Oficina jefe grupo 1	B	6	1	0	5	2
	L15	Oficina jefe grupo 2	B	6	1	0	5	2
	L16	Oficina jefe grupo 3	B	6	1	0	5	2
	L17	Oficina jefe grupo 4	B	6	1	0	5	2
	L18	Laboratorio 1	A	8	2	0	8	5
	L19	Laboratorio 2	A	8	2	0	8	5
	L20	Laboratorio 3	A	8	2	0	8	5
	L21	Laboratorio 4	A	8	2	0	8	5
	L22	Sala Servidores 1	M	8	5	0	8	7
	L23	Sala Servidores 2	M	8	5	0	8	7
	L24	Despacho director	M	6	2	0	5	5
	L25	Despacho subdirector general	M	6	2	0	5	5

	L26	Despacho subdirector investigación	M	6	2	0	5	5
	L27	Despacho secretario	M	6	2	0	5	5
	L28	Sala copias de seguridad	M	8	5	0	8	7
	L29	Sala servidores globales	M	8	5	0	8	7
Hardware [HW]	HW1	Servidor correo	M	8	8	8	8	7
	HW2	Servidor web	B	8	4	6	5	7
	HW3	Servidor BBDD huellas	M	8	8	9	9	7
	HW4	Servidores repositorio código (2)	M	8	8	8	8	7
	HW5	Equipos copias seguridad (2)	M	8	8	8	7	7
	HW6	Ordenadores simulación (10)	M	7	8	9	9	7
	HW7	Firewall (2)	M	8	8	7	6	8
	HW8	Impresoras de red (5)	MB	7	8	0	3	4
	HW9	Teléfonos IP (85)	MB	6	7	7	4	6
	HW10	Portátiles	B	8	9	8	9	8
	HW11	PCs personal investigación	B	8	9	8	9	8
	HW12	PCs administración	B	9	9	9	9	9
	HW13	Punto acceso Wi-Fi	MB	7	7	8	5	8
	HW14	Escáner huellas (7)	B	8	3	7	9	8
Aplicación [SW]	SW1	S.O. Windows 7 Professional	B	8	7	7	9	6
	SW2	S.O. Ubuntu	MB	8	7	8	9	6
	SW3	Microsoft Windows Server 2008	B	8	7	9	9	8
	SW4	Microsoft Office 2013	B	6	6	7	5	6
	SW5	Microsoft Visual Studio	B	7	6	8	8	7
	SW6	Matlab	B	7	6	8	8	7
	SW7	Adobe Acrobat Professional	B	5	6	7	3	7
	SW8	LaTeX	B	5	6	7	6	7
	SW9	Antivirus	B	7	8	9	9	7
	SW10	Aplicaciones internas administración	B	9	9	9	9	8
	SW11	Aplicación gestión copias de seguridad	B	8	8	9	9	8
Datos [D]	D1	Base de datos de huellas	A	9	9	9	9	8
	D2	Datos de los trabajadores	A	8	9	7	7	8

	D3	Datos de los clientes	MA	9	10	8	8	8
	D4	Información del acceso de visitas	MB	3	2	2	1	2
	D5	Copias seguridad servidores	M	8	8	9	9	8
	D6	Código fuente desarrollos	MA	9	10	10	10	9
	D7	Datos de investigaciones y experimentos	MA	8	10	9	9	8
Red [COM]	COM1	Cableado eléctrico	A	0	0	0	9	0
	COM2	Cableado telecomunicaciones	A	0	0	0	9	0
	COM3	Servicio VoIP	MB	8	8	5	5	7
	COM4	Servicio Internet	M	8	8	8	8	7
	COM5	Red inalámbrica	MB	8	8	8	3	7
Servicios [S]	S1	Correo electrónico	M	8	9	8	8	7
	S2	Acceso remoto	MB	8	8	7	6	7
	S3	Página web	MB	4	4	8	6	6
Equipamiento auxiliar [AUX]	AUX1	Sistema de climatización	A	0	0	0	9	0
	AUX2	Sistema detección incendios	A	0	0	0	9	0
	AUX3	Sistema de alimentación ininterrumpido (SAI)	A	0	0	0	9	0
	AUX4	Extintores (5)	A	0	0	0	9	0
	AUX5	Televisión	MB	0	0	0	2	0
	AUX6	Generador de señales IQ (2)	M	0	0	0	3	0
	AUX7	Analizador de espectro	M	0	0	0	3	0
	AUX8	Femtocelda LTE	M	0	0	0	3	0
	AUX9	Receptor de señales IQ (2)	M	0	0	0	3	0
	AUX10	Analizador de red vectorial (2)	M	0	0	0	3	0
	AUX11	Conversor de frecuencia	M	0	0	0	3	0
	AUX12	Fuente de radiofrecuencia	M	0	0	0	3	0
	AUX13	Analizador de espectro óptico	M	0	0	0	3	0
	AUX14	Osciloscopio (3)	M	0	0	0	3	0
	AUX15	Equipamiento radiodifusión	M	0	0	0	3	0
	AUX16	Terminales móviles (3)	MB	8	7	7	3	4
	AUX17	Altavoces (10)	B	0	0	0	3	0

	AUX18	Micrófonos (10)	B	0	0	0	3	0
	AUX19	Analizador de audio	M	0	0	0	3	0
	AUX20	Destructor papeles	MB	0	0	0	1	0
Personal [P]	P1	Director general	MA	0	0	0	9	0
	P2	Subdirector general	A	0	0	0	8	0
	P3	Subdirector investigación	A	0	0	0	8	0
	P4	Secretario	M	0	0	0	7	0
	P5	Personal administración	M	0	0	0	8	0
	P6	Responsable Seguridad	M	0	0	0	8	0
	P7	Técnico centro investigación	M	0	0	0	8	0
	P8	Técnicos de grupo	M	0	0	0	7	0
	P9	Jefes de grupo	M	0	0	0	7	0
	P10	Personal de investigación	A	0	0	0	8	0

Tabla 15. Valoración de los activos de CEINTECO

3.6. Análisis de amenazas

Todos los activos de una organización están expuestos a diversas amenazas que pueden afectar a los distintos aspectos de la seguridad de la empresa. Por este motivo en este apartados se van a analizar qué amenazas pueden afectar a qué activos de CEINTECO. Posteriormente, se va a estimar cuán vulnerable es cada uno de los activos a la materialización de la amenaza así como la estimación de la frecuencia de la misma.

Se va a utilizar la metodología MAGERIT para realizar este análisis de amenazas. Las amenazas están clasificadas en los siguientes grupos:

Desastres naturales [N].
De origen industrial [I].
Errores y fallos no intencionados [E].
Ataques intencionados [A].

A continuación, en la Tabla 16, se presenta el catálogo de las amenazas posibles sobre los activos de CEINTECO.

Grupo	ID	Amenaza
Desastres naturales [N]	N1	Fuego
	N2	Daños por agua
	N3	Tormenta eléctrica
	N4	Terremoto
De origen industrial [I]	I1	Fuego
	I2	Daños por agua
	I3	Sobrecarga eléctrica
	I4	Explosión
	I5	Derrumbe
	I6	Contaminación mecánica
	I7	Contaminación electromagnética
	I8	Avería de origen física o lógico
	I9	Corte eléctrico
	I10	Condiciones inadecuadas de temperatura y/o humedad
	I11	Fallo del servicio de comunicaciones
	I12	Interrupción de otros servicios y suministros esenciales
	I13	Degradación de los soportes de almacenamiento de la información
	I14	Emanaciones electromagnéticas
Errores y fallos no intencionados [E]	E1	Errores de los investigadores
	E2	Errores de los técnicos
	E3	Errores de monitorización
	E4	Errores de configuración
	E5	Deficiencias en la organización
	E6	Difusión de software dañino
	E7	Errores de (re-)encaminamiento
	E8	Errores de secuencia
	E9	Escapes de información
	E10	Alteración accidental de información
	E11	Destrucción de información
	E12	Fugas de información

	E13	Vulnerabilidades del software
	E14	Errores de mantenimiento/actualización de software
	E15	Errores de mantenimiento/actualización de hardware
	E16	Caída del sistema por agotamiento de recursos
	E17	Pérdida de equipos
	E18	Indisponibilidad del personal
Ataques intencionados [A]	A1	Manipulación de los registros de actividad
	A2	Manipulación de la configuración
	A3	Suplantación de la identidad del usuario
	A4	Abuso de privilegios de acceso
	A5	Uso no previsto
	A6	Difusión de software dañino
	A7	(Re)-encaminamiento de mensajes
	A8	Alteración de secuencia
	A9	Acceso no autorizado
	A10	Análisis de tráfico
	A11	Repudio
	A12	Interceptación de información
	A13	Modificación deliberada de la información
	A14	Destrucción de información
	A15	Divulgación de información
	A16	Manipulación de software
	A17	Manipulación de equipos
	A18	Denegación de servicio
	A19	Robo
	A20	Ataque destructivo
	A21	Ocupación enemiga
	A22	Indisponibilidad del personal
	A23	Extorsión
	A24	Ingeniería social

Tabla 16. Catálogo de amenazas posibles

La frecuencia de la ocurrencia de una amenaza se va a medir como se muestra en la Tabla 17.

Vulnerabilidad	ID	Rango	Valor
Frecuencia muy alta	MA	1 vez al día	1
Frecuencia alta	A	1 vez cada 2 semanas	26/365 = 0.071
Frecuencia media	M	1 vez cada 2 meses	6/365 = 0.016
Frecuencia baja	B	1 vez cada 6 meses	2/365 = 0.005
Frecuencia muy baja	MB	1 vez al año	1/365 = 0.002

Tabla 17. Frecuencia de ocurrencia de una amenaza

La valoración del impacto que la ocurrencia de una amenaza produciría sobre las dimensiones de seguridad de un activo se muestra en la Tabla 18.

Impacto	ID	Valor
Muy alto	MA	100%
Alto	A	75%
Medio	M	50%
Bajo	B	20%
Muy bajo	MB	5%

Tabla 18. Valoración del impacto de una amenaza

A continuación se muestra, en la Tabla 19, el análisis de las amenazas que afectan a cada uno de los activos de CEINTECO, detallando en ella la frecuencia de ocurrencia de cada amenaza sobre cada activo y el impacto que tendría la ocurrencia de cada una de las amenazas sobre cada una de las cinco dimensiones de seguridad de cada activo.

Grupo	Amenaza	Activo	Frecuencia amenaza		Impacto amenaza (%)				
			Frec.	Valor	A	C	I	D	T
Desastres naturales [N]	Fuego [N1]	Instalaciones [I]	MB	0.002				100	
		Hardware [HW]						100	
		Cableado eléctrico [COM1]						100	
		Cableado telecomunicaciones [COM2]						100	
		Equipamiento auxiliar [AUX]						100	
	Daños por agua [N2]	Instalaciones [I]	MB	0.002				75	
		Hardware [HW]						75	
		Equipamiento auxiliar [AUX]						75	
	Tormenta eléctrica [N3]	Hardware [HW]	MB	0.002				75	
		Cableado eléctrico [COM1]						50	

		Equipamiento auxiliar [AUX]						50	
	Terremoto [N4]	Instalaciones [I]	MB	0.002				100	
		Hardware [HW]						75	
		Equipamiento auxiliar [AUX]						75	
De origen industrial [I]	Fuego [I1]	Instalaciones [I]	MB	0.002				100	
		Hardware [HW]						100	
		Cableado eléctrico [COM1]						100	
		Cableado telecomunicaciones [COM2]						100	
		Equipamiento auxiliar [AUX]						100	
	Daños por agua [I2]	Instalaciones [I]	MB	0.002				75	
		Hardware [HW]						75	
		Equipamiento auxiliar [AUX]						75	
	Sobrecarga eléctrica [I3]	Hardware [HW]	B	0.005				75	
		Cableado eléctrico [COM1]						50	
		Equipamiento auxiliar [AUX]						50	
	Explosión [I4]	Instalaciones [I]	MB	0.002				100	
		Hardware [HW]						100	
		Equipamiento auxiliar [AUX]						100	
		Cableado eléctrico [COM1]						100	
		Cableado telecomunicaciones [COM2]						100	
	Derrumbe [I5]	Instalaciones [I]	MB	0.002				100	
		Hardware [HW]						75	
		Equipamiento auxiliar [AUX]						75	
		Cableado eléctrico [COM1]						50	
		Cableado telecomunicaciones [COM2]						50	
	Contaminación mecánica [I6]	Hardware [HW]	MB	0.002				50	
		Equipamiento auxiliar [AUX]						50	
	Contaminación electromagnética [I7]	Hardware [HW]	MB	0.002				75	
		Equipamiento auxiliar [AUX]						75	
	Avería de origen física o	Instalaciones [I]	B	0.005				50	

	lógico [I8]	Hardware [HW]						50	
		Software [SW]						50	
		Equipamiento auxiliar [AUX]						20	
		Servicios [S]						50	
	Corte eléctrico [I9]	Hardware [HW]	B	0.005				100	
		Equipamiento auxiliar [AUX]						100	
	Condiciones inadecuadas de temperatura y/o humedad [I10]	Hardware [HW]	B	0.05				50	
		Equipamiento auxiliar [AUX]						50	
		Servicios [S]						50	
	Fallo del servicio de comunicaciones [I11]	Servicio VoIP [COM3]	M	0.016				100	
		Servicio Internet [COM4]						100	
		Red inalámbrica [COM5]						100	
		Correo electrónico [S1]						100	
		Acceso remoto [S2]						100	
	Interrupción de otros servicios y suministros esenciales [I12]	Sistema de climatización [AUX1]	B	0.05				50	
		Sistema de alimentación ininterrumpido [AUX2]						5	
	Degradación de los soportes de almacenamiento de la información [I13]	Servidor BBDD huellas [HW3]	MB	0.002				75	
		Servidor repositorio código [HW4]						75	
		Equipos copias de seguridad [HW5]						75	
	Emanaciones electromagnéticas [I14]	Instalaciones [I]	MB	0.002		20			
		Hardware [HW]				50			
		Equipamiento auxiliar [AUX]				20			
Errores y fallos no intencionados [E]	Errores de los investigadores [E1]	Instalaciones [I]	M	0.016		20	50	5	
		Hardware [HW]				20	20	50	
		Software [SW]				50	75	50	
		Equipamiento auxiliar [AUX]				20	20	50	
		Datos [D]				75	75	50	
	Errores de los técnicos [E2]	Instalaciones [I]	M	0.016		20	20	50	
		Hardware [HW]				20	50	5	
		Software [SW]				50	75	50	

		Equipamiento auxiliar [AUX]				20	20	50	
		Datos [D]				75	75	50	
		Servicios [S]				50	75	50	
	Errores de monitorización [E3]	Datos	B	0.005					20
	Errores de configuración [E4]	Software [SW]	B	0.005				50	
		Datos [D]						50	
	Deficiencias en la organización [E5]	Personal [P]	M	0.016				75	
		Instalaciones [I]						75	
		Datos [S]						75	
	Difusión de software dañino [E6]	Software [SW]	MB	0.002		75	75	75	
		Datos [D]				50	50	50	
	Errores de (re-)encaminamiento [E7]	Software [SW]	MB	0.02		50			
		Servicio VoIP [COM1]				50			
		Servicio Internet [COM2]				50			
		Red inalámbrica [COM3]				50			
		Servicios [S]				50			
	Errores de secuencia [E8]	Software [SW]	MB	0.02		50			
		Servicio VoIP [COM1]				50			
		Servicio Internet [COM2]				50			
		Red inalámbrica [COM3]				50			
		Servicios [S]				50			
	Escapes de información [E9]	Instalaciones [I]	B	0.005		20			
		Software [SW]				20			
		Datos [D]				100			
		Servicios [S]				20			
	Alteración accidental de información [E10]	Datos [D]	M	0.016			75		
	Destrucción de información [E11]	Datos [D]	B	0.005				100	
	Fugas de información [E12]	Instalaciones [I]	B	0.005		20			
		Software [SW]				20			
		Datos [D]				100			

		Servicios [S]				20			
	Vulnerabilidades del software [E13]	Software [SW]	M	0.016		75	20	75	
		Datos [D]				75	50	75	
	Errores de mantenimiento/actualización de software [E14]	Software [SW]	B	0.005			50	75	
	Errores de mantenimiento/actualización de hardware [E15]	Hardware [HW]	B	0.005				75	
	Caída del sistema por agotamiento de recursos [E16]	Servicio VoIP [COM1]	MB	0.002				100	
		Servicio Internet [COM2]						100	
		Red inalámbrica [COM3]						100	
		Servicios [S]						100	
	Pérdida de equipos [E17]	Hardware [HW]	B	0.005				100	
		Equipamiento auxiliar [AUX]						100	
	Indisponibilidad del personal [E18]	Personal [P]	A	0.071				100	
Ataques intencionados [A]	Manipulación de los registros de actividad [A1]	Datos [D]	MB	0.002					75
	Manipulación de la configuración [A2]	Datos [D]	MB	0.002	75	75	75		
	Suplantación de la identidad del usuario [A3]	Software [SW]	B	0.005	75	75	50		
		Datos [D]			100	75	50		
		Servicios [S]			75	75	50		
		Servicio VoIP [COM3]			75	75	50		
		Red inalámbrica [COM5]			75	75	50		
	Abuso de privilegios de acceso [A4]	Instalaciones [I]	B	0.005		75	50	50	
		Hardware [HW]				75	50	50	
		Equipamiento auxiliar [AUX]				50	50	50	
		Software [SW]				100	50	50	
		Datos [D]				100	50	50	
		Servicios [S]				75	50	50	
	Uso no previsto [A5]	Hardware [HW]	MB	0.002		20	20	20	
		Equipamiento auxiliar [AUX]				20	20	20	
		Software [SW]				20	20	20	
		Datos [D]				20	20	20	

		Servicios [S]				20	20	20	
	Difusión de software dañino [A6]	Software [SW]	MB	0.002		75	75	75	
	(Re)-encaminamiento de mensajes [A7]	Software [SW]	MB	0.002		50			
		Servicio VoIP [COM1]				50			
		Servicio Internet [COM2]				50			
		Red inalámbrica [COM3]				50			
		Servicios [S]				50			
	Alteración de secuencia [A8]	Software [SW]	MB	0.002				50	
		Servicio VoIP [COM1]						50	
		Servicio Internet [COM2]						50	
		Red inalámbrica [COM3]						50	
		Servicios [S]						50	
	Acceso no autorizado [A9]	Instalaciones [I]	B	0.005		50		5	
		Hardware [HW]				50		5	
		Equipamiento auxiliar [AUX]				50		5	
		Software [SW]				75		75	
		Datos [D]				100		75	
		Red [COM]				75		75	
		Servicios [S]				75		75	
	Análisis de tráfico [A10]	Datos [D]	MB	0.002		50			
	Repudio [A11]	Servicios [S]	MB	0.002					75
	Interceptación de información [A12]	Datos [D]	B	0.005		100			
	Modificación deliberada de la información [A13]	Instalaciones [I]	MB	0.002			50		
		Datos [D]					100		
		Software [SW]					75		
		Servicios [S]					50		
	Destrucción de información [A14]	Datos [D]	MB	0.002				100	
		Servicios [S]						100	
	Divulgación de información [A15]	Personal [P]	M	0.016		20			
		Datos [D]				100			

	Manipulación de software [A16]	Software [SW]	MB	0.002			75	75	
	Manipulación de equipos [A17]	Hardware [HW]	MB	0.002		50		50	
		Equipamiento auxiliar [AUX]				50		50	
		Software [SW]				50		50	
	Denegación de servicio [A18]	Software [SW]	B	0.005				100	
		Servicio VoIP [COM1]						100	
		Servicio Internet [COM2]						100	
		Red inalámbrica [COM3]						100	
		Servicios [S]						100	
	Robo [A19]	Hardware [HW]	MB	0.002		20		100	
		Equipamiento auxiliar [AUX]				20		100	
		Datos [D]				100		100	
		Red [COM]				75		100	
		Servicios [S]				50		100	
	Ataque destructivo [A20]	Instalaciones [I]	MB	0.002				100	
		Hardware [HW]						100	
		Equipamiento auxiliar [AUX]						100	
		Datos [D]						100	
		Red [COM]						100	
		Servicios [S]						100	
	Ocupación enemiga [A21]	Instalaciones [I]	MB	0.002		50		100	
		Hardware [HW]				50		100	
		Equipamiento auxiliar [AUX]				50		100	
		Datos [D]				100		100	
		Red [COM]				50		100	
		Servicios [S]				50		100	
	Indisponibilidad del personal [A22]	Personal [P]	A	0.071				100	
	Extorsión [A23]	Personal [P]	MB	0.002		20	20	20	
	Ingeniería social [A24]	Personal [P]	MB	0.002		20	20	20	

Tabla 19. Análisis de amenazas

A continuación se muestra en la Tabla 20 resumen del impacto máximo de las amenazas sobre las distintas dimensiones de los activos.

