Escuela Politécnica Superior

Plan para la implementación de un SGSI en un centro educativo

Grado en Ingeniería Informática

Trabajo Fin de Grado

Autor:
Carlos Pérez Serrano

Tutor/es:
José Vicente Berna Martínez

Universitat d'Alacant
Universidad de Alicante

Junio 2019

Resumen

A lo largo de este trabajo se han llevado a cabo las tareas necesarias para implantar un Sistema de Gestión de la Seguridad de la Información en un centro educativo concertado de la ciudad de Alicante.

Para ello, se ha seguido el marco propuesto por la metodología MAGERIT para la gestión de riesgos en los Sistemas de Información, orientado a cubrir las necesidades planteadas por la normativa ISO 27000.

En el presente documento se presentan los conceptos principales de los Sistemas de Información y se detallan los procesos realizados para la creación del catálogo de activos, la identificación de amenazas, el proceso de la gestión del riesgo y la evaluación de salvaguardas.

Por último, con los resultados obtenidos de este proceso de análisis, se explica en detalle cómo se ha llevado a cabo la creación de los programas y planes de seguridad para asegurar el Sistema de Información del centro educativo.

Además de lo explicado en el documento, se adjuntan un documento anexo que será el que una vez finalizado el trabajo se entregará al colegio con los resultados de todos los procesos mencionados previamente para que puedan ser aplicados y mejorar la seguridad de la información del centro.

Motivación, justificación y objetivo general

Hoy en día vivimos en una sociedad digital y estamos permanentemente conectados con acceso a Internet desde prácticamente cualquier dispositivo. Y aunque esto nos ofrece un amplio abanico de posibilidades, no siempre estamos preparados para hacer frente a esta realidad.

Están a la orden del día las noticias sobre brechas de seguridad, robo de datos o pérdidas de información y muchas de estas situaciones vienen provocadas debido a un mal uso de las tecnologías de información o al desconocimiento sobre estas.

Si bien en España hay numerosas empresas que han realizado un fuerte esfuerzo para ponerse al día en estas cuestiones y ser *Empresas 3.0*, una inmensa mayoría de pequeñas empresas u organizaciones, o bien no han decidido dar el salto a esa digitalización o lo han hecho sin ser conscientes de las consecuencias que ello conlleva.

De esta realidad surge la idea de este proyecto. En él se pretende abordar el concepto de los Sistemas de Gestión de la Seguridad de la Información basado en las normas ISO 27000, e implantar este sistema en un centro educativo. Para ello se realizará un análisis del contexto de la organización, se realizará una evaluación de riesgos e identificación de recursos y se fijarán los objetivos pertinentes para el SGSI.

Este proyecto me permitirá aplicar conceptos estudiados durante el grado de Ingeniería Informática, como conceptos básicos en Seguridad de la Información o sobre análisis y evaluación de riesgos. Además, me permitirá utilizarlos en una empresa real que me permita tener una visión más cercana de la situación actual en las empresas con respecto a la seguridad Informática.

Agradecimientos

A mi familia, por la educación que me ha hecho ser quien soy.

A mi pareja, por darme el ánimo que a veces no tenía.

A aquellos amigos que fueron, son y serán.

Citas

"La prueba del éxito de la educación no es lo que un muchacho sabe según los exámenes al salir del colegio, sino lo que está haciendo diez años más tarde."

Robert Baden Powell

"Aprender a volar es todo un arte. Aunque solo hay que cogerle el truco, consiste en tirarse al suelo y fallar."

Guía del autoestopista galáctico (1979). Douglas Adams

Índice de contenido

Índice de tablas

Índice de figuras

Índice de Ilustraciones

1. Introducción

En los últimos años con la capacidad de acceder a Internet desde prácticamente cualquier dispositivo electrónico, el auge de los servicios en la nube y el creciente conocimiento sobre las nuevas tecnologías, muchas son las empresas que han decidido dar un paso hacia la digitalización.

Evidentemente las empresas del sector tecnológico fueron las primeras en abordar este cambio. Sin embargo, tras estas, un enorme número de organizaciones decidieron seguir sus pasos y apostar por la digitalización de la información, el marketing digital, la movilización, la ciberseguridad e incluso ofrecer servicios a través de internet.

De hecho, observando el informe *Integration of Digital Technology by Enteprise* [1] elaborado por la Comisión Europea y que mide, entre otras cosas, el nivel de digitalización de las empresas, se observa una tendencia al alza medida en 4 factores: La información compartida a través de medios digitales, la recuperación de datos remotos mediante la tecnología RFID, el uso de redes sociales y de dispositivos electrónicos.

Si bien esta tendencia hacia la digitalización es evidente en toda Europa, España no está todavía a la vanguardia de este cambio. De hecho en ese mismo estudio, y tal y como se observa en la Figura1, se sitúa a España en el 7º puesto en esta cuestión (Por delante de Eslovenia y Lituania) y en el *Informe Bankia Índicex 2016: La digitalización en España* [2] la nota media de digitalización de las empresas en España, siguiendo diferentes factores como el posicionamiento SEO, la movilidad, la seguridad etc, es de 5 puntos en una escala de 10.