Activos		**Impacto**				
		A	**C**	**I**	**D**	**T**
Instalaciones [I]			75%	50%	100%	
Hardware [HW]			75%	50%	100%	
Software [SW]		75%	100%	75%	100%	
Datos [D]		100%	100%	100%	100%	75%
Red [COM]	COM1		75%		100%	
	COM2					
	COM3	75%		50%		
	COM4					
	COM5	75%		50%		
Servicios [S]		75%	75%	50%	100%	75%
Equipamiento auxiliar [AUX]			50%	50%	100%	
Personal [P]			20%	20%	100%	

Tabla 20. Impacto máximo sobre las dimensiones de los activos

3.7. Impacto potencial

Una vez realizado el inventario y la valoración de los activos así como el análisis de las posibles amenazas, se tienen todos los datos necesarios para calcular el impacto potencial que puede suponer para CEINTECO la materialización de las amenazas encontradas. Este impacto potencial permitirá a la organización priorizar el plan de acción y, a su vez, evaluar cómo se verá modificado este valor una vez se apliquen las contramedidas oportunas.

El impacto potencial se calcula siguiendo la siguiente fórmula:

Impacto potencial = Valor del activo * Valor del impacto de la amenaza

Aplicando esta fórmula a los datos que ya tenemos de las tablas anteriores obtenemos los datos que se muestran en la Tabla 21.

Activo	Valoración					Impacto					Impacto potencial				
	A	C	I	D	T	A	C	I	D	T	A	C	I	D	T
[L1] Pasillo administración y despachos dirección	8	0	0	8	5						0	0	0	8	0
[L2] Pasillo grupo investigación	8	0	0	8	0						0	0	0	8	0
[L3] Pasillo grupo investigación 2	8	0	0	8	0						0	0	0	8	0
[L4] Pasillo grupo investigación 3	8	0	0	8	0						0	0	0	8	0
[L5] Pasillo grupo investigación 4	8	0	0	8	0						0	0	0	8	0
[L6] Sala 1.1	8	1	0	8	2						0	0,75	0	8	0
[L7] Sala 1.2	8	1	0	8	2						0	0,75	0	8	0
[L8] Sala 2.1	8	1	0	8	2						0	0,75	0	8	0
[L9] Sala 2.2	8	1	0	8	2						0	0,75	0	8	0
[L10] Sala 3.1	8	1	0	8	2						0	0,75	0	8	0
[L11] Sala 3.2	8	1	0	8	2						0	0,75	0	8	0
[L12] Sala 4.1	8	1	0	8	2						0	0,75	0	8	0
[L13] Sala 4.2	8	1	0	8	2						0	0,75	0	8	0
[L14] Oficina jefe grupo 1	6	1	0	5	2		75%	50%	100%		0	0,75	0	5	0
[L15] Oficina jefe grupo 2	6	1	0	5	2						0	0,75	0	5	0
[L16] Oficina jefe grupo 3	6	1	0	5	2						0	0,75	0	5	0
[L17] Oficina jefe grupo 4	6	1	0	5	2						0	0,75	0	5	0
[L18] Laboratorio 1	8	2	0	8	5						0	1,5	0	8	0
[L19] Laboratorio 2	8	2	0	8	5						0	1,5	0	8	0
[L20] Laboratorio 3	8	2	0	8	5						0	1,5	0	8	0
[L21] Laboratorio 4	8	2	0	8	5						0	1,5	0	8	0
[L22] Sala Servidores 1	8	5	0	8	7						0	3,75	0	8	0
[L23] Sala Servidores 2	8	5	0	8	7						0	3,75	0	8	0
[L24] Despacho director	6	2	0	5	5						0	1,5	0	5	0
[L25] Despacho subdirector general	6	2	0	5	5						0	1,5	0	5	0
[L26] Despacho subdirector investigación	6	2	0	5	5						0	1,5	0	5	0

[L27] Despacho secretario	6	2	0	5	5						0	1,5	0	5	0
[L28]Sala copias de seguridad	8	5	0	8	7						0	3,75	0	8	0
[L29] Sala servidores globales	8	5	0	8	7						0	3,75	0	8	0
[HW1] Servidor correo	8	8	8	8	7						0	6	4	8	0
[HW2] Servidor web	8	4	6	5	7						0	3	3	5	0
[HW3] Servidor BBDD huellas	8	8	9	9	7						0	6	4,5	9	0
[HW4] Servidores repositorio código (2)	8	8	8	8	7						0	6	4	8	0
[HW5] Equipos copias seguridad (2)	8	8	8	7	7						0	6	4	7	0
[HW6] Ordenadores simulación (10)	7	8	9	9	7						0	6	4,5	9	0
[HW7] F irewall (2)	8	8	7	6	8						0	6	3,5	6	0
[HW8] Impresoras de red (5)	7	8	0	3	4		75%	50%	100%		0	6	0	3	0
[HW9] Teléfonos IP (85)	6	7	7	4	6						0	5,25	3,5	4	0
[HW10] Portátiles	8	9	8	9	8						0	6,75	4	9	0
[HW11] PCs personal investigación	8	9	8	9	8						0	6,75	4	9	0
[HW12] PCs administración	9	9	9	9	9						0	6,75	4,5	9	0
[HW13] Punto acceso Wi-Fi	7	7	8	5	8						0	5,25	4	5	0
[HW14] Escáner huellas (7)	8	3	7	9	8						0	2,25	3,5	9	0
[SW1] S.O. Windows 7 Professional	8	7	7	9	6						6	7	5,25	9	0
[SW2] S.O. Ubuntu	8	7	8	9	6						6	7	6	9	0
[SW3] Microsoft Windows Server 2008	8	7	9	9	8						6	7	6,75	9	0
[SW4] Microsoft Office 2013	6	6	7	5	6						4,5	6	5,25	5	0
[SW5] Microsoft Visual Studio	7	6	8	8	7						5,25	6	6	8	0
[SW6] Matlab	7	6	8	8	7						5,25	6	6	8	0
[SW7] Adobe Acrobat Professional	5	6	7	3	7		75%	100%	75%	100%	3,75	6	5,25	3	0
[SW8] LaTeX	5	6	7	6	7						3,75	6	5,25	6	0
[SW9] Antivirus	7	8	9	9	7						5,25	8	6,75	9	0
[SW10] Aplicaciones internas administración	9	9	9	9	8						6,75	9	6,75	9	0
[SW11] Aplicación gestión copias de seguridad	8	8	9	9	8						6	8	6,75	9	0

[D1] Base de datos de huellas	9	9	9	9	8	100%	100%	100%	100%	75%	9	9	9	9	6
[D2] Datos de los trabajadores	8	9	7	7	8						8	9	7	7	6
[D3] Datos de los clientes	9	10	8	8	8						9	10	8	8	6
[D4] Información del acceso de visitas	3	2	2	1	2						3	2	2	1	1,5
[D5] Copias seguridad servidores	8	8	9	9	8						8	8	9	9	6
[D6] Código fuente desarrollos	9	10	10	10	9						9	10	10	10	6,75
[D7] Datos de investigaciones y experimentos	8	10	9	9	8						8	10	9	9	6
[COM1] Cableado eléctrico	0	0	0	9	0						0	0	0	9	0
[COM2] Cableado telecomunicaciones	0	0	0	9	0						0	0	0	9	0
[COM3] Servicio VoIP	8	8	5	5	7	75%	75%	50%	100%		6	6	2,5	7	0
[COM4] Servicio Internet	8	8	8	8	7						0	6	0	8	0
[COM5] Red inalámbrica	8	8	8	3	7	75%		50%			6	6	4	3	0
[S1] Correo electrónico	8	9	8	8	7	75%	75%	50%	100%	100%	6	6,75	4	8	7
[S2] Acceso remoto	8	8	7	6	7						6	6	3,5	6	7
[S3] Página web	4	4	8	6	6						3	3	4	6	6
[AUX1] Sistema de climatización	0	0	0	9	0	50%	50%	50%	100%		0	0	0	9	0
[AUX2] Sistema detección incendios	0	0	0	9	0						0	0	0	9	0
[AUX3] Sistema de alimentación ininterrumpido (SAI)	0	0	0	9	0						0	0	0	9	0
[AUX4] Extintores (5)	0	0	0	9	0						0	0	0	9	0
[AUX5] Televisión	0	0	0	2	0						0	0	0	2	0
[AUX6] Generador de señales IQ (2)	0	0	0	3	0						0	0	0	3	0
[AUX7] Analizador de espectro	0	0	0	3	0						0	0	0	3	0
[AUX8] Femtocelda LTE	0	0	0	3	0						0	0	0	3	0
[AUX9] Receptor de señales IQ (2)	0	0	0	3	0						0	0	0	3	0
[AUX10] Analizador de red vectorial (2)	0	0	0	3	0						0	0	0	3	0
[AUX11] Conversor de frecuencia	0	0	0	3	0						0	0	0	3	0
[AUX12] Fuente de radiofrecuencia	0	0	0	3	0						0	0	0	3	0

[AUX13] Analizador de espectro óptico	0	0	0	3	0						0	0	0	3	0
[AUX14] Osciloscopio (3)	0	0	0	3	0						0	0	0	3	0
[AUX15] Equipamiento radiodifusión	0	0	0	3	0						0	0	0	3	0
[AUX16] Terminales móviles (3)	8	7	7	3	4						0	3,5	3,5	3	0
[AUX17] Altavoces (10)	0	0	0	3	0						0	0	0	3	0
[AUX18] Micrófonos (10)	0	0	0	3	0						0	0	0	3	0
[AUX19] Analizador de audio	0	0	0	3	0						0	0	0	3	0
[AUX20] Destructor papeles	0	0	0	1	0						0	0	0	1	0
[P1] Director general	0	0	0	9	0						0	0	0	9	0
[P2] Subdirector general	0	0	0	8	0						0	0	0	8	0
[P3] Subdirector investigación	0	0	0	8	0						0	0	0	8	0
[P4] Secretario	0	0	0	7	0						0	0	0	7	0
[P5] Personal administración	0	0	0	8	0						0	0	0	8	0
[P6] Responsable Seguridad	0	0	0	8	0		20%	20%	100%		0	0	0	8	0
[P7] Técnico centro investigación	0	0	0	8	0						0	0	0	8	0
[P8] Técnicos de grupo	0	0	0	7	0						0	0	0	7	0
[P9] Jefes de grupo	0	0	0	7	0						0	0	0	7	0
[P10] Personal de investigación	0	0	0	8	0						0	0	0	8	0

Tabla 21. Tabla de impacto potencial

3.8. Nivel de riesgo aceptable y riesgo residual

Por último, teniendo definidos todos los datos calculados en los apartados anteriores y sabiendo que los riesgos no pueden eliminarse por completo, es necesario definir un límite a partir del cual podamos decidir si asumir un riesgo o no para cada uno de los activos.

Por una parte, se debe establecer el riesgo aceptable, es decir, el nivel de riesgo a partir del cual la organización considera una amenaza importante y debe aplicar controles para reducirlo.

Una vez establecidos los controles el riesgo de cada activo se verá reducido, pero seguirá existiendo en un nivel menor que antes. A este riesgo que permanece después de aplicar los controles de seguridad se le denomina riesgo residual.

Para calcular el riesgo de cada uno de los activos se va a utilizar la siguiente fórmula:

Riesgo = Impacto potencial * Frecuencia

En la Tabla 22 se muestran las escalas que se van a utilizar para medir el impacto, la frecuencia y el riesgo.

Escalas		
Impacto	**Frecuencia**	**Riesgo**
MA: Muy alto	**MA**: Prácticamente seguro	**MA**: Crítico
A: Alto	**A**: Probable	**A**: Importante
M: Medio	**M**: Posible	**M**: Apreciable
B: Bajo	**B**: Poco probable	**B**: Bajo
MB: Muy bajo	**MB**: Muy raro	**MB**: Despreciable

Tabla 22. Escalas de evaluación de impacto, frecuencia y riesgo

El impacto y la frecuencia se combinan en la Tabla 23 para calcular el riesgo.

Riesgo		**Frecuencia**				
		MB (0,002)	**B (0,005)**	**M (0,016)**	**A (0,071)**	**MA (1)**
Impacto	**MA (10)**	A	MA	MA	MA	MA
	A (7-9)	M	A	A	MA	MA
	M (4-6)	B	M	M	A	A
	B (2-3)	MB	B	B	M	M
	MB (1)	MB	MB	MB	B	B

Tabla 23. Escala de evaluación de riesgos

En la Tabla 24 se muestra el análisis del nivel de riesgo de CEINTECO.

Activo	**Frecuencia**		**Impacto potencial**					**Riesgo**				
	Frec.	**Valor**	**A**	**C**	**I**	**D**	**T**	**A**	**C**	**I**	**D**	**T**
[L1] Pasillo administración y despachos dirección			0	0	0	8	0	0	0	0	0,128	0
[L2] Pasillo grupo investigación			0	0	0	8	0	0	0	0	0,128	0
[L3] Pasillo grupo investigación 2			0	0	0	8	0	0	0	0	0,128	0
[L4] Pasillo grupo investigación 3			0	0	0	8	0	0	0	0	0,128	0
[L5] Pasillo grupo investigación 4			0	0	0	8	0	0	0	0	0,128	0
[L6] Sala 1.1			0	0,75	0	8	0	0	0,012	0	0,128	0

[L7] Sala 1.2	M	0,016	0	0,75	0	8	0	0	0,012	0	0,128	0
[L8] Sala 2.1			0	0,75	0	8	0	0	0,012	0	0,128	0
[L9] Sala 2.2			0	0,75	0	8	0	0	0,012	0	0,128	0
[L10] Sala 3.1			0	0,75	0	8	0	0	0,012	0	0,128	0
[L11] Sala 3.2			0	0,75	0	8	0	0	0,012	0	0,128	0
[L12] Sala 4.1			0	0,75	0	8	0	0	0,012	0	0,128	0
[L13] Sala 4.2			0	0,75	0	8	0	0	0,012	0	0,128	0
[L14] Oficina jefe grupo 1			0	0,75	0	5	0	0	0,012	0	0,08	0
[L15] Oficina jefe grupo 2			0	0,75	0	5	0	0	0,012	0	0,08	0
[L16] Oficina jefe grupo 3			0	0,75	0	5	0	0	0,012	0	0,08	0
[L17] Oficina jefe grupo 4			0	0,75	0	5	0	0	0,012	0	0,08	0
[L18] Laboratorio 1			0	1,5	0	8	0	0	0,024	0	0,128	0
[L19] Laboratorio 2			0	1,5	0	8	0	0	0,024	0	0,128	0
[L20] Laboratorio 3			0	1,5	0	8	0	0	0,024	0	0,128	0
[L21] Laboratorio 4			0	1,5	0	8	0	0	0,024	0	0,128	0
[L22] Sala Servidores 1			0	3,75	0	8	0	0	0,06	0	0,128	0
[L23] Sala Servidores 2			0	3,75	0	8	0	0	0,06	0	0,128	0
[L24] Despacho director			0	1,5	0	5	0	0	0,024	0	0,08	0
[L25] Despacho subdirector general			0	1,5	0	5	0	0	0,024	0	0,08	0
[L26] Despacho subdirector investigación			0	1,5	0	5	0	0	0,024	0	0,08	0
[L27] Despacho secretario			0	1,5	0	5	0	0	0,024	0	0,08	0
[L28]Sala copias de seguridad			0	3,75	0	8	0	0	0,06	0	0,128	0
[L29] Sala servidores globales			0	3,75	0	8	0	0	0,06	0	0,128	0
[HW1] Servidor correo			0	6	4	8	0	0	0,096	0,064	0,128	0
[HW2] Servidor web			0	3	3	5	0	0	0,048	0,048	0,08	0
[HW3] Servidor BBDD huellas			0	6	4,5	9	0	0	0,096	0,072	0,144	0
[HW4] Servidores repositorio código (2)			0	6	4	8	0	0	0,096	0,064	0,128	0
[HW5] Equipos copias seguridad (2)			0	6	4	7	0	0	0,096	0,064	0,112	0

[HW6] Ordenadores simulación (10)	M	0,016	0	6	4,5	9	0	0	0,096	0,072	0,144	0
[HW7] F irewall (2)			0	6	3,5	6	0	0	0,096	0,056	0,096	0
[HW8] Impresoras de red (5)			0	6	0	3	0	0	0,096	0	0,048	0
[HW9] Teléfonos IP (85)			0	5,25	3,5	4	0	0	0,084	0,056	0,064	0
[HW10] Portátiles			0	6,75	4	9	0	0	0,108	0,064	0,144	0
[HW11] PCs personal investigación			0	6,75	4	9	0	0	0,108	0,064	0,144	0
[HW12] PCs administración			0	6,75	4,5	9	0	0	0,108	0,072	0,144	0
[HW13] Punto acceso Wi-Fi			0	5,25	4	5	0	0	0,084	0,064	0,08	0
[HW14] Escáner huellas (7)			0	2,25	3,5	9	0	0	0,036	0,056	0,144	0
[SW1] S.O. Windows 7 Professional	M	0,016	6	7	5,25	9	0	0,096	0,112	0,084	0,144	0
[SW2] S.O. Ubuntu			6	7	6	9	0	0,096	0,112	0,096	0,144	0
[SW3] Microsoft Windows Server 2008			6	7	6,75	9	0	0,096	0,112	0,108	0,144	0
[SW4] Microsoft Office 2013			4,5	6	5,25	5	0	0,072	0,096	0,084	0,08	0
[SW5] Microsoft Visual Studio			5,25	6	6	8	0	0,084	0,096	0,096	0,128	0
[SW6] Matlab			5,25	6	6	8	0	0,084	0,096	0,096	0,128	0
[SW7] Adobe Acrobat Professional			3,75	6	5,25	3	0	0,016	0,096	0,084	0,048	0
[SW8] LaTeX			3,75	6	5,25	6	0	0,016	0,096	0,084	0,096	0
[SW9] Antivirus			5,25	8	6,75	9	0	0,084	0,128	0,108	0,144	0
[SW10] Aplicaciones internas administración			6,75	9	6,75	9	0	0,108	0,144	0,108	0,144	0
[SW11] Aplicación gestión copias de seguridad			6	8	6,75	9	0	0,096	0,128	0,108	0,144	0
[D1] Base de datos de huellas	M	0,016	9	9	9	9	6	0,144	0,144	0,144	0,144	0,096
[D2] Datos de los trabajadores			8	9	7	7	6	0,128	0,144	0,112	0,112	0,096
[D3] Datos de los clientes			9	10	8	8	6	0,144	0,16	0,128	0,128	0,096
[D4] Información del acceso de visitas			3	2	2	1	1,5	0,048	0,032	0,032	0,016	0,024
[D5] Copias seguridad servidores			8	8	9	9	6	0,128	0,128	0,144	0,144	0,096
[D6] Código fuente desarrollos			9	10	10	10	6,75	0,144	0,16	0,16	0,16	0,108
[D7] Datos de investigaciones y experimentos			8	10	9	9	6	0,128	0,16	0,144	0,144	0,096
[COM1] Cableado eléctrico	B	0,005	0	0	0	9	0	0	0	0	0,045	0

[COM2] Cableado telecomunicaciones	MB	0,002	0	0	0	9	0	0	0	0	0,018	0
[COM3] Servicio VoIP	M	0,016	6	6	2,5	7	0	0,096	0,096	0,04	0,112	0
[COM4] Servicio Internet			0	6	0	8	0	0	0,096	0	0,128	0
[COM5] Red inalámbrica			6	6	4	3	0	0,096	0,096	0,064	0,048	0
[S1] Correo electrónico	M	0,016	6	6,75	4	8	7	0,096	0,108	0,064	0,128	0,112
[S2] Acceso remoto			6	6	3,5	6	7	0,096	0,096	0,056	0,096	0,112
[S3] Página web			3	3	4	6	6	0,048	0,048	0,064	0,096	0,096
[AUX1] Sistema de climatización	M	0,016	0	0	0	9	0	0	0	0	0,144	0
[AUX2] Sistema detección incendios			0	0	0	9	0	0	0	0	0,144	0
[AUX3] Sistema de alimentación ininterrumpido (SAI)			0	0	0	9	0	0	0	0	0,144	0
[AUX4] Extintores (5)			0	0	0	9	0	0	0	0	0,144	0
[AUX5] Televisión			0	0	0	2	0	0	0	0	0,032	0
[AUX6] Generador de señales IQ (2)			0	0	0	3	0	0	0	0	0,048	0
[AUX7] Analizador de espectro			0	0	0	3	0	0	0	0	0,048	0
[AUX8] Femtocelda LTE			0	0	0	3	0	0	0	0	0,048	0
[AUX9] Receptor de señales IQ (2)			0	0	0	3	0	0	0	0	0,048	0
[AUX10] Analizador de red vectorial (2)			0	0	0	3	0	0	0	0	0,048	0
[AUX11] Conversor de frecuencia			0	0	0	3	0	0	0	0	0,048	0
[AUX12] Fuente de radiofrecuencia			0	0	0	3	0	0	0	0	0,048	0
[AUX13] Analizador de espectro óptico			0	0	0	3	0	0	0	0	0,048	0
[AUX14] Osciloscopio (3)			0	0	0	3	0	0	0	0	0,048	0
[AUX15] Equipamiento radiodifusión			0	0	0	3	0	0	0	0	0,048	0
[AUX16] Terminales móviles (3)			0	3,5	3,5	3	0	0	0,056	0,056	0,048	0
[AUX17] Altavoces (10)			0	0	0	3	0	0	0	0	0,048	0
[AUX18] Micrófonos (10)			0	0	0	3	0	0	0	0	0,048	0
[AUX19] Analizador de audio			0	0	0	3	0	0	0	0	0,048	0
[AUX20] Destructor papeles			0	0	0	1	0	0	0	0	0,016	0
[P1] Director general			0	0	0	9	0	0	0	0	0,144	0

[P2] Subdirector general	A	0,071	0	0	0	8	0	0	0	0	0,128	0
[P3] Subdirector investigación			0	0	0	8	0	0	0	0	0,128	0
[P4] Secretario			0	0	0	7	0	0	0	0	0,112	0
[P5] Personal administración			0	0	0	8	0	0	0	0	0,128	0
[P6] Responsable Seguridad			0	0	0	8	0	0	0	0	0,128	0
[P7] Técnico centro investigación			0	0	0	8	0	0	0	0	0,128	0
[P8] Técnicos de grupo			0	0	0	7	0	0	0	0	0,112	0
[P9] Jefes de grupo			0	0	0	7	0	0	0	0	0,112	0
[P10] Personal de investigación			0	0	0	8	0	0	0	0	0,128	0

Tabla 24. Análisis del nivel de riesgo

Tras este análisis del nivel de riesgo la Dirección de CEINTECO ha tomado la decisión de establecer el nivel de riesgo aceptable en medio. Esto quiere decir que todos los activos cuyo riesgo sea medio o esté por debajo de este nivel no supondrán una amenaza importante para la organización. Sin embargo, si el nivel de riesgo de un activo es alto o muy alto se considera una amenaza y, por tanto, hay que establecer controles para reducirlo.

A continuación se muestra en la Tabla 25 los activos cuyo riesgo supera el aceptable y, por tanto, para los que habrá que establecer controles para reducir su riesgo.

Activo	**Riesgo**				
	A	**C**	**I**	**D**	**T**
[L1] Pasillo administración y despachos dirección	0	0	0	0,128	0
[L2] Pasillo grupo investigación	0	0	0	0,128	0
[L3] Pasillo grupo investigación 2	0	0	0	0,128	0
[L4] Pasillo grupo investigación 3	0	0	0	0,128	0
[L5] Pasillo grupo investigación 4	0	0	0	0,128	0
[L6] Sala 1.1	0	0,012	0	0,128	0
[L7] Sala 1.2	0	0,012	0	0,128	0
[L8] Sala 2.1	0	0,012	0	0,128	0
[L9] Sala 2.2	0	0,012	0	0,128	0
[L10] Sala 3.1	0	0,012	0	0,128	0
[L11] Sala 3.2	0	0,012	0	0,128	0
[L12] Sala 4.1	0	0,012	0	0,128	0
[L13] Sala 4.2	0	0,012	0	0,128	0

[L18] Laboratorio 1	0	0,024	0	0,128	0
[L19] Laboratorio 2	0	0,024	0	0,128	0
[L20] Laboratorio 3	0	0,024	0	0,128	0
[L21] Laboratorio 4	0	0,024	0	0,128	0
[L22] Sala Servidores 1	0	0,06	0	0,128	0
[L23] Sala Servidores 2	0	0,06	0	0,128	0
[L28]Sala copias de seguridad	0	0,06	0	0,128	0
[L29] Sala servidores globales	0	0,06	0	0,128	0
[HW1] Servidor correo	0	0,096	0,064	0,128	0
[HW3] Servidor BBDD huellas	0	0,096	0,072	0,144	0
[HW4] Servidores repositorio código (2)	0	0,096	0,064	0,128	0
[HW5] Equipos copias seguridad (2)	0	0,096	0,064	0,112	0
[HW6] Ordenadores simulación (10)	0	0,096	0,072	0,144	0
[HW10] Portátiles	0	0,108	0,064	0,144	0
[HW11] PCs personal investigación	0	0,108	0,064	0,144	0
[HW12] PCs administración	0	0,108	0,072	0,144	0
[HW14] Escáner huellas (7)	0	0,036	0,056	0,144	0
[SW1] S.O. Windows 7 Professional	0,096	0,112	0,084	0,144	0
[SW2] S.O. Ubuntu	0,096	0,112	0,096	0,144	0
[SW3] Microsoft Windows Server 2008	0,096	0,112	0,108	0,144	0
[SW5] Microsoft Visual Studio	0,084	0,096	0,096	0,128	0
[SW6] Matlab	0,084	0,096	0,096	0,128	0
[SW9] Antivirus	0,084	0,128	0,108	0,144	0
[SW10] Aplicaciones internas administración	0,108	0,144	0,108	0,144	0
[SW11] Aplicación gestión copias de seguridad	0,096	0,128	0,108	0,144	0
[D1] Base de datos de huellas	0,144	0,144	0,144	0,144	0,096
[D2] Datos de los trabajadores	0,128	0,144	0,112	0,112	0,096
[D3] Datos de los clientes	0,144	0,16	0,128	0,128	0,096
[D5] Copias seguridad servidores	0,128	0,128	0,144	0,144	0,096
[D6] Código fuente desarrollos	0,144	0,16	0,16	0,16	0,108
[D7] Datos de investigaciones y experimentos	0,128	0,16	0,144	0,144	0,096
[COM3] Servicio VoIP	0,096	0,096	0,04	0,112	0

[COM4] Servicio Internet	0	0,096	0	0,128	0
[S1] Correo electrónico	0,096	0,108	0,064	0,128	0,112
[S2] Acceso remoto	0,096	0,096	0,056	0,096	0,112
[AUX1] Sistema de climatización	0	0	0	0,144	0
[AUX2] Sistema detección incendios	0	0	0	0,144	0
[AUX3] Sistema de alimentación ininterrumpido (SAI)	0	0	0	0,144	0
[AUX4] Extintores (5)	0	0	0	0,144	0
[P1] Director general	0	0	0	0,144	0
[P2] Subdirector general	0	0	0	0,128	0
[P3] Subdirector investigación	0	0	0	0,128	0
[P4] Secretario	0	0	0	0,112	0
[P5] Personal administración	0	0	0	0,128	0
[P6] Responsable Seguridad	0	0	0	0,128	0
[P7] Técnico centro investigación	0	0	0	0,128	0
[P8] Técnicos de grupo	0	0	0	0,112	0
[P9] Jefes de grupo	0	0	0	0,112	0
[P10] Personal de investigación	0	0	0	0,128	0

Tabla 25. Activos que superan el riesgo aceptable

Como se puede observar, muchos de los activos de CEINTECO tienen un nivel de riesgo alto o superior y habrá que reducir el nivel de riesgo de cada uno de ellos.

Puesto que no se va a poder reducir el nivel de riesgo de todos los activos a la vez se va a llevar a cabo una priorización y se reducirá primero el riesgo de los activos más prioritarios.

Los activos más prioritarios serán aquellos que tengan el mayor nivel de riesgo y en más dimensiones. Por tanto, el activo más prioritario al que habrá que reducir el riesgo es el código fuente de los desarrollos, seguido de los datos de los clientes y los datos de las investigaciones y experimentos, ya que todos ellos tienen un nivel muy alto de riesgo en alguna, o varias, de sus dimensiones de seguridad.

Los siguientes activos a reducir el nivel de riesgo serán los que tengan un mayor número de dimensiones con nivel de riesgo alto. De estos, serán más prioritarios aquellos que, además de nivel de riesgo alto en alguna dimensión, tengan nivel de riesgo medio en otra dimensión.

Los que menor prioridad tendrán serán aquellos que únicamente tengan una dimensión de seguridad con nivel de riesgo alto y el resto de dimensiones sin riesgos.

A continuación se muestran en la Tabla 26 los activos que superan el riesgo aceptable ordenados por orden de prioridad.

Activo	Riesgo				
	A	C	I	D	T
[D6] Código fuente desarrollos	0,144	0,16	0,16	0,16	0,108
[D3] Datos de los clientes	0,144	0,16	0,128	0,128	0,096
[D7] Datos de investigaciones y experimentos	0,128	0,16	0,144	0,144	0,096
[D1] Base de datos de huellas	0,144	0,144	0,144	0,144	0,096
[D5] Copias seguridad servidores	0,128	0,128	0,144	0,144	0,096
[D2] Datos de los trabajadores	0,128	0,144	0,112	0,112	0,096
[SW10] Aplicaciones internas administración	0,108	0,144	0,108	0,144	0
[SW9] Antivirus	0,084	0,128	0,108	0,144	0
[S1] Correo electrónico	0,096	0,108	0,064	0,128	0,112
[SW11] Aplicación gestión copias de seguridad	0,096	0,128	0,108	0,144	0
[SW1] S.O. Windows 7 Professional	0,096	0,112	0,084	0,144	0
[SW2] S.O. Ubuntu	0,096	0,112	0,096	0,144	0
[SW3] Microsoft Windows Server 2008	0,096	0,112	0,108	0,144	0
[SW5] Microsoft Visual Studio	0,084	0,096	0,096	0,128	0
[SW6] Matlab	0,084	0,096	0,096	0,128	0
[S2] Acceso remoto	0,096	0,096	0,056	0,096	0,112
[HW3] Servidor BBDD huellas	0	0,096	0,072	0,144	0
[HW6] Ordenadores simulación (10)	0	0,096	0,072	0,144	0
[HW10] Portátiles	0	0,108	0,064	0,144	0
[HW11] PCs personal investigación	0	0,108	0,064	0,144	0
[HW12] PCs administración	0	0,108	0,072	0,144	0
[HW1] Servidor correo	0	0,096	0,064	0,128	0
[HW4] Servidores repositorio código (2)	0	0,096	0,064	0,128	0
[HW5] Equipos copias seguridad (2)	0	0,096	0,064	0,112	0
[COM3] Servicio VoIP	0,096	0,096	0,04	0,112	0
[COM4] Servicio Internet	0	0,096	0	0,128	0
[HW14] Escáner huellas (7)	0	0,036	0,056	0,144	0
[L22] Sala Servidores 1	0	0,06	0	0,128	0
[L23] Sala Servidores 2	0	0,06	0	0,128	0
[L28]Sala copias de seguridad	0	0,06	0	0,128	0
[L29] Sala servidores globales	0	0,06	0	0,128	0
[L6] Sala 1.1	0	0,012	0	0,128	0
[L7] Sala 1.2	0	0,012	0	0,128	0
[L8] Sala 2.1	0	0,012	0	0,128	0
[L9] Sala 2.2	0	0,012	0	0,128	0

[L10] Sala 3.1	0	0,012	0	0,128	0
[L11] Sala 3.2	0	0,012	0	0,128	0
[L12] Sala 4.1	0	0,012	0	0,128	0
[L13] Sala 4.2	0	0,012	0	0,128	0
[L18] Laboratorio 1	0	0,024	0	0,128	0
[L19] Laboratorio 2	0	0,024	0	0,128	0
[L20] Laboratorio 3	0	0,024	0	0,128	0
[L21] Laboratorio 4	0	0,024	0	0,128	0
[AUX1] Sistema de climatización	0	0	0	0,144	0
[AUX2] Sistema detección incendios	0	0	0	0,144	0
[AUX3] Sistema de alimentación ininterrumpido (SAI)	0	0	0	0,144	0
[AUX4] Extintores (5)	0	0	0	0,144	0
[P1] Director general	0	0	0	0,144	0
[L1] Pasillo administración y despachos dirección	0	0	0	0,128	0
[L2] Pasillo grupo investigación	0	0	0	0,128	0
[L3] Pasillo grupo investigación 2	0	0	0	0,128	0
[L4] Pasillo grupo investigación 3	0	0	0	0,128	0
[L5] Pasillo grupo investigación 4	0	0	0	0,128	0
[P2] Subdirector general	0	0	0	0,128	0
[P3] Subdirector investigación	0	0	0	0,128	0
[P4] Secretario	0	0	0	0,112	0
[P5] Personal administración	0	0	0	0,128	0
[P6] Responsable Seguridad	0	0	0	0,128	0
[P10] Personal de investigación	0	0	0	0,128	0
[P7] Técnico centro investigación	0	0	0	0,128	0
[P8] Técnicos de grupo	0	0	0	0,112	0
[P9] Jefes de grupo	0	0	0	0,112	0

Tabla 26. Activos con nivel de riesgo superior al aceptable por orden de prioridad

4. Fase 4: Propuesta de proyectos

4.1. Introducción

Tras haber realizado el análisis de riesgos de CEINTECO donde se han identificado los activos de la organización, las posibles amenazas, el impacto que tendría la ocurrencia de dichas amenazas sobre los activos y el nivel de riesgo de cada uno de los activos, disponemos de una visión más amplia y exacta del estado de la seguridad de la información de la empresa.

En esta fase se van a plantear diferentes proyectos con el objetivo de reducir el nivel riesgo actual de CEINTECO y con ello mejorar el estado de la seguridad de la organización.

Las proyectos que se van a plantear son los resultantes de agrupar un conjunto de recomendaciones identificadas en la fase de análisis de riesgos para facilitar su ejecución. Se va incidir en la mejora en relación con la gestión de la seguridad así como en posibles beneficios colaterales como la optimización de recursos o la mejora en la gestión de procesos y tecnologías presentes en CEINTECO.

En el siguiente apartado se presentan los diferentes proyectos con los que se espera mejorar el estado de la seguridad de la organización.

4.2. Propuestas

PROYECTO-01: MEJORA DE LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	
Objetivo	Mejora de la versión actual de la política de seguridad de la información de CEINTECO.
Descripción	Se va a realizar una revisión de la política de la seguridad de la información de CEINTECO en busca de puntos de mejora y puntos que puedan faltar para conseguir un mayor nivel de seguridad en la organización. El equipo de dirección de la organización deberá aprobar esta nueva versión de la política de seguridad y ponerla en conocimiento de todos los empleados de CEINTECO. Este proyecto se llevará a cabo al menos una vez al año durante toda la vida de la empresa para asegurar una mejora continua de la política de seguridad.
Activos cuyo riesgo se verá reducido	Instalaciones [L]: todos los activos Hardware [HW]: todos los activos Aplicación [SW]: todos los activos Datos [D]: todos los activos Red [COM]: todos los activos Servicios [S]: todos los activos Equipamiento auxiliar [AUX]: todos los activos
Dimensiones de seguridad cuyo riesgo se verá reducido	Confidencialidad [C] Integridad [I] Disponibilidad [D]
Responsable	Responsable de seguridad.
Controles	A.5
Indicadores	[IN1] Política de seguridad.
Coste	Horas de dedicación del responsable de seguridad. Horas de dedicación del Comité de Seguridad. Horas de dedicación del equipo de dirección. 3000€.
Duración	3 semanas.

Tabla 27. Proyecto-01: Mejora de la política de seguridad de la información.

PROYECTO-02: FORMACIÓN CONTINUA EN SEGURIDAD	
Objetivo	Concienciar a los empleados de CEINTECO en materia de seguridad de la información.
Descripción	Se va a establecer un calendario de formación en el que se impartirá un curso básico de seguridad de la información a todos los empleados de CEINTECO. El curso tiene como objetivo dar a conocer los principios básicos de seguridad de la información en general para cualquier organización así como las normas de seguridad a aplicar en CEINTECO en particular. El curso lo impartirá el responsable de seguridad y el aforo está limitado a 10 personas, de ahí la necesidad de establecer un calendario para que todo el personal de la organización acuda al curso. Cada año se establecerá un nuevo calendario de formación en materia de seguridad.
Activos cuyo riesgo se verá reducido	Instalaciones [L]: todos los activos Hardware [HW]: todos los activos Aplicación [SW]: todos los activos Datos [D]: todos los activos Red [COM]: todos los activos Servicios [S]: todos los activos Equipamiento auxiliar [AUX]: todos los activos Personal [P]: todos los activos
Dimensiones de seguridad cuyo riesgo se verá reducido	Confidencialidad [C] Integridad [I] Disponibilidad [D]
Responsable	Responsable de seguridad.
Controles	A.7.2.2
Indicadores	[IN4] Formación.
Coste	Horas de dedicación del responsable de seguridad a preparar la formación y a darla a los empleados. Horas de los empleados que están en el curso de formación y no produciendo. 1500€.
Duración	4 semanas en las que se impartirán 2 cursos de 3h cada semana .

Tabla 28. Proyecto-02: Formación continua en seguridad

PROYECTO-03: PLAN DE CONTINUIDAD DE NEGOCIO	
Objetivo	Definir un plan de actuación para proteger los procesos y actividades críticas de CEINTECO de desastres y garantizar el restablecimiento del funcionamiento normal de la organización en un plazo aceptable.
Descripción	Se va a establecer un plan de continuidad de negocio para disponer de un plan de actuación para que la interrupción de las actividades de la organización sea la mínima posible en caso de desastre. Para realizar este plan de continuidad se va a partir del análisis de riesgos realizado previamente del que se van a determinar los procesos más críticos del negocio. Sabiendo cuáles son los procesos críticos, se van a detallar en un documento los pasos a seguir por CEINTECO en caso de que ocurra un desastre que afecte a dichos procesos. Este documento deberá ser aprobado por la Dirección de la organización. Se realizará un seguimiento continuo por parte del Comité de Seguridad para mejorar continuamente el plan de continuidad de negocio.
Activos cuyo riesgo se verá reducido	Instalaciones: [L22], [L23], [L28], [L29] Hardware: [HW1], [HW2], [HW3], [HW4], [HW5], [HW6], [HW10], [HW11], [HW12] Aplicación: [SW10], [SW11] Datos: [D1], [D2], [D3], [D5], [D6], [D7] Red:[COM3], [COM4], [COM5] Servicios [S]: todos los activos Equipamiento auxiliar [AUX]: todos los activos Personal [P]: todos los activos
Dimensiones de seguridad cuyo riesgo se verá reducido	Disponibilidad [D]
Responsable	Responsable de seguridad.
Controles	A.17.1
Indicadores	[IN28] Continuidad de negocio.
Coste	Horas de dedicación del responsable de seguridad. Horas de dedicación del Comité de Seguridad. Horas de dedicación del equipo de dirección. 4000€.
Duración	6 semanas.

Tabla 29. Proyecto-03: Plan de continuidad de negocio

PROYECTO-04: PROTECCIÓN DE LOS DATOS MEDIANTE TÉCNICAS CRIPTOGRÁFICAS	
Objetivo	Asegurar la protección de la autenticidad, confidencialidad e integridad de los datos de CEINTECO.
Descripción	Se van a implantar controles criptográficos en todos los servidores de la organización que contengan información confidencial así como en los discos duros de los equipos de todos los empleados para asegurar la autenticidad, confidencialidad e integridad de la información de la organización en caso de la ocurrencia de cualquier amenaza que ponga en peligro cualquiera de estas dimensiones de seguridad. Además, se establecerán procedimientos para: • La administración de las claves criptográficas a utilizar. • La recuperación de la información cifrada en caso de pérdida, daño o compromiso de las claves. • El reemplazo de las claves cada cierto tiempo.
Activos cuyo riesgo se verá reducido	Datos: [D1], [D2], [D3], [D5], [D6], [D7]
Dimensiones de seguridad cuyo riesgo se verá reducido	Autenticidad [A] Confidencialidad [C] Integridad [I]
Responsable	Responsable de seguridad.
Controles	A.10.1
Indicadores	[IN11] Controles criptográficos.
Coste	Horas de dedicación del responsable de seguridad. 2000€.
Duración	4 semanas.

Tabla 30. Proyecto-04: Protección de los datos mediante técnicas criptográficas

PROYECTO-05: MEJORA DE LOS PROCEDIMIENTOS DE RECURSOS HUMANOS	
Objetivo	Mejorar los procedimientos de recursos humanos de CEINTECO en todo el ciclo de vida de todos los empleados, desde su contratación hasta que dejan la empresa.
Descripción	Se van a establecer directrices a seguir en todos los procedimientos que realiza el personal de recursos humanos/administración. Los empleados deben ser seleccionados adecuadamente. Por ese motivo, antes de la contratación, el personal de RRHH/Administración de la empresa deberá verificar los antecedentes de todo candidato de acuerdo a la legislación vigente. En el momento de contratación, se establecerá claramente en el contrato las responsabilidades y condiciones en materia de seguridad de la información que tendrá el nuevo trabajador. Se definirá el proceso disciplinario a seguir en caso de que algún empleado incumpla la política o normas de seguridad de información la organización. Se definirá el procedimiento de actuación para cuando un empleado abandone la empresa, bien por propia voluntad o bien por despido. En este documento se describirá tanto el proceso de devolución de los activos de la organización que haya estado usando el empleado como el de revocación de sus derechos de acceso a las instalaciones y equipos de la organización.
Activos cuyo riesgo se verá reducido	Personal [P]: todos los activos Datos [D]: todos los activos Instalaciones [I]: todos los activos Hardware: [HW10], [HW11], [HW12] Equipamiento auxiliar [AUX]: todos los activos
Dimensiones de seguridad cuyo riesgo se verá reducido	Autenticidad [A] Confidencialidad [C] Disponibilidad [D]
Responsable	Responsable de seguridad.
Controles	A.7 A.8.1.2
Indicadores	[IN5] Disciplina.
Coste	Horas de dedicación del responsable de seguridad. Horas de dedicación del personal de administración. 5000€.
Duración	4 semanas.