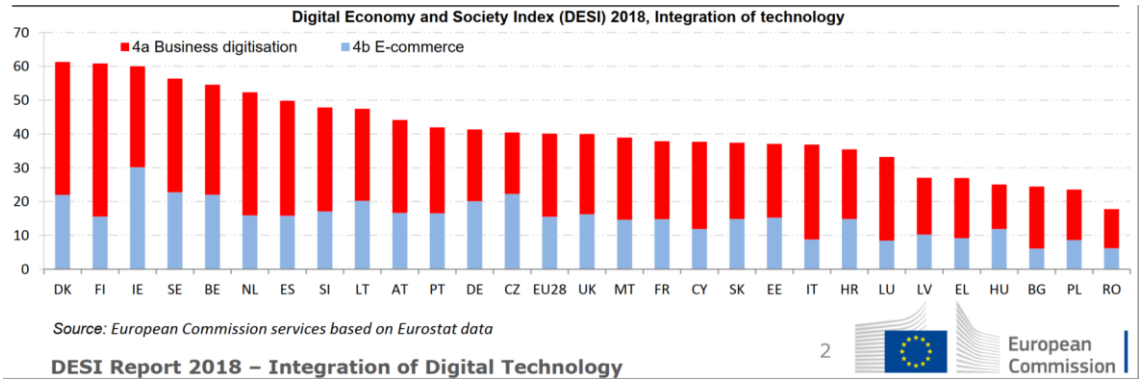

Figura 1. Niveles de integración de la tecnología en las empresas
Fuente: Integration of Digital Technology by Enterprise

Y aunque en España falte mucho para igualarse a otros países europeos en diferentes aspectos relacionados con la digitalización, es cada vez más frecuente que las empresas basen sus sistemas de información en nuevas tecnologías. De esta forma, si bien aún es posible encontrar empresas y organizaciones que basan su sistema de información en soportes físicos como cuadernos, archivadores y numerosas anotaciones en papel, esto es cada vez menos común. Actualmente la mayor parte de la información reside en equipos informáticos, redes de datos y soportes de almacenamiento.

Estos nuevos sistemas de información basados en el uso de las nuevas tecnologías tienen una enorme cantidad de virtudes y ofrecen multitud de posibilidades. Sin embargo, están sujetos a riesgos y amenazas, tanto desde el exterior como desde la propia organización. Estos riesgos pueden ser o bien riesgos físicos que pueden conllevar la perdida de información y recursos, o bien riesgos lógicos relacionados con la propia tecnología (Hackeos, robo de información y ataques informáticos entre muchos otros).

Debido a este contexto y a que la información es un activo valioso del que muchas veces depende el buen funcionamiento del negocio, o incluso es el pilar en el que se basa el modelo de negocio de una empresa, surge la necesidad de proteger esta información, mantener su integridad, disponibilidad y confidencialidad.

Es en este punto donde surgen los Sistemas de Gestión de la Seguridad de la Información.

El organismo ISO, *International Organization for Standardization,* es un organismo no gubernamental con reconocimiento a nivel mundial que busca la creación de estándares para la resolución de problemas a nivel global. En su familia de normativas ISO-27000, donde aborda la seguridad de la información, propone los Sistemas de Gestión de la Seguridad de la Información (a partir de ahora SGSI) como una herramienta o metodología sencilla de utilizar por cualquier empresa independientemente de su tamaño y que permita establecer normas, procedimientos y controles para disminuir los riesgos de una organización en el campo del sistema de información.

Las normativas ISO no son obligatorias por ley tal, y como recoge el propio organismo en su página web [3]: *"Like other ISO management system standards, certification to ISO/IEC 27001 is possible but not obligatory*". Sin embargo, para una empresa es muy conveniente aplicar estas normativas, en este caso la familia 27000. En primer lugar, porque permite que la gestión de la seguridad del sistema de información pase de ser un conjunto de tareas aisladas a un sistema con un ciclo de vida controlado en el que participa toda la organización. Y en segundo lugar porque si bien no es un requerimiento legal, el cumplimiento de estas normativas permite

diferenciar a una empresa entre la competencia y asegurar a clientes y proveedores que se siguen una serie de controles para afianzar la seguridad de la empresa.

Los SGSI son un pilar fundamental para asegurar el correcto funcionamiento del sistema de información de una organización. Por eso, empresas y organizaciones de cualquier ámbito dedican numerosos esfuerzos en desarrollar un sistema que se encargue de la protección y la seguridad de su información.

El siguiente trabajo, consistirá en el desarrollo de un Sistema para la Gestión de la Seguridad de la Información para un centro educativo concertado de la ciudad de Alicante.

Los centros educativos, como cualquier otra organización en la que participan varios cientos de personas generan un gran volumen de información, tanto en tareas relacionadas con la administración del centro como en cuestiones educativas y pedagógicas. Esto hace que tengan las mismas necesidades de protección que otras organizaciones a la hora de asegurar la disponibilidad, integridad y confidencialidad de los datos que manejan.

Para realizar este trabajo se analizará el contexto del centro para determinar la situación actual de su sistema de información, se realizará un catálogo de activos y se analizarán las posibles amenazas que puedan perjudicar a esos activos. Tras esto se hará un análisis de riesgos que permitirá establecer una serie de controles y medidas de seguridad con el objetivo de intentar afianzar la seguridad de los elementos del sistema de información.

2. Planificación

La elaboración de este trabajo de fin de grado comienza la primera semana de octubre de 2018. En este apartado se intentará realizar una planificación temporal del proyecto teniendo en cuenta los apartados a realizar y una estimación del tiempo requerido para llevar a cabo estos apartados.

A continuación, se especifica una tabla con las diferentes etapas del proyecto y su estimación temporal. Estas están agrupadas en diferentes fases teniendo en cuenta tanto mi disponibilidad para realizar el trabajo como la disponibilidad del centro educativo para poder llevar a cabo el análisis del mismo.

Contenidos	Fecha límite fin
Motivación, justificación y objetivo general Introducción	20 de octubre
Estado del arte	13 de enero
Análisis de la organización Objetivos y propuesta	17 de febrero
Catálogo de activos Listado de amenazas	17 de marzo
Evaluación y gestión de riesgos	21 de abril
Elaboración de planes de seguridad	12 de mayo

Tabla 1. Planificación temporal TFG

Debido al carácter metodológico y teórico del trabajo, en la planificación no se tendrán en cuenta etapas habituales en otros proyectos relacionados con la ingeniería informática como el diseño, la implementación o la validación.

Sin embargo, tendrán una gran importancia en el proyecto otras fases como “Análisis de la organización”, dónde se realizará un análisis de la realidad del centro, o las fases más enfocadas a la consecución de los objetivos del trabajo, como la elaboración del catálogo de activos y de amenazas, la gestión de riesgos o la creación de los planes de seguridad.

3. Estado del arte.

3.1. Sistemas de gestión de la seguridad

La Asociación Española para la Calidad define así la seguridad de la información:

"La Seguridad de la información tiene como fin la protección de la información y los sistemas de información del acceso, uso, divulgación, interrupción o destrucción no autorizada" [4]

Actualmente todas las empresas, independientemente de su tamaño o su sector de actividad, procesan y almacenan una gran cantidad de información, y tanto esta como los sistemas y procesos que interactúan con estos datos son importantes activos para las ellas. Es precisamente por esto, que la seguridad de la información es un pilar fundamental para el buen funcionamiento de la empresa, para cumplir la legislación referente a esta cuestión y para evitar una gran cantidad de riesgos inherentes al manejo de datos.

Debido a la importancia de proteger estos activos, la seguridad de la información no puede basarse en tareas aisladas. Esta debe ser parte de un sistema que esté regulado, con ciclos de vida periódicos, diseñado expresamente para involucrar a toda la organización y que sea evaluable para asegurar su continuo desarrollo y mejora. Es aquí donde se enmarcan los Sistemas de Gestión de la Seguridad de la Información.

Según la norma española UNE-ISO/IEC 27000[**¡Error! No se encuentra el origen de la r eferencia.**] *"Un SGSI (Sistema de Gestión de la Seguridad de la Información) proporciona un modelo para establecer, implementar, operar, monitorizar, revisar, mantener y mejorar la protección de los activos de información para alcanzar los objetivos de negocio, basado en una apreciación del riesgo y en los niveles de aceptación…"*

Según esta definición, un SGSI es un sistema de gestión, lo que implica llevar a cabo una serie de tareas que permitan dirigir y controlar los procesos llevados a cabo en los diferentes niveles de la organización. Para implementar un SGSI es importante que el conjunto de la organización esté involucrado.

Además, según la definición, el objetivo principal de un SGSI es proteger los activos de información. En este caso se puede entender el objetivo de esa protección como asegurar la confidencialidad, disponibilidad e integridad de los activos de información. Para esto es imprescindible llevar a cabo una correcta gestión de las tecnologías de la información y la

comunicación utilizadas en el sistema, así como de los procesos y el personal que intervienen en el mismo.

3.2. Normativas ISO

En el año 1901 surge, como la primera entidad normalizadora a nivel mundial, la BSI (*British Standards Institution*) y en el año 1995 aparece la normativa BS 7799. Esta, recoge una serie de buenas prácticas para la gestión de los sistemas de información en las empresas y los requisitos que debería tener un SGSI para ser certificable por una entidad independiente.

Estas normas fueron revisadas por la organización ISO y en el año 2005 y fueron adoptadas por esta organización como las normativas ISO 27001 e ISO 27002.