Tabla 31. Proyecto-05: Mejora de los procedimientos de Recursos Humanos

PROYECTO-06: MEJORA EN LA GESTIÓN DE INCIDENTES DE SEGURIDAD	
Objetivo	Establecer los procedimientos de notificación y actuación de incidentes de seguridad de la información de CEINTECO con el fin de los incidentes sean resueltos lo más rápidamente y eficazmente posible.
Descripción	Se va a definir de manera clara el procedimiento de notificación de los incidentes de seguridad que aparezcan en la empresa así como de los puntos débiles que puedan encontrar los empleados en cualquier sistema o proceso de la organización. Asimismo, en este documento se describirán las responsabilidades que tiene cada empleado en cuanto a los incidentes de seguridad y cómo debe actuar cada trabajar en cada caso, dependiendo del rol que tenga en la organización. También se va a definir el procedimiento de actuación para resolver los incidentes de seguridad que puedan aparecer. Además, se guardará en una base de datos toda la información conocida de los incidentes de seguridad que vayan apareciendo en la organización para estudiarlas posteriormente y poder aprender de ellas.
Activos cuyo riesgo se verá reducido	Instalaciones [L]: todos los activos Hardware [HW]: todos los activos Aplicación [SW]: todos los activos Datos [D]: todos los activos Red [COM]: todos los activos Servicios [S]: todos los activos Equipamiento auxiliar [AUX]: todos los activos
Dimensiones de seguridad cuyo riesgo se verá reducido	Autenticidad [A] Confidencialidad [C] Integridad [I] Disponibilidad [D]
Responsable	Responsable de seguridad.
Controles	A.16
Indicadores	[IN26] Puntos débiles de seguridad. [IN27] Incidentes.
Coste	Horas de dedicación del responsable de seguridad. Horas de dedicación del técnico del centro de investigación. 3000€.
Duración	4 semanas.

Tabla 32. Proyecto-06: Mejora en la gestión de incidentes de seguridad

PROYECTO-07: INSTALACIÓN Y MANTENIMIENTO DE SOFTWARE	
Objetivo	Disponer en los equipos de las últimas versiones de software así como evitar posibles problemas debidos a software no permitido.
Descripción	Se van a establecer mecanismos de control para evitar que los usuarios no administradores de los equipos puedan instalar software. Se revisará el software instalado en los equipos de usuario y se instalará todo el software que debería estar instalado y no lo está, como pudiese ser el antivirus. Se van a establecer mecanismos que comprueben si hay nuevas actualizaciones de software disponibles y, en el caso de que las haya, se instalen de manera automática en los equipos de los empleados.
Activos cuyo riesgo se verá reducido	Software: [SW1], [SW2], [SW3], [SW4], [SW5], [SW6], [SW7], [SW8], [SW9], [SW10], [SW11] Datos: [D1], [D2], [D3], [D5], [D6], [D7]
Dimensiones de seguridad cuyo riesgo se verá reducido	Confidencialidad [C] Integridad [I] Disponibilidad [D]
Responsable	Responsable de seguridad
Controles	A.12.2.1 A.12.5 A.12.6 A.14.2.4
Indicadores	[IN20] Antivirus [IN21] Licencias de software [IN23] Software no autorizado instalado
Coste	Horas de dedicación del responsable de seguridad. Horas de dedicación del técnico del centro de investigación. Horas de dedicación de los técnicos de grupo. Licencias de software. 6000€.
Duración	4 semanas.

Tabla 33. Proyecto-07: Instalación y mantenimiento de software

PROYECTO-08: MEJORA EN LA GESTIÓN DE ACTIVOS	
Objetivo	Tener conocimiento preciso de todos los activos que posee CEINTECO.
Descripción	A partir del inventario de activos realizado en la fase 3 se asignará a cada activo un propietario o responsable de éste y se llevará a cabo la clasificación y etiquetado de todos los activos. Se va a redactar un documento en el que se expliquen las normas de uso adecuado de los activos así como el procedimiento a seguir si un empleado necesita manipular un activo o sacarlo fuera de las instalaciones de la organización.
Activos cuyo riesgo se verá reducido	Instalaciones [L]: todos los activos Hardware [HW]: todos los activos Aplicación [SW]: todos los activos Datos [D]: todos los activos Red [COM]: todos los activos Servicios [S]: todos los activos Equipamiento auxiliar [AUX]: todos los activos Personal [P]: todos los activos
Dimensiones de seguridad cuyo riesgo se verá reducido	Confidencialidad [C] Integridad [I] Disponibilidad [D]
Responsable	Responsable de seguridad.
Controles	A.8 A.11.2.5
Indicadores	[IN6] Inventario de activos [IN7] Mal uso de activos [IN8] Extravío de activos
Coste	Horas de dedicación del responsable de seguridad. Horas de dedicación del técnico del centro de investigación 2000€.
Duración	3 semanas

Tabla 34. Proyecto-08: Mejora en la gestión de activos

PROYECTO-09: MEJORA EN LOS REQUISITOS Y COMUNICACIONES	
Objetivo	Identificar y analizar los requisitos de seguridad necesarios para cualquier proyecto que se realice en CEINTECO así como proteger la información que se comunica por las redes de la organización.
Descripción	Se deberá realizar un análisis de requisitos de seguridad para los sistemas de información existentes en la organización y se tendrá que hacer también para los nuevos sistemas que aparezcan en la empresa. Se van a establecer medidas para proteger todas las comunicaciones y transacciones que se realicen por las redes de la organización así como por las redes públicas.
Activos cuyo riesgo se verá reducido	Red: [COM3], [COM4], [COM5] Servicios: [S1], [S2], [S3] Datos: [D1], [D2], [D3], [D5], [D6], [D7]
Dimensiones de seguridad cuyo riesgo se verá reducido	Confidencialidad [C] Integridad [I]
Responsable	Responsable de seguridad.
Controles	A.14.1 A.13.2.1 A.13.2.2 A.13.2.3 A.6.1.5
Indicadores	[IN27] Incidentes. [IN24] Comunicaciones externas.
Coste	Horas de dedicación del responsable de seguridad. 1500€.
Duración	3 semanas

Tabla 35. Proyecto-09: Mejora en los requisitos y comunicaciones

PROYECTO-10: MEJORA EN LOS DESARROLLOS	
Objetivo	Incluir controles de seguridad en los desarrollos realizados en CEINTECO.
Descripción	Se va a definir un documento en el que se expliquen las reglas para el desarrollo de software en la organización. Se van a implantar procedimientos de control de cambios para los desarrollos. Se van a definir los principios para la construcción de software seguro que todo empleado deberá conocer y seguir así como las pruebas básicas que se deben realizar a todo software para asegurar su seguridad.
Activos cuyo riesgo se verá reducido	Software: [SW10], [SW11] Datos: [D6]
Dimensiones de seguridad cuyo riesgo se verá reducido	Confidencialidad [C] Integridad [I] Disponibilidad [D]
Responsable	Responsable de seguridad.
Controles	A.14.2
Indicadores	[IN27] Incidentes.
Coste	Horas de dedicación del responsable de seguridad. 1500€.
Duración	3 semanas

Tabla 36. Proyecto-10: Mejora en los desarrollos

PROYECTO-11: MONITORIZACIÓN DE SISTEMAS	
Objetivo	Controlar todos los sistemas de CEINTECO con el fin de evitar potenciales amenazas.
Descripción	Se van a implantar soluciones para monitorear los sistemas de la organización de acuerdo con la legislación vigente. Se van a implantar soluciones para proteger los registros obtenidos de la monitorización de accesos no autorizados o alteraciones.
Activos cuyo riesgo se verá reducido	Instalaciones: [L1], [L2], [L3], [L4], [L5], [L22], [L23], [L28], [L29] Aplicación: [SW1], [SW2], [SW3], [SW10], [SW11] Datos: [D1], [D2], [D3], [D5], [D6], [D7] Red: [COM1], [COM2], [COM3] Servicios [S]: todos los activos
Dimensiones de seguridad cuyo riesgo se verá reducido	Confidencialidad [C] Integridad [I] Trazabilidad [T]
Responsable	Responsable de seguridad.
Controles	A.12.1.3 A.12.4 A.9.4.5
Indicadores	Registros de actividad.
Coste	Horas de dedicación del responsable de seguridad. 1500€.
Duración	2 semanas

Tabla 37. Proyecto-11. Monitorización de sistemas

PROYECTO-12: MEJORA DE LA SEGURIDAD EN LAS RELACIONES CON SUMINISTRADORES	
Objetivo	Comprobar que los suministradores de CEINTECO disponen del nivel de seguridad suficiente en los servicios que ofrecen a la organización.
Descripción	En primer lugar se va a comprobar la implementación de los acuerdos a los que se llegaron con los suministradores. Se verificará que el servicio ofrecido por el suministrador es el acordado. Se van a monitorear las conexiones para identificar las conexiones con terceras partes y el riesgo que éstas conllevan con el fin de mitigar estos riegos.
Activos cuyo riesgo se verá reducido	Red: [COM3], [COM4], [COM5] Servicios [S]: todos los activos Datos: [D1], [D2], [D3], [D5], [D6], [D7]
Dimensiones de seguridad cuyo riesgo se verá reducido	Autenticidad [A] Confidencialidad [C] Integridad [I] Disponibilidad [D] Trazabilidad [T]
Responsable	Responsable de seguridad.
Controles	A.15
Indicadores	[IN25] Revisión prestación servicios proveedores.
Coste	Horas de dedicación del responsable de seguridad. 1500€.
Duración	2 semanas.

Tabla 38. Proyecto-12: Mejora de la seguridad en las relaciones con suministradores

PROYECTO-13: REVISIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	
Objetivo	Comprobar el cumplimiento de las políticas y normas de seguridad de CEINTECO.
Descripción	Se va a contratar a un auditor externo para que realice una auditoría a la seguridad de la información de la organización para así tener una visión independiente del estado de la seguridad en la organización así como para que dé una valoración de las posibles mejoras a llevar a cabo. Por otra parte, tanto la Dirección como el Responsable de seguridad deberán revisar el cumplimiento de los procedimientos de seguridad establecidos por la organización que sean de su competencia. Este proyecto se repetirá anualmente.
Activos cuyo riesgo se verá reducido	Instalaciones [L]: todos los activos Hardware [HW]: todos los activos Aplicación [SW]: todos los activos Datos [D]: todos los activos Red [COM]: todos los activos Servicios [S]: todos los activos Equipamiento auxiliar [AUX]: todos los activos Personal [P]: todos los activos
Dimensiones de seguridad cuyo riesgo se verá reducido	Autenticidad [A] Confidencialidad [C] Integridad [I] Disponibilidad [D] Trazabilidad [T]
Responsable	Auditor externo. Dirección. Responsable de seguridad.
Controles	A.18.2
Indicadores	[IN29] Auditorías internas.
Coste	Horas de dedicación del equipo de dirección. Horas de dedicación del responsable de seguridad. Horas de dedicación del auditor externo. 6000€.
Duración	12 semanas para la auditoría. 2 semanas para la revisión por Dirección y Responsable de seguridad.

Tabla 39. Proyecto-13: Revisión de la seguridad de la información

4.3. Planificación de los proyectos

En este apartado se muestra la planificación en semanas de los proyectos propuestos para reducir el nivel de riesgo de CEINTECO (Tabla 40).

Como se puede observar, se conseguirá la completa realización de todos los proyectos propuestos tras 56 semanas, ya que se irá iniciando un nuevo proyecto cuando el proyecto previo haya terminado de implantarse. Se debe tener en cuenta también, que de estas 56 semanas, las últimas 14 se van a dedicar al Proyecto-13: revisión de la seguridad de la información, proyecto en el que se deberá realizar una auditoría externa y en el que la Dirección deberá revisar los procedimientos de seguridad establecidos hasta ese momento.

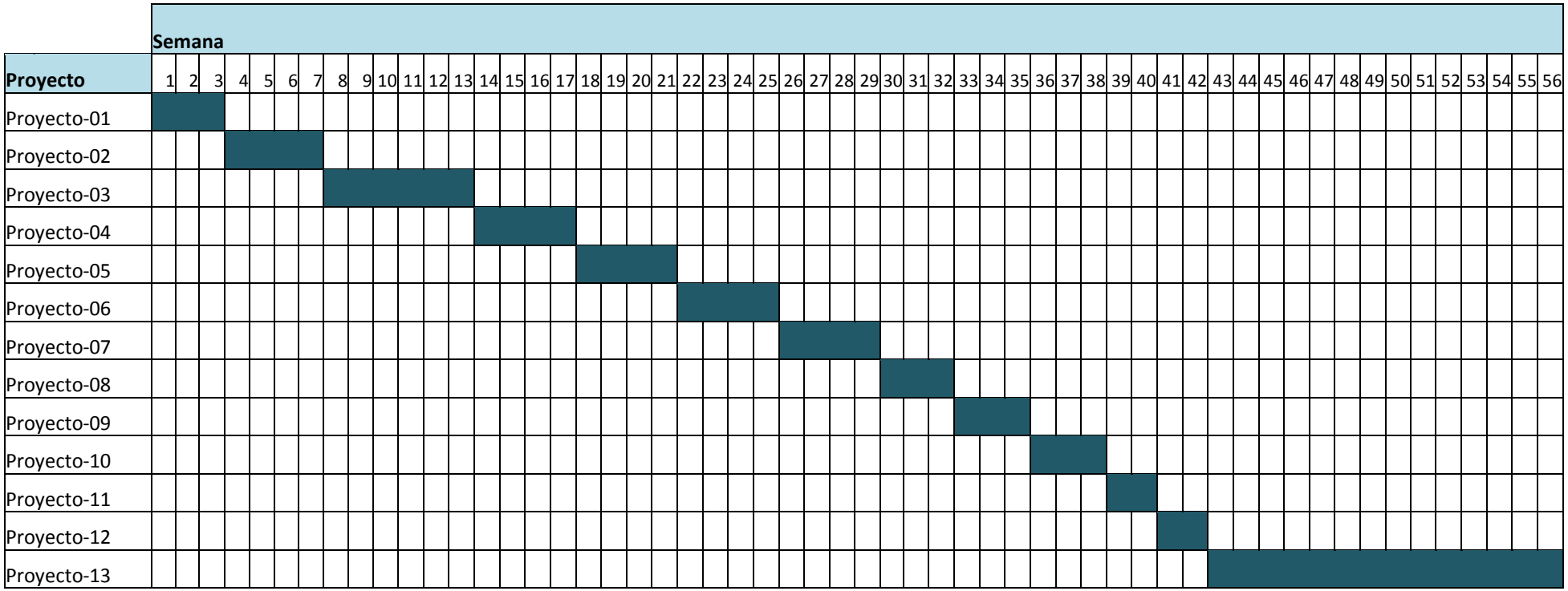


Tabla 40. Planificación proyectos de seguridad de CEINTEC

4.4. Resultados esperados tras la realización de los proyectos

Como se ha mencionado previamente, los proyectos propuestos en esta fase tienen como objetivo principal la reducción del riesgo de los activos analizados en la fase anterior. Además, con la realización de estos proyectos se va a conseguir una mejora del estado de los dominios de la ISO/IEC 27002:2013.

A continuación, en la Tabla 41, se muestra la comparación entre la situación inicial de los controles de la ISO 27002 que se obtuvo en la fase 1 y la situación que se espera obtener tras la realización de los proyectos.

ID	Control ISO 27002:2013	Situación inicial	Situación tras proyectos
A.5	**POLÍTICAS DE SEGURIDAD**		
A.5.1	**Directrices de la Dirección en seguridad de la información**		
A.5.1.1	Conjunto de políticas para la seguridad de la información	L0 -Inexistente	L4 -Administrado
A.5.1.2	Revisión de las políticas para la seguridad de la información	L0 -Inexistente	L4 -Administrado
A.6	**ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMACIÓN**		
A.6.1	**Organización interna**		
A.6.1.1	Asignación de responsabilidades para la seguridad de la información	L2 -Repetible	L4 -Administrado
A.6.1.2	Segregación de tareas	L2 -Repetible	L4 -Administrado
A.6.1.3	Contacto con las autoridades	L0 -Inexistente	L3 -Definido
A.6.1.4	Contacto con grupos de interés especial	L0 -Inexistente	L3 -Definido
A.6.1.5	Seguridad de la información en la gestión de proyectos	L1 -Inicial	L3 -Definido
A.6.2	**Dispositivos para movilidad y teletrabajo**		
A.6.2.1	Política de uso de dispositivos para movilidad	L0 -Inexistente	L2 -Repetible
A.6.2.2	Teletrabajo	L0 -Inexistente	L2 -Repetible
A.7	**SEGURIDAD LIGADA A LOS RECURSOS HUMANOS**		
A.7.1	**Antes de la contratación**		
A.7.1.1	Investigación de antecedentes	L0 -Inexistente	L4 -Administrado
A.7.1.2	Términos y condiciones de contratación	L3 -Definido	L4 -Administrado
A.7.2	**Durante la contratación**		
A.7.2.1	Responsabilidades de gestión	L3 -Definido	L4 -Administrado
A.7.2.2	Concienciación, educación y capacitación en seguridad de la información	L0 -Inexistente	L4 -Administrado
A.7.2.3	Proceso disciplinario	L0 -Inexistente	L4 -Administrado
A.7.3	**Cese o cambio de puesto de trabajo**		
A.7.3.1	Cese o cambio de puesto de trabajo	L3 -Definido	L4 -Administrado
A.8	**GESTIÓN DE ACTIVOS**		
A.8.1	**Responsabilidad sobre los activos**		
A.8.1.1	Inventario de activos	L2 -Repetible	L4 -Administrado
A.8.1.2	Propiedad de los activos	L0 -Inexistente	L4 -Administrado
A.8.1.3	Uso aceptable de los activos	L2 -Repetible	L4 -Administrado
A.8.1.4	Devolución de los activos	L5 - Optimizado	L4 -Administrado

A.8.2	**Clasificación de la información**		
A.8.2.1	Directrices de clasificación	L0 -Inexistente	L3 -Definido
A.8.2.2	Etiquetado y manipulado de la información	L0 -Inexistente	L3 -Definido
A.8.2.3	Manipulación de activos	L3 -Definido	L4 -Administrado
A.8.3	**Manejo de los soportes de almacenamiento**		
A.8.3.1	Gestión de los soportes extraíbles	L2 -Repetible	L3 -Definido
A.8.3.2	Eliminación de soportes	L0 -Inexistente	L1 -Inicial
A.8.3.3	Soportes físicos en tránsito	L2 -Repetible	L3 -Definido
A.9	**CONTROL DE ACCESOS**		
A.9.1	**Requisitos de negocio para el control de accesos**		
A.9.1.1	Política de control de accesos	L3 -Definido	L4 -Administrado
A.9.1.2	Control de acceso a las redes y servicios asociados	L3 -Definido	L4 -Administrado
A.9.2	**Gestión de acceso de usuario**		
A.9.2.1	Gestión de altas/bajas en el registro de usuarios	L3 -Definido	L4 -Administrado
A.9.2.2	Gestión de los derechos de acceso asignados a usuarios	L3 -Definido	L4 -Administrado
A.9.2.3	Gestión de los derechos de acceso con privilegios especiales	L3 -Definido	L4 -Administrado
A.9.2.4	Gestión de información confidencial de autenticación de usuarios	L0 -Inexistente	L3 -Definido
A.9.2.5	Revisión de los derechos de acceso de los usuarios	L0 -Inexistente	L3 -Definido
A.9.2.6	Retirada o adaptación de los derechos de acceso	L3 -Definido	L4 -Administrado
A.9.3	**Responsabilidades del usuario**		
A.9.3.1	Uso de información confidencial para la autenticación	L1 -Inicial	L3 -Definido
A.9.4	**Control de acceso a sistemas y aplicaciones**		
A.9.4.1	Restricción del acceso a la información	L3 -Definido	L4 -Administrado
A.9.4.2	Procedimientos seguros de inicio de sesión	L4 -Administrado	L4 -Administrado
A.9.4.3	Gestión de contraseñas de usuario	L2 -Repetible	L4 -Administrado
A.9.4.4	Uso de herramientas de administración de sistemas	L1 -Inicial	L3 -Definido
A.9.4.5	Control de acceso al código fuente de los programas	L3 -Definido	L3 -Definido
A.10	**CIFRADO**		
A.10.1	**Controles criptográficos**		
A.10.1.1	Política de uso de los controles criptográficos	L0 -Inexistente	L3 -Definido
A.10.1.2	Gestión de claves	L0 -Inexistente	L3 -Definido
A.11	**SEGURIDAD FÍSICA Y AMBIENTAL**		
A.11.1	**Áreas seguras**		
A.11.1.1	Perímetro de seguridad física	L3 -Definido	L4 -Administrado
A.11.1.2	Controles físicos de entrada	L3 -Definido	L4 -Administrado
A.11.1.3	Seguridad de oficinas, despachos y recursos	L3 -Definido	L4 -Administrado
A.11.1.4	Protección contra las amenazas externas y ambientales	L3 -Definido	L4 -Administrado
A.11.1.5	El trabajo en áreas seguras	L2 -Repetible	L3 -Definido
A.11.1.6	Áreas de acceso público, carga y descarga	L1 -Inicial	L2 -Repetible
A.11.2	**Seguridad de los equipos**		
A.11.2.1	Emplazamiento y protección de equipos	L0 -Inexistente	L3 -Definido
A.11.2.2	Instalaciones de suministro	L3 -Definido	L4 -Administrado
A.11.2.3	Seguridad del cableado	L2 -Repetible	L3 -Definido