Desde ese momento y en un periodo de tiempo entre los años 2005 y 2011 surgen todas las normativas de las familias 27000 entre las que, puesto que serán a las que más se haga referencia en el presente documento, se destacan las siguientes:

Normativa	Descripción
ISO/IEC 27000	*Visión de conjunto y vocabulario*. Proporciona una visión general de las normas de la familia 27000 y describe los fundamentos y puntos clave de los SGSI.
ISO/IEC 27001	*Requisitos*. *"…establece los requisitos normativos para el desarrollo y operación de un SGSI, incluyendo un conjunto de controles para el control y mitigación de los riesgos asociados con los activos de información que la organización trata de proteger mediante la operación de su SGSI". [5]*
ISO/IEC 27002	*Código de buenas prácticas para la gestión de la seguridad de la información. "…proporciona una lista de objetivos de control comúnmente aceptados, así como las mejores prácticas en controles de seguridad".* [5]
ISO/IEC 27003	*Guía de implementación de un SGSI. "Esta norma internacional proporciona orientación para la implementación práctica e información adicional para establecer, implementar, operar, supervisar, revisar, mantener y mejorar un SGSI…".* [5]

Tabla 2. Familia ISO 27000 – Normas principales

3.3 Importancia de la gestión de riesgos

Para llevar a cabo un Sistema de Gestión de la Seguridad de la Información, tal y como se explica en la normativa ISO 27002, es esencial que una organización identifique sus requisitos de seguridad. Estos requisitos de seguridad se obtienen de tres fuentes diferentes: En primer lugar, los objetivos y requisitos de negocio, que marcarán el nivel de seguridad necesario en la organización. En segundo lugar, los requisitos legales o contractuales necesarios para cumplir con la normativa vigente o con los acuerdos contractuales con los clientes de la organización. Y, por último, la evaluación de los riesgos de la información que conforma otra fuente fundamental para determinar los requisitos de seguridad.

El proceso de evaluación de riesgos se define como una fuente fundamental para la obtención de requisitos de la seguridad. En la ISO 27002 [6] este proceso está definido de la siguiente manera: *"… teniendo en cuenta los objetivos y estrategia de negocio globales de la organización y a través de una evaluación de los riesgos, se identifican las amenazas de los activos, se evalúa la vulnerabilidad y la probabilidad de su ocurrencia y se estima su impacto potencial… Los resultados de la evaluación de riesgos ayudarán a guiar y determinar las acciones de gestión más adecuadas y las prioridades para la gestión de los riesgos de seguridad, así como para la implantación ellos controles seleccionados para protegerse contra esos riesgos"*. Para comprender esta definición a continuación se describen algunos de los elementos principales en el proceso de evaluación de riesgos.

3.3.1 Activos

En el ámbito de los sistemas de información, la UNE 71504, define un activo como "Componente o funcionalidad de un sistema de información que tiene algún valor para la organización y es susceptible de ser atacado deliberada o accidentalmente".

De cara a la gestión de riesgos es necesario desarrollar un catálogo de activos y para ello, identificar los activos esenciales para una organización, que son aquellos cuya falta pondría en riesgo la supervivencia de la organización. Además, se tendrán en cuenta también otros activos referentes a la arquitectura del sistema, la información manejada por la organización, el personal de la misma o los servicios ofrecidos.

3.3.2 Amenazas

Según la norma UNE 71504 [7] es posible definir amenaza como "*Causa potencial de un incidente que puede causar daños a un sistema de información o a una organización*".

Si antes se describía los activos de una empresa como los elementos que generan valor en la misma, las amenazas podrían definirse como sucesos que potencialmente pueden afectar negativamente a estos activos, reduciendo su valor y causando daño a la organización.

Las amenazas que puedan afectar a una organización pueden tener un origen externo a esta o bien provenir del interior de la propia organización. Además, es posible distinguir amenazas de muy diverso origen, como desastres naturales, acciones llevadas a cabo de forma accidental por personal interno o externo e incluso ataques intencionados contra una organización o empresa.

3.3.3 Impacto

El impacto se define como la gravedad de las consecuencias de una potencial amenaza sobre un activo en una organización. El impacto tiene un papel fundamental en el análisis de riesgos, puesto que marcará los esfuerzos para proteger un determinado activo o para evitar una potencial amenaza.

Para el análisis de riesgos, este impacto no puede calcularse de una manera empírica, pero existen dos relaciones que permiten determinar el impacto de una amenaza concreta.

En primer lugar, es posible calcular el impacto como una relación de valor-degradación. En este caso para una potencial amenaza se determina el valor del activo al que afecta y el nivel de degradación del valor que supondría esta amenaza sobre ese activo. De esta manera estableceremos como impacto muy alto aquellas amenazas que supongan una alta degradación sobre activos con alto valor y un impacto bajo aquellas amenazas que supongan una degradación pequeña sobre activos de bajo valor.

		Degradación		
		1%	**10%**	**100%**
Valor	**Muy Alto**	Medio	Alto	Muy Alto
	Alto	Bajo	Medio	Alto
	Medio	Muy Bajo	Bajo	Medio
	Bajo	Muy Bajo	Muy Bajo	Bajo
	Muy Bajo	Muy Bajo	Muy Bajo	Muy Bajo

Tabla 3. Matriz para la estimación del impacto
Fuente: MAGERIT I

Además, de la definición anterior se puede utilizar el impacto como una medida que permita calcular el riesgo que conlleva una potencial amenaza. Para ello, teniendo en cuenta la gravedad del efecto causado por esta amenaza y la probabilidad de que ocurra, se identificará un riesgo crítico en aquellas amenazas que generen un alto impacto con una probabilidad alta y se entenderá como riesgo asumible el producido por amenazas poco probables que no generen un gran impacto.

Riesgo		**Probabilidad**				
		Muy raro	**Poco probable**	**Posible**	**Probable**	**Prácticamente Seguro**
Impacto	**Muy Alto**	Importante	Crítico	Crítico	Crítico	Crítico
	Alto	Apreciable	Importante	Importante	Crítico	Crítico
	Medio	Bajo	Apreciable	Apreciable	Importante	Importante
	Bajo	Asumible	Bajo	Bajo	Apreciable	Apreciable
	Muy Bajo	Asumible	Asumible	Asumible	Bajo	Bajo

Tabla 4. Matriz para la estimación del riesgo
Fuente: MAGERIT I

3.4 Metodología de Análisis y Gestión de Riesgos ne los Sistemas de Información

En el punto anterior se ha definido el proceso de Análisis de Riesgos como un estudio sistemático y estructurado de los activos de una empresa, sobre los cuales se analizan sus vulnerabilidades con el objetivo de estudiar el riesgo que estas suponen.

El análisis de riesgos debe ser entendido como un proceso con diferentes tareas que han de llevarse a cabo como parte de un proyecto de gestión de la seguridad y que ha de ser revisado y mejorado de forma continua, no como una serie de tareas independientes. Es por esto por lo que es de vital importancia utilizar una metodología para este proceso.

El término metodología se puede definir como un grupo de mecanismos o procedimientos racionales empleados para el logro de un objetivo o serie de objetivos.

El método MAGERIT o Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información [**¡Error! No se encuentra el origen de la referencia.**] es un documento elaborado p or el Consejo Superior de Administración Electrónica, según se explica en el propio documento *"… como respuesta a la percepción de que la Administración pública (y en general toda la sociedad) depende de forma creciente de los sistemas de información para alcanzar sus objetivos"*.

Este documento describe una metodología que permite llevar a cabo la Gestión de riesgos descrita en la ISO 31000 Sistemas de gestión de riesgos [9]. Esta metodología define una serie de pasos a seguir que en el propio documento se describen de la siguiente manera:

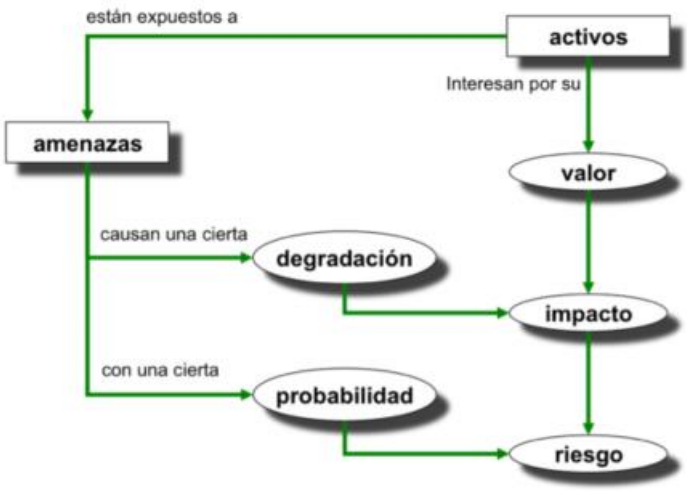

Ilustración 1. Elementos del análisis de riesgos potenciales
Fuente: MAGERIT – Libro1

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

Si bien existen un gran número de metodologías para el análisis y la gestión de riesgos (Por ejemplo, OCTAVE desarrollada por la Universidad Carnegie Mellon o NIST SP 800-30 definida por el Instituto Nacional de Estándares y Tecnología), para la elaboración del presente documento se utilizará la metodología MAGERIT por ser la metodología más utilizada actualmente en España para el proceso de gestión de riesgos enmarcado en los sistemas SGSI.

3.5. Los sistemas de información en los centros educativos

Ya se ha mencionado en los apartados anteriores qué son los sistemas de información y su importancia en las empresas y organizaciones actuales. Y, como también se ha comentado, si bien todas las organizaciones que trabajan con una cantidad importante de datos deberían contar con un sistema de información, las necesidades de este variarán en función del ámbito de la organización.

En este punto, se va a abordar cuales son las tareas que deben realizar los sistemas de información en un centro escolar y cuál es la realidad de estos, tanto a nivel nacional, como en la Comunidad Valenciana.

3.5.1 Importancia de los sistemas de información en los centros escolares

Actualmente, el sistema de información es un punto clave para la gestión y la organización de los centros escolares, principalmente por dos factores:

En primer lugar, un sistema de información es un elemento fundamental para asegurar el buen funcionamiento del centro, ya que este interviene en un gran número de procesos relacionados con el centro tanto a nivel educativo, como a nivel administrativo.

Pero los sistemas de información no son importantes únicamente para agilizar las gestiones de los centros educativos. Además de su utilidad a corto plazo, los sistemas de información tienen un importante papel a largo plazo, puesto que son una herramienta indispensable de cara a establecer las estrategias de los planes institucionales.

Las instituciones educativas deben hacer frente a diferentes retos y para ello, es importante contar con herramientas que permitan ayudar a la toma de decisiones, tanto en la gestión como en el modelo educativo.