A.11.2.4	Mantenimiento de los equipos	L2 -Repetible	L4 -Administrado
A.11.2.5	Salida de activos fuera de las dependencias de la empresa	L3 -Definido	L3 -Definido
A.11.2.6	Seguridad de los equipos y activos fuera de las instalaciones	L2 -Repetible	L3 -Definido
A.11.2.7	Reutilización o retirada segura de dispositivos de almacenamiento	L2 -Repetible	L3 -Definido
A.11.2.8	Equipo informático de usuario desatendido	L1 -Inicial	L3 -Definido
A.11.2.9	Política de puesto de trabajo despejado y bloqueo de pantalla	L1 -Inicial	L3 -Definido
A.12	**SEGURIDAD EN LA OPERATIVA**		
A.12.1	**Responsabilidades y procedimientos de operación**		
A.12.1.1	Documentación de procedimientos de operación	L0 -Inexistente	L3 -Definido
A.12.1.2	Gestión de cambios	L2 -Repetible	L2 -Repetible
A.12.1.3	Gestión de capacidades	L0 -Inexistente	L3 -Definido
A.12.1.4	Separación de entornos de desarrollo, prueba y producción	L0 -Inexistente	L0 -Inexistente
A.12.2	**Protección contra código malicioso**		
A.12.2.1	Controles contra el código malicioso	L4 -Administrado	L4 -Administrado
A.12.3	**Copias de seguridad**		
A.12.3.1	Copias de seguridad de la información	L2 -Repetible	L3 -Definido
A.12.4	**Registro de actividad y supervisión**		
A.12.4.1	Registro y gestión de eventos de actividad	L0 -Inexistente	L4 -Administrado
A.12.4.2	Protección de los registros de información	L0 -Inexistente	L4 -Administrado
A.12.4.3	Registros de actividad del administrador y operador del sistema	L0 -Inexistente	L4 -Administrado
A.12.4.4	Sincronización de relojes	L5 - Optimizado	L5 - Optimizado
A.12.5	**Control del software en explotación**		
A.12.5.1	Instalación del software en sistemas en producción	L3 -Definido	L4 -Administrado
A.12.6	**Gestión de la vulnerabilidad técnica**		
A.12.6.1	Gestión de las vulnerabilidades técnicas	L0 -Inexistente	L3 -Definido
A.12.6.2	Restricciones en la instalación de software	L0 -Inexistente	L3 -Definido
A.12.7	**Consideraciones de las auditorías de los sistemas de información**		
A.12.7.1	Controles de auditoría de los sistemas de información	L0 -Inexistente	L3 -Definido
A.13	**SEGURIDAD EN LAS TELECOMUNICACIONES**		
A.13.1	**Gestión de la seguridad en las redes**		
A.13.1.1	Controles de red	L1 -Inicial	L2 -Repetible
A.13.1.2	Mecanismos de seguridad asociados a servicios en red	L0 -Inexistente	L2 -Repetible
A.13.1.3	Segregación de redes	L3 -Definido	L3 -Definido
A.13.2	**Intercambio de información con partes externas**		
A.13.2.1	Políticas y procedimientos de intercambio de información	L1 -Inicial	L3 -Definido
A.13.2.2	Acuerdos de intercambio	L0 -Inexistente	L3 -Definido
A.13.2.3	Mensajería electrónica	L0 -Inexistente	L3 -Definido
A.13.2.4	Acuerdos de confidencialidad y secreto	L1 -Inicial	L3 -Definido
A.14	**ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN**		
A.14.1	**Requisitos de seguridad de los sistemas de información**		
A.14.1.1	Análisis y especificación de los requisitos de seguridad	L0 -Inexistente	L3 -Definido
A.14.1.2	Seguridad de las comunicaciones en servicios accesibles por redes públicas	L0 -Inexistente	L3 -Definido

A.14.1.3	Protección de las transacciones por redes telemáticas	L0 -Inexistente	L3 -Definido
A.14.2	**Seguridad en los procesos de desarrollo y soporte**		
A.14.2.1	Política de desarrollo seguro de software	L0 -Inexistente	L3 -Definido
A.14.2.2	Procedimientos de control de cambios en los sistemas	L0 -Inexistente	L3 -Definido
A.14.2.3	Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo	L0 -Inexistente	L3 -Definido
A.14.2.4	Restricciones a los cambios en los paquetes de software	L0 -Inexistente	L4 -Administrado
A.14.2.5	Uso de principios de ingeniería en protección de sistemas	L0 -Inexistente	L3 -Definido
A.14.2.6	Seguridad en entornos de desarrollo	L0 -Inexistente	L3 -Definido
A.14.2.7	Externalización del desarrollo software	L0 -Inexistente	L0 -Inexistente
A.14.2.8	Pruebas de funcionalidad durante el desarrollo de los sistemas	L0 -Inexistente	L2 -Repetible
A.14.2.9	Pruebas de aceptación	L0 -Inexistente	L2 -Repetible
A.14.3	**Datos de prueba**		
A.14.3.1	Protección de los datos utilizados en pruebas	L3 -Definido	L4 -Administrado
A.15	**RELACIONES CON SUMINISTRADORES**		
A.15.1	**Seguridad de la información en las relaciones con suministradores**		
A.15.1.1	Política de seguridad de la información para suministradores	L0 -Inexistente	L3 -Definido
A.15.1.2	Tratamiento del riesgo dentro de acuerdos de suministradores	L0 -Inexistente	L3 -Definido
A.15.1.3	Cadena de suministro en tecnologías de la información y comunicaciones	L3 - Definido	L4 -Administrado
A.15.2	**Gestión de la prestación del servicio por suministradores**		
A.15.2.1	Supervisión y revisión de los servicios prestados por terceros	L0 -Inexistente	L3 -Definido
A.15.2.2	Gestión de cambios en los servicios prestados por terceros	L0 -Inexistente	L3 -Definido
A.16	**GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN**		
A.16.1	**Gestión de incidentes de seguridad de la información y mejoras**		
A.16.1.1	Responsabilidades y procedimientos	L2 -Repetible	L4 -Administrado
A.16.1.2	Notificación de los eventos de seguridad de la información	L2 -Repetible	L4 -Administrado
A.16.1.3	Notificación de puntos débiles de la seguridad	L2 -Repetible	L4 -Administrado
A.16.1.4	Valoración de eventos de seguridad de la información y toma de decisiones	L1 -Inicial	L3 -Definido
A.16.1.5	Respuesta a los incidentes de seguridad	L1 -Inicial	L3 -Definido
A.16.1.6	Aprendizaje de los incidentes de seguridad de la información	L1 -Inicial	L3 -Definido
A.16.1.7	Recopilación de las evidencias	L0 -Inexistente	L2 -Repetible
A.17	**ASPECTOS DE LA SEGURIDAD DE LA INFORMACIÓN EN LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO**		
A.17.1	**Continuidad de la seguridad de la información**		
A.17.1.1	Planificación de la continuidad de la seguridad de la información	L0 -Inexistente	L3 -Definido
A.17.1.2	Implantación de la continuidad de la seguridad de la información	L0 -Inexistente	L3 -Definido
A.17.1.3	Verificación, revisión y evaluación de la continuidad de la seguridad de la información	L0 -Inexistente	L3 -Definido
A.17.2	**Redundancias**		
A.17.2.1	Disponibilidad de instalaciones para el procesamiento de la información	L0 -Inexistente	L0 -Inexistente
A.18	**CUMPLIMIENTO**		
A.18.1	**Cumplimiento de los requisitos legales y contractuales**		

A.18.1.1	Identificación de la legislación aplicable	L4 -Administrado	L4 -Administrado
A.18.1.2	Derechos de propiedad intelectual (DPI)	L4 -Administrado	L4 -Administrado
A.18.1.3	Protección de los registros de la organización	L3 -Definido	L4 -Administrado
A.18.1.4	Protección de datos y privacidad de la información personal	L3 -Definido	L4 -Administrado
A.18.1.5	Regulación de los controles criptográficos	L1 -Inicial	L3 -Definido
A.18.2	**Revisiones de la seguridad de la información**		
A.18.2.1	Revisión independiente de la seguridad de la información	L0 -Inexistente	L3 -Definido
A.18.2.2	Cumplimiento de las políticas y normas de seguridad	L0 -Inexistente	L3 -Definido
A.18.2.3	Comprobación del cumplimiento	L0 -Inexistente	L3 -Definido

Tabla 41. Situación inicial de los controles vs situación esperada tras realizar los proyectos propuestos

Tal como se hizo en la fase 1 para la situación inicial de los controles de seguridad implantados en CEINTECO, si se hace una media de la situación esperada tras la realización de los proyectos de los distintos controles de cada dimensión y se cambia la escala para verla en porcentaje, se obtiene la evaluación general esperada para cada dimensión de la ISO 27002. La situación esperada en la que quedaría la implementación de la ISO 27002 en CEINTECO tras llevar a cabo los proyectos propuestos en esta fase se muestra en la Tabla 42.

Control ISO 27002:2013	**% Efectividad**
A.5 POLÍTICAS SEGURIDAD	95%
A.6 ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMACIÓN	80%
A.7 SEGURIDAD LIGADA A LOS RECURSOS HUMANOS	95%
A.8 GESTIÓN DE ACTIVOS	84,5%
A.9 CONTROL DE ACCESOS	93,21%
A.10 CIFRADO	90%
A.11 SEGURIDAD FÍSICA Y AMBIENTAL	89,33%
A.12 SEGURIDAD EN LA OPERATIVA	83,21%
A.13 SEGURIDAD EN LAS TELECOMUNICACIONES	78,57%
A.14 ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN	84,16%
A.15 RELACIONES CON SUMINISTRADORES	90%
A.16 GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN	86,42%
A.17 ASPECTOS DE LA SEGURIDAD DE LA INFORMACIÓN EN LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO	67,5%
A.18 CUMPLIMIENTO	92,5%

Tabla 42. Estado de la implementación ISO 27002:2013 esperado tras realizar los proyectos propuestos

A continuación, en la Imagen 22, se muestra el estado de los controles de la ISO 27002:2013 al que se espera llegar tras aplicar los proyectos propuestos en esta fase comparado con el estado inicial de la seguridad de la información, con el estado al que se quiere llegar tras la implementación del SGSI y con el que sería el estado óptimo.

En este caso, la línea azul representa el estado inicial del cumplimiento de los controles, la línea morada el estado que se espera obtener tras la aplicación de los proyectos propuestos, la línea roja un posible objetivo de cumplimiento a largo plazo y, por último, la línea verde

representa el nivel de cumplimiento óptimo. Los números que se muestran en la gráfica hacen referencia a los diferentes dominios contemplados en la ISO 27002:2013.

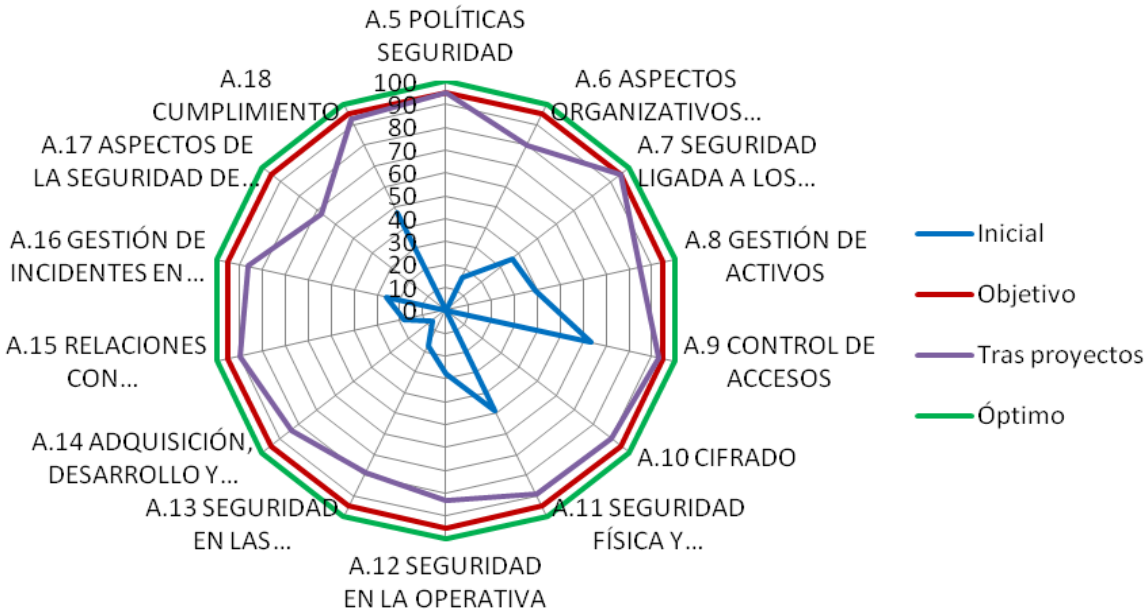


Imagen 22. Estado de los controles esperado tras realizar los proyectos propuestos

Vemos que tras llevar a cabo los proyectos propuestos en esta fase se espera alcanzar un estado muy cercano al objetivo que se planteó la organización al iniciar este proyecto de implantación de la norma ISO/IEC 27001:2013.

5. Fase 5: Auditoría de cumplimiento

5.1. Introducción

En esta fase se va a realizar la auditoría de cumplimiento, que tiene como objetivo la evaluación del estado de la seguridad de la información de CEINTECO tras haber finalizado con éxito todas las fases anteriores. Para ello, se evaluará el grado de madurez en lo que respecta a los diferentes dominios y controles planteados por la ISO/IEC 27002:2013.

Antes de empezar a realizar la auditoría de cumplimiento, vamos a suponer que los proyectos propuestos en la fase anterior se han implementado correctamente en la organización. Por lo tanto, se partirá de ese supuesto para llevar a cabo la evaluación de la seguridad de CEINTECO.

5.2. Metodología

Para evaluar correctamente la madurez de la seguridad de la información de CEINTECO se va a utilizar el estándar ISO/IEC 27002:2013, puesto que se trata de un estándar internacionalmente conocido y es perfectamente válido para la mayoría de organizaciones.

Como se ha mencionado en capítulos anteriores, el estándar ISO/IEC 27002:2013 está formado por 114 controles o salvaguardas organizadas en 14 dominios y 35 objetivos de control. Para comprobar el estado de la seguridad de la organización, se evaluará el nivel de madurez de cada uno de los controles existentes en la norma. Para ello, se volverá a utilizar el Modelo de Madurez de Capacidades (CCM) que se utilizó para realizar el análisis diferencial del estado inicial de la seguridad de CEINTECO, que se encuentra definido en la Tabla 1.

Recordamos en la Tabla 43, sin volver a entrar en detalle, los niveles que se van a utilizar para evaluar el grado de madurez de cada uno de los controles.

Nivel	Efectividad	Significado
L0	0%	Inexistente
L1	10%	Inicial
L2	50%	Repetible
L3	90%	Definido
L4	95%	Administrado
L5	100%	Optimizado

Tabla 43.Niveles CMM

5.3. Evaluación de la madurez

A continuación, en la Tabla 44, se muestra el nivel de madurez de cada uno de los controles de la ISO 27002:2013 así como la justificación de dicho nivel.

ID	Control ISO 27002:2013	CCM	Justificación
A.5	**POLÍTICAS DE SEGURIDAD**		
A.5.1	**Directrices de la Dirección en seguridad de la información**		
A.5.1.1	Conjunto de políticas para la seguridad de la información	L5	Se ha comprobado que existe una política de seguridad y que se le aplican mejoras .
A.5.1.2	Revisión de las políticas para la seguridad de la información	L5	Existe un proyecto anual de mejora de la política de seguridad que ya ha sido aplicado al menos una vez.
A.6	**ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMACIÓN**		
A.6.1	**Organización interna**		
A.6.1.1	Asignación de responsabilidades para la seguridad de la información	L4	Existe un documento en el que se asignan los roles de los empleados en lo referente a la seguridad de la información cuya evolución se comprueba anualmente a través de un indicador. Sin embargo, no se ha podido demostrar que este proceso se revise y mejore cada cierto tiempo.
A.6.1.2	Segregación de tareas	L4	Existe un documento en el que se describen las tareas de los empleados en lo referente a la seguridad de la información y se ha comprobado que éstas se están realizando correctamente por las personas adecuadas, gracias a los indicadores, de acuerdo al documento.
A.6.1.3	Contacto con las autoridades	L2	Se ha comprobado que ha existido contacto con las autoridades. Sin embargo, no hay ningún documento formal que indique cómo se debe realizar este contacto ni cuándo, ni existen indicadores que permitan medir correctamente este control.
A.6.1.4	Contacto con grupos de interés especial	L2	Se ha comprobado que ha existido contacto con grupos de interés relacionados con la seguridad de la información. Sin embargo, no hay ningún documento que indique cómo se debe realizar este contacto ni existen indicadores que permitan medir correctamente este control.
A.6.1.5	Seguridad de la información en la gestión de proyectos	L3	Se ha comprobado que se han realizado análisis de requisitos para los sistemas y procesos existentes y que se realizan para los nuevos procesos.
A.6.2	**Dispositivos para movilidad y teletrabajo**		

A.6.2.1	Política de uso de dispositivos para movilidad	L4	Existen normas definidas y empleados por los trabajadores respecto al uso de dispositivos móviles, así como indicadores para seguir su evolución y mejorar esta política.
A.6.2.2	Teletrabajo	L2	Existen algunas normas no escritas para el teletrabajo, pero no una política específica que especifique el procedimiento a seguir.
A.7	**SEGURIDAD LIGADA A LOS RECURSOS HUMANOS**		
A.7.1	**Antes de la contratación**		
A.7.1.1	Investigación de antecedentes	L4	Se ha comprobado que los miembros de administración investigan sobre los posibles candidatos antes de contratarlos. Sin embargo, no se ha podido demostrar que este proceso se revise y mejore cada cierto tiempo.
A.7.1.2	Términos y condiciones de contratación	L4	Se ha comprobado que se definen correctamente los términos y condiciones de las nuevas contrataciones antes de llevarlas a cabo. Sin embargo, no se ha podido demostrar que este proceso se revise y mejore cada cierto tiempo.
A.7.2	**Durante la contratación**		
A.7.2.1	Responsabilidades de gestión	L4	Se ha comprobado que se comunica a los empleados la política de seguridad así como la necesidad de aplicarla. Sin embargo, no se ha comprobado que se revisen las responsabilidades.
A.7.2.2	Concienciación, educación y capacitación en seguridad de la información	L5	Existe un programa de formación que está en constante mejora gracias a los indicadores que controlan la evolución de este control.
A.7.2.3	Proceso disciplinario	L5	Se ha comprobado que hay definido un proceso disciplinario para cuando un empleado no cumpla las normas y que se realiza un seguimiento de éste con el objetivo de mejorarlo.
A.7.3	**Cese o cambio de puesto de trabajo**		
A.7.3.1	Cese o cambio de puesto de trabajo	L4	Existe un procedimiento de actuación para cuando un empleado abandona la empresa. Se ha comprobado que se está llevando a cabo de manera adecuada. Sin embargo, no se ha podido demostrar que este proceso esté bajo constante mejora.
A.8	**GESTIÓN DE ACTIVOS**		
A.8.1	**Responsabilidad sobre los activos**		
A.8.1.1	Inventario de activos	L5	Se ha comprobado que existe un inventario de activos y que existe un procedimiento para ir inventariando los nuevos activos.
A.8.1.2	Propiedad de los activos	L5	Se ha comprobado que todos los activos tienen un propietario y que existe un procedimiento para asignar el propietario de los nuevos activos.