De esta forma, los sistemas de información permiten recoger todos los elementos que intervienen en un centro educativo para tener una visión global sobre los mismos. Así, se hace más sencillo dirigir los esfuerzos en cumplir una serie de objetivos para alcanzar la calidad educativa, que actualmente es una de las cuestiones que genera más carga de trabajo a nivel administrativo en los centros escolares.

3.5.2 Situación actual de los sistemas de información en los centros educativos a nivel nacional

Los centros educativos, así como cualquier otra organización que trate con datos personales, se rigen a día de hoy por el nuevo Reglamento General de Protección de Datos (RGPD). El RGPD es un reglamento relativo al tratamiento de datos personales y a su libre circulación para las organizaciones que traten con datos de ciudadanos europeos. Es por ello por lo que los Sistemas de Información de todos los centros educativos deben esforzarse en cumplir las premisas propuestas por este reglamento.

Actualmente, a nivel nacional no se ha implantado un sistema de información centralizado o una propuesta específica para los sistemas de información de los centros educativos. Sin embargo, las comunidades autónomas sí proponen diferentes opciones para el desarrollo de los sistemas de información, aunque por lo general son solo soluciones parciales o plataformas para facilitar el desarrollo de partes específicas del sistema. En última instancia corresponde a los propios centros la elaboración del sistema completo siguiendo sus propios intereses.

Por poner algunos ejemplos, en Cataluña, el departamento de enseñanza en los centros docentes propone Ágora [10] que es una plataforma que permite a los centros educativos la instalación y mantenimiento de los servicios de Moodle, de forma que sean los centros los que decidan si quieres utilizar estos recursos en sus sistemas de información. También es posible encontrar otros modelos más amplios como el propuesto por la junta de Andalucía, que propuso en el año 2001 el sistema SÉNECA que fue evolucionando hasta el actual sistema SÉNECA-PASSEN [11]. Este sistema según su propia definición *"…constituye un conjunto de sistemas front-office back-office que abarca todas las facetas de la gestión de los centros de enseñanza, atendiendo a las necesidades de información y servicios de todos los miembros de la comunidad educativa*". Básicamente es una herramienta que permite a los centros educativos establecer la comunicación con padres, alumnos o asociaciones de padres y madres, además de agilizar algunos procesos como la comunicación de noticias por parte del centro, tramites de matriculación etc.

3.4.3 Sistemas de información en los centros educativos de la Comunidad Valenciana

Ya se han mencionado algunos de los modelos propuestos en algunas comunidades autónomas. Sin embargo, para la consecución de este trabajo es conveniente analizar el modelo propuesto por la comunidad valenciana donde actualmente se trabaja con el sistema ITACA [12].

ITACA es un sistema de información centralizado para todos los centros educativos públicos y concertados de la comunidad valenciana que actualmente está incorporado en más de 2.000

centros educativos según su página oficial. La idea de este sistema es que funcione como medio de enlace entre los centros y la Consellería d'Educació, pero además de eso, funciona como una propuesta de sistema de información para que puedan usarlo los centros educativos de la comunidad.

De esta forma, todos los centros tanto públicos como concertados, están obligados a su utilización para justificar ante la Consellería la gestión económica y administrativa del centro. Sin embargo, el sistema proporciona diferentes servicios que pueden ser usados por los centros de forma voluntaria para facilitar la gestión de la información.

Este sistema proporciona diferentes niveles de acceso para diferentes tipos de usuarios en función de si estos son padres de alumnos, personal docente, jefe de estudios, director de centro o director general, siendo estos dos últimos cargos de la administración de la Consellería.

ITACA proporciona diferentes servicios y está pensado de forma que el personal de los centros pueda introducir datos de diferentes ámbitos y luego este sea organizado para mostrarse de forma accesible, tanto al personal del centro como directamente a la Consellería d'Educació.

En primer lugar, el personal de los centros debe introducir datos relacionados con la administración del centro, como pueden ser la admisión de alumnos, datos personales sobre los alumnos del centro, expedientes académicos, organización de aulas etc. Tras esto, todos los datos introducidos estarán disponibles para el personal que tenga acceso a ellos en forma de diferentes listados que permitirán un acceso sencillo a toda la información.

Además, ITACA proporciona otros servicios, como la gestión de los datos relacionados la gestión del comedor escolar, la gestión del transporte hasta el centro, servicio de comunicación con las familias…

En los últimos años, la Generalitat Valenciana ha puesto en marcha, junto con su sistema ITACA, la aplicación web Docent 2 [13], que pretende ser un complemento para el personal docente. Esta aplicación está conectada con el sistema ITACA y, ocultando gran parte de la información administrativa, proporciona una interfaz más manejable para la gestión de la docencia en los centros educativos de forma que con la aplicación, los profesores puedan llevar un control de sus horarios, calificaciones de los alumnos, faltas de asistencia y otras cuestiones relevantes en la labor docente.

4. Antecedentes

Para la consecución de este trabajo, se va a realizar un plan para la implantación de un SGSI en un colegio concertado de la provincia de Alicante. Este centro educativo es un colegio fundado por una orden religiosa en los años 50 que actualmente imparte clases a alrededor de 700 niños y niñas de entre 4 y 16 años entre educación infantil, primaria, secundaria y un grado medio de formación profesional. Además, en el centro trabajan unas 60 personas entre personal docente, educadores y personal de administración y servicios.