A.8.1.3	Uso aceptable de los activos	L4	Existe un documento en el que se definen las normas de uso de los activos. Se ha comprobado que los empleados están siguiendo estas reglas. Sin embargo, no se ha podido demostrar que este proceso se revise y/o se mejore, pese a que existen indicadores para controlar la evolución de este control.
A.8.1.4	Devolución de los activos	L2	Existen normas a seguir para la devolución de activos. Sin embargo, éste no es muy claro.
A.8.2	**Clasificación de la información**		
A.8.2.1	Directrices de clasificación	L2	Los activos están clasificados. Sin embargo, no existe un documento en el que estén definidas las directrices de clasificación.
A.8.2.2	Etiquetado y manipulado de la información	L3	Los activos están etiquetados. Sin embargo, no existe un documento en el que estén definidas las directrices de etiquetado. Existen definidas algunas normas para el tratamiento de la información, pero se recomienda revisarlas y mejorarlas.
A.8.2.3	Manipulación de activos	L4	Las normas de manipulación de activos están definidas y se ha comprobado que se siguen de manera adecuada y se puede seguir quien lleva a cabo la manipulación de cada activo.
A.8.3	**Manejo de los soportes de almacenamiento**		
A.8.3.1	Gestión de los soportes extraíbles	L3	Existen procedimientos para la utilización y gestión de los soportes extraíbles. Sin embargo, no existe una métrica que permita conocer si se está aplicando correctamente.
A.8.3.2	Eliminación de soportes	L1	No se han encontrado procedimientos concretos para la eliminación de los soportes. Se reconoce que existe el problema y que hay que mejorarlo.
A.8.3.3	Soportes físicos en tránsito	L4	Existen procedimientos para el tratamiento de soportes físicos que se sacan fuera de la organización y existen medidas para controlar la evolución de este control.
A.9	**CONTROL DE ACCESOS**		
A.9.1	**Requisitos de negocio para el control de accesos**		
A.9.1.1	Política de control de accesos	L5	Existe una política de control de accesos definida y seguida por todos los trabajadores. Esta política es revisada por la dirección junto al resto de políticas cada cierto tiempo.
A.9.1.2	Control de acceso a las redes y servicios asociados	L5	Se ha comprobado que hay implantados controles de acceso a las redes y servicios así como indicadores con los que seguir su evolución y mejorar los accesos a las redes y servicios.
A.9.2	**Gestión de acceso de usuario**		

A.9.2.1	Gestión de altas/bajas en el registro de usuarios	L5	Existe un procedimiento a seguir para dar de alta y de baja usuarios en los sistemas y éste procedimiento se está midiendo de manera mensual y se revisa para mejorarlo cada cierto tiempo.
A.9.2.2	Gestión de los derechos de acceso asignados a usuarios	L5	Existe un procedimiento a seguir para otorgar y quitar derechos a los usuarios en los sistemas y éste procedimiento se está midiendo de manera mensual y se revisa para mejorarlo cada cierto tiempo.
A.9.2.3	Gestión de los derechos de acceso con privilegios especiales	L5	Existe un procedimiento a seguir para otorgar y quitar derechos especiales a los usuarios en los sistemas y éste procedimiento se está midiendo de manera mensual y se revisa para mejorarlo cada cierto tiempo.
A.9.2.4	Gestión de información confidencial de autenticación de usuarios	L2	Existen normas a seguir referentes a este control que son conocidas por los empleados. Sin embargo, no se ha encontrado un documento en el que se defina formalmente el procedimiento.
A.9.2.5	Revisión de los derechos de acceso de los usuarios	L2	Se ha comprobado que los derechos de acceso de los usuarios se revisan de vez en cuando. Sin embargo, no existe ningún documento formal que indique cada cuanto se debe realizar ni el responsable de hacerlo.
A.9.2.6	Retirada o adaptación de los derechos de acceso	L2	Se ha comprobado que los derechos de acceso de los usuarios se retiran de manera adecuada. Sin embargo, no existe ningún documento formal que indique el procedimiento a seguir ni para retirar los derechos de acceso ni para adaptarlos en el caso de que cambien los derechos de un usuario.
A.9.3	**Responsabilidades del usuario**		
A.9.3.1	Uso de información confidencial para la autenticación	L3	Se ha comprobado que a los usuarios se les exige la no utilización de información confidencial para autenticarse. Se ha comprobado que se está llevando a cabo de manera adecuada. Sin embargo, no existen indicadores para medir este control eficazmente.
A.9.4	**Control de acceso a sistemas y aplicaciones**		
A.9.4.1	Restricción del acceso a la información	L4	Hay puestas en marcha medidas para evitar el acceso a usuarios no autorizados. Sin embargo, no existe ningún documento formal que indique cada cuanto se debe realizar ni el responsable de hacerlo.
A.9.4.2	Procedimientos seguros de inicio de sesión	L3	Se ha comprobado que existen procedimientos seguros de inicio de sesión en todos los sistemas de la organización. Sin embargo, se deben implantar indicadores para comprobar su evolución e intentar mejorarlos.
A.9.4.3	Gestión de contraseñas de usuario	L5	Se ha comprobado que existe una política de contraseñas y que los sistemas de gestión de contraseñas aseguran el uso de contraseñas de calidad.

A.9.4.4	Uso de herramientas de administración de sistemas	L3	El software instalado en los equipos está totalmente controlado y ningún empleado sin derechos de administrador puede hacer uso ni modificar las herramientas de administración. Sin embargo, no existen indicadores que midan su evolución.
A.9.4.5	Control de acceso al código fuente de los programas	L5	Se ha comprobado que el acceso al código fuente de los programas está restringido y que se controla a través de monitorización. Además, existen indicadores para comprobar su evolución y así mejorarlo.
A.10	**CIFRADO**		
A.10.1	**Controles criptográficos**		
A.10.1.1	Política de uso de los controles criptográficos	L4	Se ha comprobado que hay implantados controles criptográficos en todos los sistemas de la organización. Sin embargo, no se ha podido demostrar que este proceso se revise y/o se mejore, pese a que existen indicadores para controlar la evolución de este control.
A.10.1.2	Gestión de claves	L3	Existen procedimientos para el control de las claves criptográficas utilizadas y estos se están aplicando correctamente. Sin embargo, no existe ningún indicador para controlar la evolución y no se ha podido demostrar que este proceso se revise y/o se mejore.
A.11	**SEGURIDAD FÍSICA Y AMBIENTAL**		
A.11.1	**Áreas seguras**		
A.11.1.1	Perímetro de seguridad física	L5	Existen medidas de seguridad que aseguran el perímetro de la organización. Se ha comprobado que se controla su evolución, se revisa y se intenta mejorar.
A.11.1.2	Controles físicos de entrada	L5	Existen controles físicos en todas las entradas a las instalaciones de la organización . Se ha comprobado que se controla su evolución, se revisa y se intenta mejorar.
A.11.1.3	Seguridad de oficinas, despachos y recursos	L5	Existen controles físicos en todas las salas de la organización y éstos se controlan y se encuentran en constante mejora.
A.11.1.4	Protección contra las amenazas externas y ambientales	L5	Existen medidas de protección contra las amenazas externas y ambientales así como medidas para comprobar su evolución y mejorarlo.
A.11.1.5	El trabajo en áreas seguras	L2	Existen buenas prácticas respecto a este control pero no existe un documento formal.
A.11.1.6	Áreas de acceso público, carga y descarga	L2	Existen buenas prácticas respecto a este control pero no existe un documento formal.
A.11.2	**Seguridad de los equipos**		

A.11.2.1	Emplazamiento y protección de equipos	L3	Los equipos se encuentran emplazados en lugares con control de acceso así como protegidos de posibles amenazas ambientales. Existe documentación sobre este control. Sin embargo no existen controles para comprobar su evolución.
A.11.2.2	Instalaciones de suministro	L5	Existen medidas para proteger los equipos contra fallos del suministro eléctrico y éstas son controladas y en constante mejora.
A.11.2.3	Seguridad del cableado	L4	No existen cables a la vista en toda la instalación y existen indicadores para medir el número de cables visibles.
A.11.2.4	Mantenimiento de los equipos	L5	Existe un procedimiento de mantenimiento de equipos así como un responsable para ello. También existen indicadores para comprobar la correcta realización de este procedimiento y poder aplicar mejoras.
A.11.2.5	Salida de activos fuera de las dependencias de la empresa	L4	Existe un procedimiento a seguir para cuando se quieren sacar activos fuera de las instalaciones de la organización. Existe un procedimiento para comunicar que se va a sacar un activo, por lo que este control se puede medir. Sin embargo, no se ha podido demostrar que el proceso se revise y mejore.
A.11.2.6	Seguridad de los equipos y activos fuera de las instalaciones	L3	Existe una política de uso aceptable de activos que debe aplicarse a todos los activos en general. Sin embargo, se debería especificar en un documento las medidas de seguridad a tomar en el caso concreto de que se saque un activo fuera de las instalaciones de la organización.
A.11.2.7	Reutilización o retirada segura de dispositivos de almacenamiento	L3	Existen normas documentadas a seguir respecto a este punto. Sin embargo, no existen indicadores para medir su evolución.
A.11.2.8	Equipo informático de usuario desatendido	L3	Existen normas documentadas a seguir respecto a este punto. Sin embargo, no se puede medir este control por la falta de métricas.
A.11.2.9	Política de puesto de trabajo despejado y bloqueo de pantalla	L3	Existen normas documentadas a seguir respecto a este punto. Sin embargo, no se puede medir este control puesto que no hay ningún indicador que refleje su evolución.
A.12	**SEGURIDAD EN LA OPERATIVA**		
A.12.1	**Responsabilidades y procedimientos de operación**		
A.12.1.1	Documentación de procedimientos de operación	L2	No existe un documento formal donde se encuentren documentados los procedimientos operativos. Sin embargo, los empleados sí que siguen métodos propios.
A.12.1.2	Gestión de cambios	L2	No existe ningún proceso formal para controlar los cambios que afectan a la seguridad de la información de la organización. Sin embargo, sí que se tienen algunos registros de cambios que se han ido haciendo.

A.12.1.3	Gestión de capacidades	L3	Los sistemas de la organización se encuentran monitorizados. Sin embargo, no se han encontrado evidencias de que con los registros obtenidos se ajuste el uso de los recursos de los sistemas.
A.12.1.4	Separación de entornos de desarrollo, prueba y producción	L0	No aplica
A.12.2	**Protección contra código malicioso**		
A.12.2.1	Controles contra el código malicioso	L5	Existen implantadas medidas contra código malicioso en todos los equipos de la organización, así como indicadores para medir su funcionamiento. Este proceso está en constante mejora.
A.12.3	**Copias de seguridad**		
A.12.3.1	Copias de seguridad de la información	L5	Existe un procedimiento formal a seguir para realizar las copias de seguridad y existen métricas para comprobar su funcionamiento y evolución. Además, se ha comprobado que este control está en constante mejora.
A.12.4	**Registro de actividad y supervisión**		
A.12.4.1	Registro y gestión de eventos de actividad	L4	Se ha comprobado que los eventos de actividad se registran y existen métricas para comprobar su funcionamiento y evolución. Sin embargo, no se ha podido demostrar que este proceso se revise y/o se mejore.
A.12.4.2	Protección de los registros de información	L4	Se ha comprobado que los registros de información que se crean y guardan están correctamente protegidos. Sin embargo, no se ha encontrado una métrica para comprobar el funcionamiento y evolución de este control.
A.12.4.3	Registros de actividad del administrador y operador del sistema	L4	Se ha comprobado que los eventos de actividad de los administradores se registran y existen métricas para comprobar su funcionamiento y evolución. Sin embargo, no se ha podido demostrar que este proceso se revise y/o se mejore.
A.12.4.4	Sincronización de relojes	L5	Los relojes de los sistemas de la organización están correctamente sincronizados.
A.12.5	**Control del software en explotación**		
A.12.5.1	Instalación del software en sistemas en producción	L4	Existen procedimientos a seguir para instalar software en los sistemas. Se controla la evolución de este control utilizando un indicador. Sin embargo, no se ha podido demostrar que este proceso se revise y/o se mejore.
A.12.6	**Gestión de la vulnerabilidad técnica**		
A.12.6.1	Gestión de las vulnerabilidades técnicas	L2	Se obtiene información sobre las vulnerabilidades pero no existe un proceso formal para ello que indique con qué frecuencia se debe obtener esta información. Cada uno de los empleados responsables de esta tarea lo hace a su propia manera y buscando la información en sitios distintos.

A.12.6.2	Restricciones en la instalación de software	L4	Existen controles para evitar que cualquier usuario pueda instalar cualquier software en los ordenadores e indicadores que sirven para comprobar el estado de este control así como su evolución.
A.12.7	**Consideraciones de las auditorías de los sistemas de información**		
A.12.7.1	Controles de auditoría de los sistemas de información	L3	Existe un plan de auditoría para comprobar la seguridad de la organización que incluye auditar los sistemas de información de la organización. Sin embargo, no existe un indicador para comprobar la evolución de este control en concreto.
A.13	**SEGURIDAD EN LAS TELECOMUNICACIONES**		
A.13.1	**Gestión de la seguridad en las redes**		
A.13.1.1	Controles de red	L2	Se realizan controles de red de vez en cuando y no siempre de la misma manera.
A.13.1.2	Mecanismos de seguridad asociados a servicios en red	L1	La organización conoce la necesidad de aplicar mecanismos de seguridad asociados a servicios de red pero todavía no existen ningún procedimiento respecto a este control
A.13.1.3	Segregación de redes	L4	Se ha comprobado que existen diferentes redes para los diferentes grupos y salas de servidores. Sin embargo, no se ha podido demostrar que se revise y/o mejore este proceso.
A.13.2	**Intercambio de información con partes externas**		
A.13.2.1	Políticas y procedimientos de intercambio de información	L5	Existe una política respecto a cómo se debe realizar el intercambio de información entre los empleados y con el exterior. Existe un indicador para medir este control y esto se revisa y se mejora periódicamente.
A.13.2.2	Acuerdos de intercambio	L4	Hay definidas normas a seguir para realizar las transferencias de información de manera segura. Existe un indicador para comprobar la evolución de este control.
A.13.2.3	Mensajería electrónica	L4	La información incluida en mensajería electrónica está debidamente protegida. Existe un indicador para comprobar la evolución de este control.
A.13.2.4	Acuerdos de confidencialidad y secreto	L3	Existen acuerdos de confidencialidad con los empleados de la organización. Sin embargo, éstos no se revisan regularmente.
A.14	**ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN**		
A.14.1	**Requisitos de seguridad de los sistemas de información**		
A.14.1.1	Análisis y especificación de los requisitos de seguridad	L3	Se ha comprobado que se realizan análisis de requisitos a los sistemas de la organización. Sin embargo, faltan indicadores para comprobar la evolución de este control.
A.14.1.2	Seguridad de las comunicaciones en servicios accesibles por redes públicas	L3	Existen medidas implantadas para proteger las comunicaciones por redes públicas.

A.14.1.3	Protección de las transacciones por redes telemáticas	L3	Existen medidas implantadas para proteger las transacciones que se realicen por las redes de la organización.
A.14.2	**Seguridad en los procesos de desarrollo y soporte**		
A.14.2.1	Política de desarrollo seguro de software	L3	Existe un documento con la política de desarrollo de software seguro. Sin embargo, no existen indicadores para controlar la evolución de este control.
A.14.2.2	Procedimientos de control de cambios en los sistemas	L3	Existe un procedimiento de control de cambios para los desarrollos. Sin embargo, no existen indicadores para controlar que este procedimiento se está llevando a cabo correctamente.
A.14.2.3	Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo	L2	No existe un procedimiento a seguir tras haber realizado cambios en el sistema operativo de algún equipo de la organización. Es el empleado el que las realiza y no sigue ningún procedimiento, sino que realiza las pruebas que considera oportunas.
A.14.2.4	Restricciones a los cambios en los paquetes de software	L5	Existen controles para evitar la instalación de software indebido. Este control se mide a través de un indicador y se revisa y mejora periódicamente.
A.14.2.5	Uso de principios de ingeniería en protección de sistemas	L1	No existe un documento en el que se establezcan los principios de seguridad en ingeniería de sistemas. Sin embargo, la organización está al corriente de este problema y sabe que debe mejorar este control.
A.14.2.6	Seguridad en entornos de desarrollo	L3	Los entornos de desarrollo se encuentran protegidos adecuadamente con medidas de seguridad.
A.14.2.7	Externalización del desarrollo software	L0	No aplica
A.14.2.8	Pruebas de funcionalidad durante el desarrollo de los sistemas	L3	Se han definido en un documento las pruebas básica que se deben realizar a todo software para asegurar su seguridad. Sin embargo, no existen un indicador concreta para medir si está funcionando correctamente.
A.14.2.9	Pruebas de aceptación	L2	Se realizan pruebas a los sistemas. Sin embargo, no existe un documento formal que indique la metodología a seguir y cada empleado lo realiza cómo y cuándo le parece adecuado.
A.14.3	**Datos de prueba**		
A.14.3.1	Protección de los datos utilizados en pruebas	L3	Los datos utilizados en pruebas se encuentran protegidos.
A.15	**RELACIONES CON SUMINISTRADORES**		
A.15.1	**Seguridad de la información en las relaciones con suministradores**		
A.15.1.1	Política de seguridad de la información para suministradores	L3	Existen documentos en los que aparecen los acuerdos con los suministradores. Sin embargo, no existen indicadores para este control.

A.15.1.2	Tratamiento del riesgo dentro de acuerdos de suministradores	L3	Los requisitos de seguridad con los suministradores están establecidos en el acuerdo con éstos. Sin embargo, no existen indicadores para este control.
A.15.1.3	Cadena de suministro en tecnologías de la información y comunicaciones	L3	El acuerdo con los suministradores incluye los requisitos para abordar los riesgos de seguridad de la información asociados con la cadena de suministro de los servicios.
A.15.2	**Gestión de la prestación del servicio por suministradores**		
A.15.2.1	Supervisión y revisión de los servicios prestados por terceros	L4	La organización monitorea las conexiones con terceras partes y deja registros para comprobar su estado y evolución. Sin embargo, no se ha podido demostrar que se revise y/o mejore este proceso.
A.15.2.2	Gestión de cambios en los servicios prestados por terceros	L2	No existe un proceso formal de administración de cambios en los servicios prestados por los proveedores.
A.16	**GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN**		
A.16.1	**Gestión de incidentes de seguridad de la información y mejoras**		
A.16.1.1	Responsabilidades y procedimientos	L5	Las responsabilidades y los procedimientos para gestionar los incidentes de seguridad están documentados de manera adecuada. Además, existen métricas para controlar la evolución de los incidentes y procesos de mejora de estos procedimientos.
A.16.1.2	Notificación de los eventos de seguridad de la información	L3	Se ha comprobado que existe un procedimiento a seguir para notificar los incidentes de seguridad. Sin embargo, no existe un indicador con el que se pueda medir correctamente si este control se está llevando a cabo correctamente.
A.16.1.3	Notificación de puntos débiles de la seguridad	L4	Existe un procedimiento a seguir para notificar los puntos débiles de la seguridad de la organización. La evolución de este control se está midiendo con un indicador. Sin embargo, no se ha podido demostrar que se revise y/o mejore este proceso.
A.16.1.4	Valoración de eventos de seguridad de la información y toma de decisiones	L2	No existe un procedimiento formal para valorar y clasificar los incidentes de seguridad que surgen. Para ello, cada empleado encargado de tratar los incidentes utiliza su propio método de valoración.
A.16.1.5	Respuesta a los incidentes de seguridad	L5	Existe un procedimiento a seguir de actuación ante cualquier incidente de seguridad así como métricas para medir su evolución. Estos incidentes se revisan periódicamente y se mejoran.

A.16.1.6	Aprendizaje de los incidentes de seguridad de la información	L3	Existen una base de datos en la que se guarda la información de los incidentes ocurridos con el objetivo de aprender de ellos y mejorar la seguridad. Sin embargo, no existe ninguna métrica para comprobar que se está utilizando esta información con el fin expuesto.
A.16.1.7	Recopilación de las evidencias	L2	Se ha comprobado que algunos empleados recopilan las evidencias de los incidentes. Sin embargo, no todos lo hacen ni existe un documento formal que indique el procedimiento a llevar a cabo para este fin.
A.17	**ASPECTOS DE LA SEGURIDAD DE LA INFORMACIÓN EN LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO**		
A.17.1	**Continuidad de la seguridad de la información**		
A.17.1.1	Planificación de la continuidad de la seguridad de la información	L4	Existe un documento en el que se encuentra definido el plan de continuidad de negocio de la organización. Este documento se revisa y mejora periódicamente. Sin embargo, todavía no se ha revisado por primera vez por lo que no se puede afirmar que se encuentra en constante mejora.
A.17.1.2	Implantación de la continuidad de la seguridad de la información	L5	Se han implantado las medidas oportunas para asegurar la continuidad de negocio en caso de desastre. Se puede seguir la evolución de estas medidas gracias a la existencia de indicadores que sirven para mejorarlas constantemente.
A.17.1.3	Verificación, revisión y evaluación de la continuidad de la seguridad de la información	L4	Existe un plan de seguimiento y evaluación del plan de continuidad de negocio. Sin embargo, éste todavía no se ha llevado a cabo ninguna vez.
A.17.2	**Redundancias**		
A.17.2.1	Disponibilidad de instalaciones para el procesamiento de la información	L0	No aplica
A.18	**CUMPLIMIENTO**		
A.18.1	**Cumplimiento de los requisitos legales y contractuales**		
A.18.1.1	Identificación de la legislación aplicable	L5	Se ha comprobado que se revisa periódicamente la legislación vigente aplicable.
A.18.1.2	Derechos de propiedad intelectual (DPI)	L5	Se ha comprobado que existen procedimientos que garantizan el cumplimiento de los derechos de propiedad intelectual. Además, hay implantados indicadores para comprobar su funcionamiento y evolución y así mejorar este control.
A.18.1.3	Protección de los registros de la organización	L4	Los registros de la organización están debidamente protegidos, existiendo indicadores que así lo demuestran. Sin embargo, no se ha podido demostrar que se revise y/o mejore este proceso.

A.18.1.4	Protección de datos y privacidad de la información personal	L3	La información personal identificable está adecuadamente protegida y tratada de acuerdo a la legislación vigente. Sin embargo, no existe una métrica para comprobar su evolución.
A.18.1.5	Regulación de los controles criptográficos	L4	Existen controles criptográficos de acuerdo a la legislación vigente para proteger la información de la organización. También se dispone de un indicador para controlarlo. Sin embargo, no se ha podido demostrar que se revise este control.
A.18.2	**Revisiones de la seguridad de la información**		
A.18.2.1	Revisión independiente de la seguridad de la información	L5	Se ha realizado una revisión externa independiente del estado de la seguridad de la información de la organización de la que existen indicadores para comprobar su evolución. Además, este proceso se revisa y se mejora de manera periódica.
A.18.2.2	Cumplimiento de las políticas y normas de seguridad	L5	Se lleva a cabo la revisión de las políticas y normas de seguridad y se encuentran en constante mejora.
A.18.2.3	Comprobación del cumplimiento	L5	Se lleva a cabo la revisión del cumplimiento de las políticas y normas establecidas por la organización. Este proceso se revisa y mejora de manera periódica.

Tabla 44. Nivel de madurez de los controles ISO 27002:2013 en CEINTECO

A continuación, en la Tabla 45, se muestra el nivel de madurez de cada una de las secciones de la ISO 27001:2013 así como la justificación de cada nivel.

ID	Sección ISO 27001:2013	CCM	Justificación
4	**CONTEXTO DE LA ORGANIZACIÓN**		
4.1	Comprensión de la organización y de su contexto	L5	Se ha comprobad o que se la organización y su contexto han sido comprendidas adecuadamente.
4.2	Comprensión de las necesidades y expectativas de las partes interesadas	L5	Se ha comprobad o que se han determinado todas las necesidades y expectativas dentro y fuera de la organización que afectan al SGSI.
4.3	Determinación del alcance del SGSI	L5	El alcance ha sido definido correctamente.
4.4	SGSI	L5	La organización ha implantado correctamente un SGSI que está en proceso de mejora continua.
5	**LIDERAZGO**		
5.1	Liderazgo y compromiso	L5	Se ha comprobado que existe un gran compromiso por parte de la dirección en materia de seguridad de la información.
5.2	Política	L5	Existe definida una política de seguridad que está en constante mejora.

5.3	Roles, responsabilidades y autoridades en la organización	L5	Existe un documento en el que se definen los roles y responsabilidades de todos los empleados de la organización respecto a la seguridad de la información.
6	**PLANIFICACIÓN**		
A.6.1	**Acciones para hacer frente a los riesgos y oportunidades**		
6.1.1	General	L5	Se ha realizado un análisis de riesgos para identificar los activos y valorarlos, identificar las posibles amenazas, el impacto de éstas y el riesgo de cada uno de los activos identificados, todo esto siguiendo una metodología documentada.
6.1.2	Valoración de los riesgos de seguridad de la información	L5	Se ha realizado un análisis de riesgos que ha dado como resultado la valoración de los riesgos de la seguridad de la información de la organización.
6.1.3	Tratamiento de los riesgos de seguridad de la información	L4	Se han realizando proyectos para tratar los riesgos obtenidos. Sin embargo, puesto que el SGSI se acaba de poner en marcha, no se ha refinado al 100% este punto.
6.2	Objetivos de seguridad de la información y planificación para conseguirlos	L5	Los objetivos de seguridad de la información son claros en la organización y existe una planificación para mejorar la seguridad con el fin de conseguir dichos objetivos.
7	**SOPORTE**		
7.1	Recursos	L3	La disponibilidad de recursos es buena. Sin embargo, se puede mejorar.
7.2	Competencia	L4	Las competencias de cada uno están claramente definidas y se llevan a cabo correctamente. Sin embargo, puesto que el SGSI se acaba de poner en marcha, no se ha refinado al 100% este punto.
7.3	Concienciación	L4	Se ha logrado la concienciación en materia de seguridad de todos los empleados de la organización. Sin embargo, puesto que el SGSI se acaba de poner en marcha, no se ha refinado al 100% este punto.
7.4	Comunicación	L4	Existe una buena comunicación respecto a la seguridad de la información. Sin embargo, puesto que el SGSI se acaba de poner en marcha, no se ha refinado al 100% este punto.
7.5	**Información documentada**		
7.5.1	General	L2	Existe documentación de la información. Sin embargo, algunos de los procesos no están documentados formalmente.
7.5.2	Creando y actualizando	L2	Algunos de los documentos se actualizan periódicamente y se van creado nuevos, como documentos de pruebas. Sin embargo, no existe un procedimiento formal a seguir y cada empleados lo realiza a su manera.

7.5.3	Control de la información documentada	L2	Existe control de la información documentada., pero no de toda la información . No existe definida una manera clara de realizar el control de la información documentada referente a la seguridad de la información de la organización.
8	**OPERACIÓN**		
8.1	Planificación y control	L4	Las operaciones y los requisitos de seguridad están planificadas y controladas. Sin embargo, puesto que el SGSI se acaba de poner en marcha, no se ha refinado al 100% este punto.
8.2	Valoración de los riesgos de la seguridad de la información	L5	Se ha realizado un análisis de riesgos que ha dado como resultado la valoración de los riesgos de la seguridad de la información de la organización.
8.3	Tratamiento de los riesgos de la seguridad de la información	L4	Se han realizando proyectos para tratar los riesgos obtenidos. Sin embargo, puesto que el SGSI se acaba de poner en marcha, no se ha refinado al 100% este punto.
9	**EVALUACIÓN**		
9.1	Seguimiento, medición, análisis y evaluación	L4	Existe una planificación para llevar un seguimiento y evaluación del SGSI y se puede comprobar su evolución gracias a los controles implantados y los indicadores de dichos controles. Sin embargo, puesto que el SGSI se acaba de poner en marcha, no se ha refinado al 100% este punto.
9.2	Auditoría interna	L4	Existe un plan de realización de auditorías internas que ya se ha puesto en marcha y que se puede comprobar su evolución. Sin embargo, puesto que el SGSI se acaba de poner en marcha, no se ha refinado al 100% este punto.
9.3	Revisión por la dirección	L4	Existe planificado un plan de revisión del SGSI por la dirección y hay controles implantados respecto a este punto así como indicadores para comprobar su evolución. Sin embargo, puesto que el SGSI se acaba de poner en marcha, no se ha refinado al 100% este punto.
10	**MEJORA**		
10.1	No conformidad y acciones correctivas	L4	Se identifican no conformidades y las respectivas acciones correctivas para corregirlas cuando se realizan las revisiones y auditorías. Sin embargo, puesto que el SGSI se acaba de poner en marcha, no se ha refinado al 100% este punto.
10.2	Mejora continua	L4	Existe un proceso definido de mejora continua. Sin embargo, puesto que el SGSI se acaba de poner en marcha, no se ha refinado al 100% este punto.

Tabla 45. Nivel de madurez de los controles ISO 27002:2013 en CEINTECO

5.3.1. No conformidades con la norma ISO 27002:2013

A continuación, en la Tabla 46, se muestran las no conformidades (NC) con la norma ISO 27002:2013 encontradas durante la realización de la auditoría de cumplimiento así como las acciones correctivas recomendadas a seguir para mejorar el estado de los controles con no conformidades.

Control	Tipo de NC	Descripción	Acción correctiva recomendada
A.6.1.3	Menor	No existe documento formal que indique el procedimiento a seguir para contactar con las autoridades. Tampoco existe una programación para realizar dicho contacto.	Definir un procedimiento a seguir para contactar con las autoridades así como planificar el momento de los contactos.
A.6.1.4	Menor	No existe documento formal que indique el procedimiento a seguir para contactar con grupos de interés. Tampoco existe una programación para realizar dicho contacto.	Definir un procedimiento a seguir para contactar con los grupos de interés así como planificar el momento de los contactos.
A.6.2.2	Mayor	No existe un documento formal en el que se describan las normas a seguir para cuando se teletrabaja.	Definir un documento en el que se incluyan todas las normas a seguir cuando un empleado teletrabaje.
A.8.1.4	Mayor	Las normas a seguir para llevar a cabo la devolución de activos no es claro y no existe un indicador con el que se pueda controlar si estas normas se están cumpliendo.	Elaborar un nuevo documento con las normas bien explicadas e implantar un indicador para comprobar si la devolución de los activos se está realizando correctamente.
A.8.2.1	Mayor	No existe un documento en el que se indiquen los criterios a seguir para clasificar los activos.	Redactar un documento en el que se encuentren definidas las directrices de clasificación de los activos de la organización
A.8.2.2	Mayor	No están definidas en ningún sitio las directrices de etiquetado de los activos.	Redactar un documento con las directrices a seguir para el etiquetado de los activos. Revisar y mejorar las normas de tratamiento de la información.
A.8.3.1	Menor	No es posible conocer que se está aplicando correctamente el control.	Implantar un indicador para medir la evolución de este control
A.8.3.2	Mayor	No existe ningún procedimiento a seguir para llevar a cabo la eliminación de soportes extraíbles.	Implantar un procedimiento claro de eliminación de soportes extraíbles.
A.9.2.4	Mayor	No existe un documento en el que se defina cómo gestionar la información confidencial de autenticación de usuarios.	Redactar el documento en el que definan las normas referentes al uso de información confidencial en la autenticación de usuario.

A.9.2.5	Mayor	No existe un documento en el que se especifique cuándo ni cómo se revisan los derechos de acceso de los usuarios.	Redactar el documento en el que se incluya quién es el encargado de revisar los derechos de acceso de los usuarios, cada cuánto se lleva a cabo la revisión y cómo se realiza.
A.9.2.6	Mayor	No existe un documento en el que se explique el procedimiento a seguir para retirar o adaptar los derechos de acceso de los usuario.	Redactar el documento en el que se incluya quién es el encargado de modificar los derechos de acceso de los usuarios, en qué momento y cómo se realiza.
A.9.4.2	Menor	No existen indicadores para comprobar que los procedimientos seguros de inicio de sesión están funcionando correctamente.	Implantar indicadores para medir este control a lo largo del tiempo.
A.10.1.2	Menor	No existen indicadores para comprobar la evolución de la gestión de claves.	Implantar indicadores para medir este control a lo largo del tiempo.
A.11.1.5 A.11.1.6	Mayor	No existe un documento formal.	Redactar un documento formal para cada uno de estos controles e informar a todos los empleados de su existencia.
A.11.2.6	Mayor	No existe un documento en el que se especifiquen las medidas de seguridad a tomar para cuando se saca un activo fuera de las instalaciones de la organización.	Redactar el documento con las normas a seguir e informar a todos los empleados de estas normas.
A.12.1.1	Mayor	No existe un documento formal donde se encuentren documentados los procedimientos operativos.	Redactar un documento con los procedimientos de operación.
A.12.1.2	Mayor	No existe ningún proceso formal para controlar los cambios que afectan a la seguridad de la información de la organización.	Crear registros con los cambios que se vayan realizando.
A.12.1.3	Mayor	Falta de evidencias de que con los registros obtenidos de la monitorización se ajuste el uso de los recursos de los sistemas.	Implantar indicadores para comprobar el uso de los recursos de los sistemas.
A.12.6.1	Mayor	No existe un proceso para identificar las vulnerabilidades técnicas del software.	Implantar un proceso automático que identifique las vulnerabilidades del software existente.
A.13.1.1	Mayor	No existe un procedimiento a seguir ni ninguna planificación para realizar los controles de la red.	Planificar y ejecutar controles de red de manera periódica.
A.13.1.2	Mayor	No existen mecanismos de seguridad asociados a servicios de red.	Contratar una segunda conexión con otro proveedor para conseguir redundancia.

A.14.2.3	Mayor	No existe un procedimiento a seguir tras haber realizado cambias en el sistema operativo de algún equipo de la organización.	Establecer un procedimiento a seguir para cuando se realizan cambios en los sistemas operativos y realizarlo cada vez que se realiza un cambio en el sistema operativo de un equipo de la organización.
A.14.2.5	Mayor	No existe un documento en el que se establezcan los principios de seguridad en ingeniería de sistemas	Redactar un documento con los principios de seguridad en ingeniería de sistemas.
A.14.2.9	Mayor	No existe un documento formal que indique la metodología a seguir para realizar las pruebas de los desarrollos.	Redactar un documento con los pasos a seguir a la hora de realizar las pruebas necesarias a los desarrollos.
A.15.2.2	Mayor	No existe un proceso formal de administración de cambios en los servicios prestados por los proveedores.	Definir el proceso de administración de cambios en los servicios prestados por proveedores.
A.16.1.4	Mayor	No existen directrices para clasificar los incidentes de seguridad según su importancia o prioridad.	Definir los criterios de valoración de incidencias así como las directrices a seguir para clasificarlas de la manera más eficiente posible.
A.16.1.7	Mayor	No existe un documento en el que se especifique cuándo hay que recoger evidencias ni cómo se debe hacer.	Redactar un documento con el procedimiento a seguir para recopilar evidencias e informar a todos los empleados de este documento y de la importancia de la recopilación.

Tabla 46. No conformidades a la norma ISO 27002:2013

5.3.2. No conformidades con la norma ISO 27001:2013

A continuación, en la Tabla 47, se muestran las no conformidades (NC) con la norma ISO 27001:2013 encontradas durante la realización de la auditoría de cumplimiento así como las acciones correctivas recomendadas a seguir para mejorar el estado de las secciones con no conformidades.

Control	Tipo de NC	Descripción	Acción correctiva recomendada
7.1	Menor	La disponibilidad de recursos es mejorable.	Se debe mejorar la disponibilidad de los recursos de la organización.
7.5.1	Mayor	Algunos de los procesos no están documentados formalmente.	Documentar todos los procesos relacionados con la seguridad de la información que se lleven a cabo en la organización.
7.5.2	Mayor	No existe un procedimiento formal a seguir para la creación y actualización de documentos.	Definir un procedimiento a seguir para la creación y actualización de documentos.

7.5.3	Mayor	No existe definida una manera clara de realizar el control de la información documentada referente a la seguridad de la información de la organización.	Definir el procedimiento a seguir para realizar el control de la documentación.

Tabla 47. No conformidades a la norma ISO 27001:2013

5.4. Resultados

En este apartado se van a mostrar los resultados obtenidos en el apartado anterior en forma de gráficas.

En primer lugar, en la Imagen 23, se muestra el porcentaje de madurez de los controles ISO 27002:2013 implantados en CEINTECO.

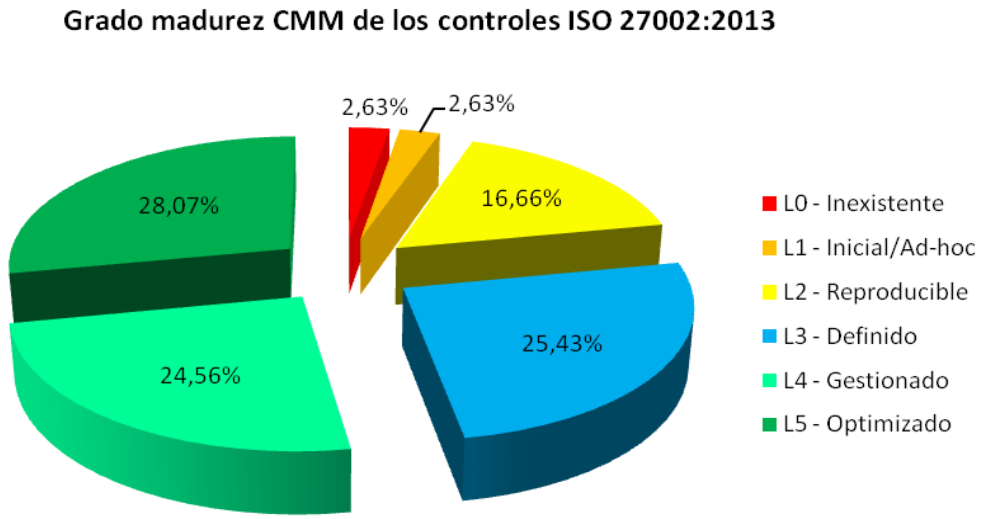


Imagen 23. Grado de madurez CMM de los controles ISO 27002:2013

En la Imagen 24, se muestra el porcentaje de madurez de las secciones de la ISO 27001:2013.

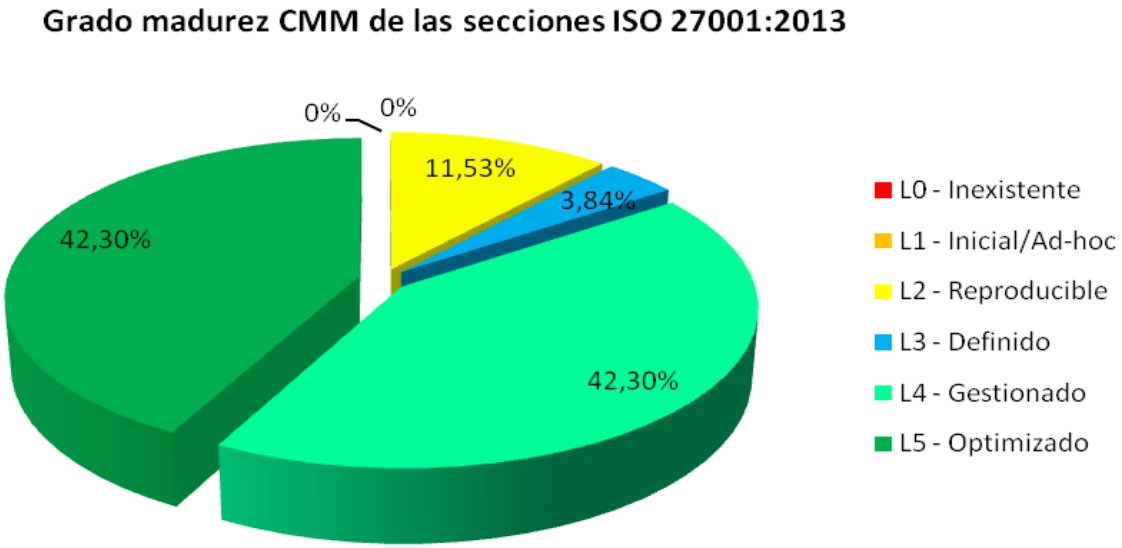


Imagen 24. Grado madurez CCM de las secciones ISO 27001:2013

Por otra parte, a partir de la Tabla 44 y conociendo la efectividad correspondiente a cada nivel CMM, se obtiene la Tabla 48, en la que se muestra el grado de madurez de cada uno de los controles y el total de cada uno de los dominios que forman parte de la ISO 27002:2013. Se observa que la efectividad de cada uno de los controles es significativamente mejor que la efectividad de dichos controles al inicio del proyecto.