4.1 Estructura y organización del centro

En referencia a la estructura organizativa del centro, el titular de este es una persona perteneciente a la orden religiosa que gestiona la administración del centro. El resto del personal del centro se puede dividir en personal administrativo y personal docente, que además de su labor pedagógica estarán involucrados en mayor o menor medida en tareas relacionadas con la administración. El personal docente, además, está organizado en diferentes departamentos según su rama de conocimiento tal y como se define en la Figura 2 y se explica a continuación.

El director o, en este caso, directora del centro, es una persona del personal docente del centro que cada 4 años se presenta para formar, junto con la persona titular, el equipo directivo del centro.

El consejo escolar es la plataforma que permite la comunicación entre el profesorado del centro y el equipo de madres y padres de alumnos y el departamento de calidad es el responsable del sistema de gestión de la calidad educativa del centro.

Por último, del equipo directivo depende el personal docente del centro, que además de estar organizado en diferentes departamentos, su área de trabajo está claramente delimitada por los ciclos educativos en los que trabaja. De esta forma es posible dividir el profesorado entre aquellos que trabajan en la educación infantil, educación primaria, educación secundaria o educación especial (nombre que se le da en el colegio a las clases orientadas a alumnos con discapacidades psicológicas en diferentes grados).

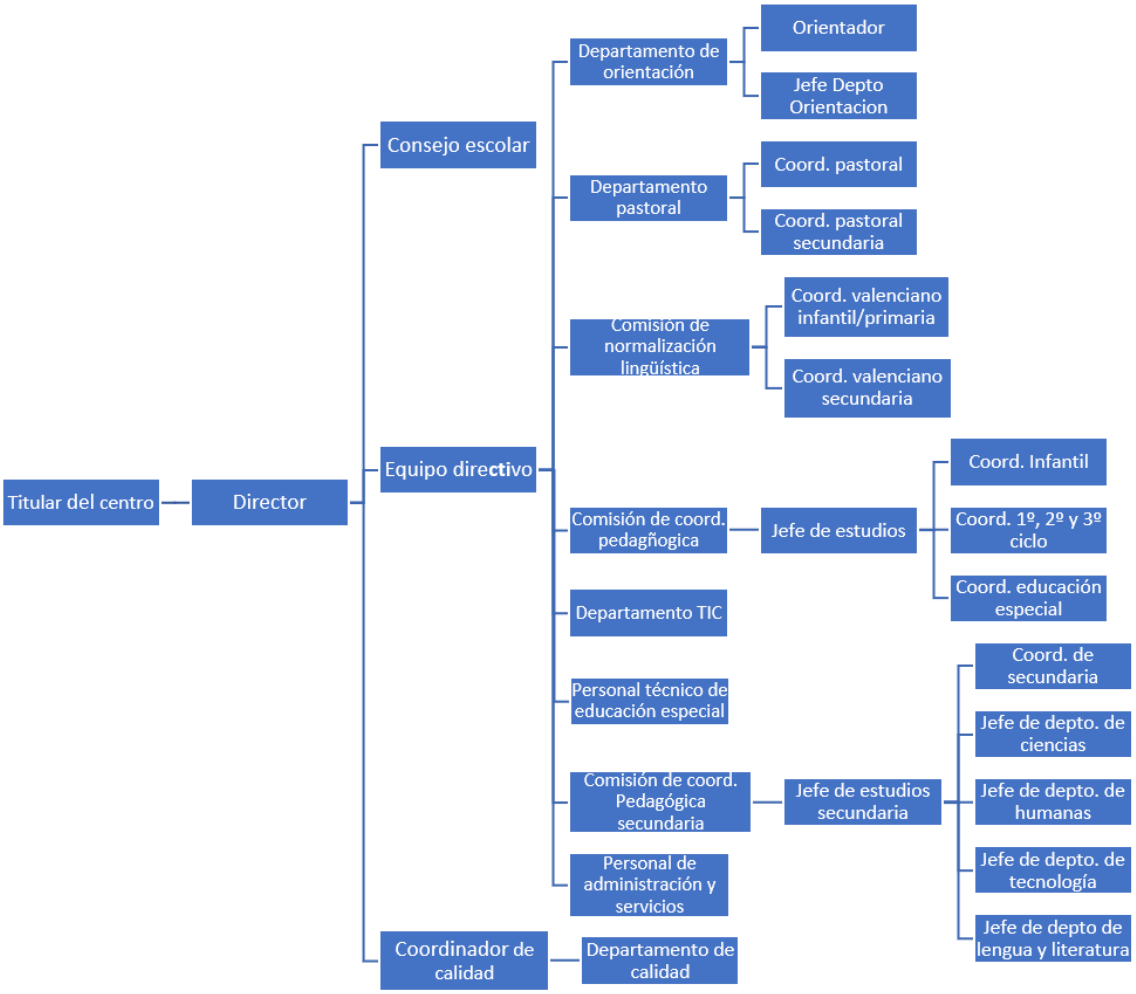

Figura 2. Organigrama del centro escolar

4.2 Contexto

Este colegio es un centro educativo concertado, es decir, que está administrado de forma privada, aunque su financiación es mayoritariamente pública gracias a diferentes conciertos y subvenciones. De cara a la gestión del centro, esta situación implica que la Consellería d'Educació de la Comunidad Valenciana debe tener acceso a la información académica y contable del centro. Precisamente por esto, tal y como se ha desarrollado en apartados anteriores, el colegio está obligado a la utilización de la plataforma ITACA.