Control ISO 27002:2013	**% Efectividad**
A.5 POLÍTICAS SEGURIDAD	100%
A.5.1 Directrices de la Dirección en seguridad de la información	100%
A.6 ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMACIÓN	73%
A.6.1 Organización interna	76%
A.6.2 Dispositivos para movilidad y teletrabajo	70%
A.7 SEGURIDAD LIGADA A LOS RECURSOS HUMANOS	96,1%
A.7.1 Antes de la contratación	95%
A.7.2 Durante la contratación	98,33%
A.7.3 Cese o cambio de puesto de trabajo	95%
A.8 GESTIÓN DE ACTIVOS	76,5%
A.8.1. Responsabilidad sobre los activos	86,25%
A.8.2 Clasificación de la información	78,3%
A.8.3 Manejo de los soportes de almacenamiento	65%
A.9 CONTROL DE ACCESOS	90%
A.9.1 Requisitos de negocio para el control de accesos	100%
A.9.2 Gestión de acceso de usuario	75%
A.9.3 Responsabilidades del usuario	90%
A.9.4 Control de acceso a sistemas y aplicaciones	95%
A.10 CIFRADO	92,5%
A.10.1 Controles criptográficos	92,5%
A.11 SEGURIDAD FÍSICA Y AMBIENTAL	88,3%
A.11.1 Áreas seguras	83,3%
A.11.2 Seguridad de los equipos	93,3%
A.12 SEGURIDAD EN LA OPERATIVA	88.15%
A.12.1 Responsabilidades y procedimientos de operación	63.3%
A.12.2 Protección contra código malicioso	100%
A.12.3 Copias de seguridad	100%
A.12.4 Registro de actividad y supervisión	96,25%
A.12.5 Control del software en explotación	95%
A.12.6 Gestión de la vulnerabilidad técnica	72,5%
A.12.7 Consideraciones de las auditorías de los sistemas de información	90%
A.13 SEGURIDAD EN LAS TELECOMUNICACIONES	73.3%

A.13.1 Gestión de la seguridad en las redes	51,6%
A.13.2 Intercambio de información con partes externas	95%
A.14 ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN	83,7%
A.14.1 Requisitos de seguridad de los sistemas de información	90%
A.14.2 Seguridad en los procesos de desarrollo y soporte	71.25%
A.14.3 Datos de prueba	90%
A.15 RELACIONES CON SUMINISTRADORES	80%
A.15.1 Seguridad de la información en las relaciones con suministradores	90%
A.15.2 Gestión de la prestación del servicio por suministradores	70%
A.16 GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN	82,1%
A.16.1 Gestión de incidentes de seguridad de la información y mejoras	82,1%
A.17 ASPECTOS DE LA SEGURIDAD DE LA INFORMACIÓN EN LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO	96,6%
A.17.1 Continuidad de la seguridad de la información	96,6%
A.17.2 Redundancias	0%
A.18 CUMPLIMIENTO	98%
A.18.1 Cumplimiento de los requisitos legales y contractuales	96%
A.18.2 Revisiones de la seguridad de la información	100%

Tabla 48. Grado de madurez de los controles ISO 27002:2013

A continuación, en la Imagen 25, se muestra el nivel de cumplimiento de cada dominio de la ISO 27002:2013 en un diagrama de radar del nivel obtenido tras realizar la auditoría de cumplimiento y el nivel objetivo planteado al principio del proyecto.

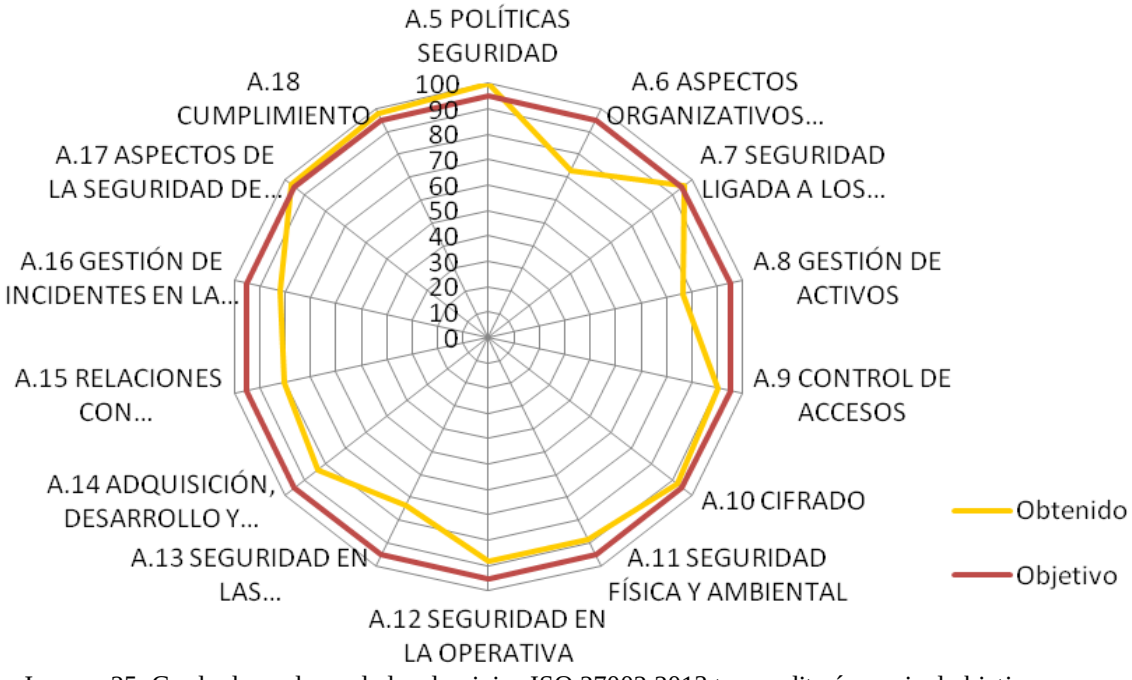


Imagen 25. Grado de madurez de los dominios ISO 27002:2013 tras auditoría vs nivel objetivo

Comparando el nivel de madurez obtenido con el nivel de madurez que se planteó como objetivo al inicio del proyecto, vemos que el nivel obtenido se aproxima al objetivo, incluso lo sobrepasa en algunos dominios. Sin embargo, para otros dominios aún quedan mejoras que hacer para llegar al objetivo fijado.

A continuación se va a mostrar la evolución de la madurez de los controles desde su estado inicial hasta el estado en el que se encuentran tras la realización de la auditoría de cumplimiento.

Esta evolución se puede apreciar en la Imagen 26, donde se han dibujado sobre el mismo diagrama de radar el estado inicial de los controles (azul), el estado objetivo propuesto (rojo), el estado óptimo (verde), el estado esperado tras la aplicación de los proyectos de la fase 4 (morado) y el estado obtenido tras la finalización de la auditoría de cumplimiento (naranja).

Vemos que, en general, el estado obtenido de la mayoría de los dominios tras la auditoría es similar al esperado tras la realización de los proyectos. Asimismo, volvemos a observar que hay que seguir trabajando en la mejora de algunos dominios para conseguir alcanzar el objetivo fijado al principio de este proyecto.

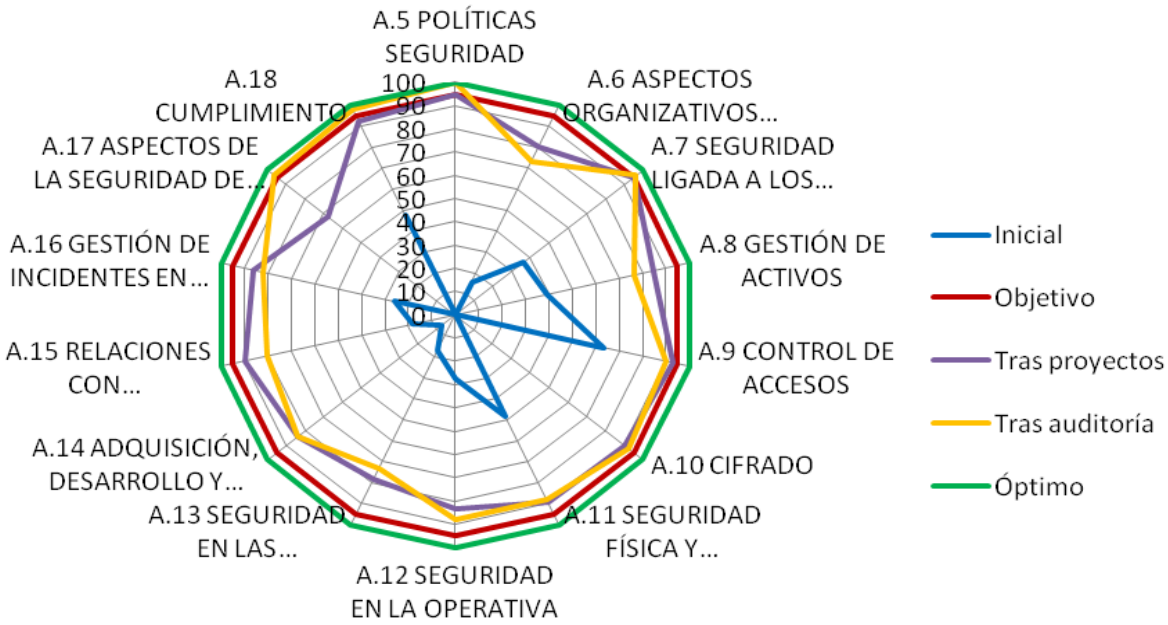


Imagen 26. Evolución del estado de los controles ISO 27002:2013

En la Tabla 49 se muestra el grado de madurez de cada una de las secciones que forman parte de la ISO 27001:2013. Estos datos se han obtenido a partir de la Tabla 45 y de la efectividad de los niveles CCM. Se observa que la efectividad de cada una de las secciones es significativamente mejor que la efectividad de dichas secciones al inicio del proyecto.

Sección ISO 27001:2013	% Efectividad
4. CONTEXTO DE LA ORGANIZACIÓN	100%
5. LIDERAZGO	100%
6. PLANIFICACION	98,75%
7. SOPORTE	75%
8. OPERACIÓN	96,6%
9. EVALUACION	95%
10. MEJORA	95%

Tabla 49. Grado de madurez de las secciones ISO 27001:2013

A continuación, en la Imagen 27, se muestra el nivel de cumplimiento obtenido de cada sección de la ISO 27001:2013 de cada sección de la ISO 27001:2013 tras realizar la auditoría de cumplimiento(naranja) comparado con el estado inicial al empezar el proyecto (azul), el estado objetivo (rojo) y el estado óptimo (verde).

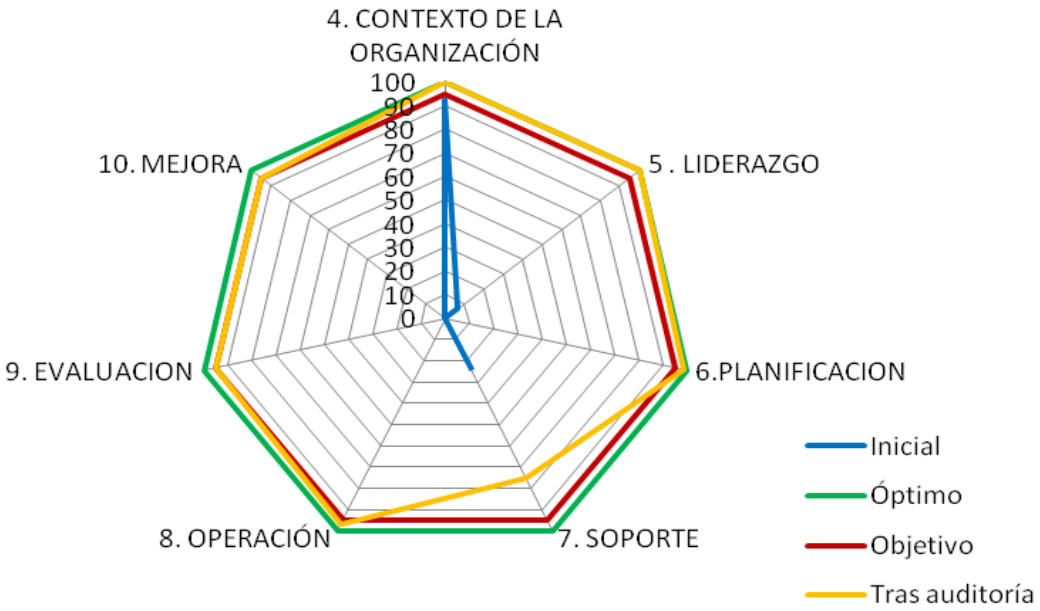


Imagen 27. Evolución del estado de las secciones ISO 27001:2013

Observamos que el estado obtenido de la ISO 27001:2013 es my similar al objetivo que se planteó al principio del proyecto, incluso en algunas secciones es superior al objetivo planteado. También podemos observar, que para la sección 7-Soporte no se ha conseguido llegar al objetivo planteado y, por tanto, habrá que trabajar en mejorar dicha sección.

6. Fase 6: Conclusiones

6.1. Introducción

Tras haber realizado con éxito todas las fases anteriores, se puede concluir que se han cumplido los objetivos propuestos al inicio de este proyecto, es decir, mejorar la seguridad de la información de la organización gracias a la implementación de un Plan de Seguridad.

6.2. Objetivos conseguidos

Se ha establecido el estado inicial de la seguridad de la información de la organización así como los objetivos a alcanzar tras la implantación del SGSI.

Se ha definido y desarrollado el esquema documental necesario para el cumplimiento normativo de la ISO 27001:2013.

Se ha realizado el análisis de riesgos de la organización del que se ha obtenido la lista de todos los activos de la empresa, las amenazas posibles a las que está expuesta la organización así el impacto y el riesgo de todos los activos de la empresa que ha permitido identificar los activos más prioritarios en cuanto a seguridad de la información.

Se han definido y completado con éxito una serie de proyectos para mejorar la seguridad de la información de la organización, teniendo en cuenta al análisis de riesgos obtenido.

Se ha evaluado el nivel de madurez de la seguridad de la información de la organización respecto a la norma ISO 27002:2013.

Se ha conseguido reducir el riesgo de los activos de la organización.

Tras la realización de todas las fases, se ha conseguido mejorar significativamente el estado inicial de la seguridad de la información de la organización.

Se ha logrado la concienciación y colaboración de los empleados en materia de seguridad de la información.

Existe el compromiso de revisar y mejorar el estado de la seguridad de la información de la organización de manera periódica.

6.3. Trabajo futuro

Se deben implantar las mejoras propuestas en la fase de auditoría de cumplimiento.

Una vez implantadas las mejoras propuestas se deberá intentar conseguir la certificación ISO 27001:2013 como se planteó al inicio del proyecto.

Se debe seguir trabajando en la mejora del estado de la seguridad de la información de la organización con el objetivo de alcanzar el estado óptimo. Para ello, se deberán plantear nuevos proyectos para mejorar los controles que están menos maduros.

Como se ha establecido en el Plan de Seguridad, se deben realizar revisiones periódicas al sistema de seguridad de la información de la organización.

Como se ha establecido en el Plan de Seguridad, se deben realizar auditorías periódicas al sistema de seguridad de la información de la organización.

7. Glosario

Acción correctiva: Acción para eliminar la causa de una no conformidad y prevenir su repetición. Va más allá de la simple corrección.

Activo: Cualquier información o elemento relacionado con el tratamiento de la misma (sistemas, soportes, edificios, personas...) que tenga valor para la organización.

Alcance: Ámbito de la organización que queda sometido al SGSI.

Amenaza: Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización.

Análisis de riesgos: Proceso para comprender la naturaleza del riesgo y determinar el nivel de riesgo.

Auditor: Persona encargada de verificar, de manera independiente, el cumplimiento de unos determinados requisitos.

Auditoría: Proceso sistemático, independiente y documentado para obtener evidencias de auditoría y evaluarlas objetivamente para determinar el grado en el que se cumplen los criterios de auditoría.

Autenticación: Provisión de una garantía de que una característica afirmada por una entidad es correcta.

Confidencialidad: Propiedad de la información de no ponerse a disposición o ser revelada a individuos, entidades o procesos no autorizados.

Control: Las políticas, los procedimientos, las prácticas y las estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido.

Declaración de aplicabilidad: Documento que enumera los controles aplicados por el SGSI de la organización y su justificación, así como la justificación de las exclusiones de controles.

Desastre: Cualquier evento accidental, natural o malintencionado que interrumpe las operaciones o servicios habituales de una organización durante el tiempo suficiente como para verse la misma afectada de manera significativa.

Directriz: Una descripción que clarifica qué debería ser hecho y cómo, con el propósito de alcanzar los objetivos establecidos en las políticas.

Disponibilidad: Propiedad de la información de estar accesible y utilizable cuando lo requiera una entidad autorizada.

Evidencia: Información, registro o declaración de hechos, cualitativa o cuantitativa, verificable y basada en observación, medida o test, sobre aspectos relacionados con la confidencialidad, integridad o disponibilidad de un proceso o servicio o con la existencia e implementación de un elemento del sistema de gestión de seguridad de la información.

Impacto: El coste para la empresa de un incidente, que puede o no ser medido en términos estrictamente financieros.

Incidente: Evento único o serie de eventos de seguridad de la información inesperados o no deseados que poseen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información.

ISO/IEC 27000: Revisión de los estándares de la serie 27000.

ISO/IEC 27001: Especificaciones para la implantación de un Sistema de Gestión de la Seguridad de la Información (SGSI).

ISO/IEC 27002: Código de buenas prácticas en la gestión de la seguridad de la información.

Integridad: Propiedad de la información relativa a su exactitud y completitud.

Inventario de activos: Lista de todos aquellos recursos (físicos, de información, software, documentos, servicios, personas, intangibles, etc.) dentro del alcance del SGSI, que tengan valor para la organización y necesiten ser protegidos de potenciales riesgos.

MAGERIT: Metodología de Análisis y Gestión de Riesgos de los sistemas de información elaborada por el Consejo Superior de Administración Electrónica.

PDCA (plan-do-check-act): Método de mejora continua de la calidad. También conocido como ciclo Deming.

No repudio: Servicio de seguridad que previene que un emisor niegue haber remitido un mensaje (cuando realmente lo ha emitido) y que un receptor niegue su recepción (cuando realmente lo ha recibido).

Objetivo: Declaración del resultado o fin que se desea lograr mediante la implementación de procedimientos de control en una actividad determinada.

Plan de continuidad de negocio: Plan orientado a permitir la continuación de las principales funciones del negocio en el caso de un evento imprevisto que las ponga en peligro.

Proceso: Conjunto de actividades que transforman unas entradas en salidas.

Riesgo: Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información.

Riesgo residual: El riesgo que permanece tras el tratamiento del riesgo.

Salvaguarda: Mecanismo de protección frente a las amenazas. Existen diferentes tipos dependiendo si se desea prevenir o corregir un incidente.

Segregación de tareas: Reparto de tareas sensibles entre distintos empleados para reducir el riesgo de un mal uso de los sistemas e informaciones deliberado o por negligencia.

Seguridad de la información: Preservación de la confidencialidad, integridad y disponibilidad de la información.

Selección de controles: Proceso de elección de los controles que aseguren la reducción de los riesgos a un nivel aceptable.

SGSI: Sistema de Gestión de Seguridad de la Información. Conjunto de elementos que utiliza una organización para establecer una política y unos objetivos de seguridad de la información y alcanzar dichos objetivos, basándose en un enfoque de gestión del riesgo y de mejora continua.

Tratamiento de riesgos: Proceso de modificar el riesgo, mediante la implementación de controles.

Trazabilidad: Cualidad que permite que todas las acciones realizadas sobre la información o un sistema de tratamiento de la información sean asociadas de modo inequívoco a un individuo o entidad.

Vulnerabilidad: Debilidad de un activo o control que puede ser explotada por una amenaza.

8. Bibliografía

- *Materiales asignatura del MISTIC, Sistemas de Gestión de la Seguridad.*
- *Materiales asignatura del MISTIC, Auditoría Técnica.*
- *http://www.iso27000.es*
- *http://www.pmg-ssi.com/2014/11/iso-270012015-un-cambio-en-la-integracion-de-los-sistemas-de-gestion/*
- *http://www.criptored.upm.es/descarga/NuevasVersionesISO27001eISO27002.pdf*
- *http://recursostic.educacion.es/observatorio/web/ca/software/software-general/1040-introduccion-a-la-seguridad-informatica?start=1*
- *http://www.magazcitum.com.mx/?p=2397#.VtLbXfnhDIU*
- *https://www.isotools.org/normas/riesgos-y-seguridad/iso-27001*
- *http://docplayer.es/12774237-Modelos-de-madurez-para-sgsi-desde-un-enfoque-practico.html*
- *http://www.network-sec.com/gobierno-TI/auditoria-CMM*
- *https://prezi.com/medejvc1z6sq/cmm-modelo-de-capacidad-de-madurez/*
- *https://www.incibe.es/empresas/que_te_interesa/Plan_director_de_seguridad*
- *https://www.incibe.es/blogs/post/Empresas/BlogSeguridad/Articulo_y_comentarios/mide_seguridad_informacion*
- *http://www.mintic.gov.co/gestionti/615/articles-5482_Controles.pdf/*
- *http://www.pmg-ssi.com/2014/12/iso-27001-auditorias-internas-del-sgsi/*
- *http://birdconsultoria.com/revision-por-la-direccion-en-la-iso/*
- *http://blog.firma-e.com/nueva-version-iso-270012013-analisis-detallado-parte-1-de-4/*
- *http://blog.firma-e.com/iso-270012013-analisis-detallado-de-la-nueva-version-parte-2-de-4/*
- *http://blog.firma-e.com/iso-270012013-analisis-detallado-de-la-nueva-version-parte-3-de-4/*
- *http://blog.firma-e.com/iso-270012013-analisis-detallado-de-la-nueva-version-parte-4-de-4/*
- *http://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html#.VwkAsvmLTIU*