Desde el curso académico 2017-2018 se está empezando a utilizar un producto privado llamado Alexia [14] que en su página web se define como *"Plataforma en constante crecimiento, que integra el área de gestión académico-administrativa y la comunicación entre colegio-familias con las herramientas 2.0 más novedosas."*

La idea del centro es usar la plataforma Alexia para llevar a cabo toda la gestión administrativa del centro, exceptuando aquellas cuestiones que por ley tengan que presentar ante la Consellería d'Educació (principalmente el ámbito de contabilidad). Sin embargo, actualmente el centro está todavía inmerso en la migración de datos y de funciones a esta plataforma, con lo que su uso está limitado a la comunicación entre el profesorado y las familias de los alumnos del centro.

Por otro lado, los centros educativos manejan una gran cantidad de información personal de los alumnos y sus familias, además de información de los propios trabajadores del centro. Esta información debe estar administrada según lo definido en el nuevo Reglamento General de Protección de Datos (RGPD) [15], teniendo especial cuidado con aquellos datos relacionados con el ámbito más y tomando medidas especiales también con el uso de las TIC con fines educativos y para la comunicación entre padres y profesores. Estas últimas cuestiones relacionadas con el ámbito de las TI cobran gran importancia, debido a que por el hecho de ser relativamente novedosas en el ámbito educativo, existen muchas dudas acerca del correcto uso de las mismas.

Otra de las responsabilidades que tiene el centro está relacionada con el uso de productos sometidos a derechos de propiedad intelectual. Según la Ley de Propiedad Intelectual, en el artículo 32, modificado en el año 2014 [16**¡Error! No se encuentra el origen de la referencia.**] *"El profesorado (…) no necesitará autorización del autor o editor para realizar actos de reproducción, distribución y comunicación pública de pequeños fragmentos de obras (…) cuando, no concurriendo una finalidad comercial se cumplan simultáneamente las siguientes condiciones: Que tales actos se hagan para la ilustración de sus actividades educativas, (…) que*

se trate de obras ya divulgadas y que las obras no tengan condición de libro de texto…". De esta forma el personal del centro educativo tiene la capacidad de usar materiales con derechos de autor en sus actividades educativas, pero teniendo en cuenta que otros materiales como libros de texto o herramientas software si pueden estar sujetas a derechos de autor y deberán utilizarse adquiriendo los derechos de estas.

Finalmente, toda la actividad del centro debe dirigirse a la consecución del objetivo de conseguir la calidad educativa, concepto que desde hace unos años se ha puesto muy de moda en el ámbito educativo, y que está regulada en la familia de normativas ISO 9000. La organización ISOTools define esta normativa de la siguiente manera: *"El concepto de calidad dentro de los centros educativos debe estar siempre enlazado con la idea de educación de calidad. Este concepto de calidad, que en ocasiones se hace tan subjetivo, queda definido en la Norma ISO 9001, en la que se establecen los requisitos que deben reunir y cumplir los Centros Educativos para la obtención del reconocimiento de la calidad en su gestión, a través de la implantación de un Modelo de Sistema de Gestión de la Calidad (SGC)."*

Si bien no hay ningún aspecto legal que obligue a la obtención de esta certificación de calidad, es beneficiosa tanto para la imagen del centro como para la propia gestión del colegio y, por tanto, actualmente tanto personal pedagógico como administrativo están realizando grandes esfuerzos para conseguir esta certificación.

4.3 Estado inicial del Sistema de Información

Para analizar el Sistema de Información del centro es importante analizar la información gestionada por este, así como el personal que interactúa con el SI y los recursos destinados a su correcto funcionamiento. En puntos anteriores ya se ha analizado el personal del centro encargado de manejar la información generada en el mismo y, en lo referente a la información, se pueden distinguir 3 campos:

Área	Descripción
Información pedagógica	Información y documentos relacionados con la labor educativa del centro como pueden ser exámenes, expedientes académicos o documentos generados a partir de la comunicación con las familias de los alumnos.
Información administrativa	Información generada a partir de la gestión administrativa del centro como documentos de matriculación, información contable, autorizaciones o documentos de la gestión interna.
Información relacionada con otras actividades	Información generada a partir de la ejecución de otras actividades en el centro como el comedor escolar, el banco de libros o actividades extraescolares.

Tabla 5. Información generada por el centro según su origen

La información administrativa y la relacionada con otras actividades, está gestionada por el equipo directivo y el personal de administración. La gestión de esta información se lleva a cabo en gran medida mediante la aplicación ITACA y se almacena también tanto en formato digital (Documentos en diferentes formatos almacenados de forma digital en un disco duro) como en documentos impresos.

La gestión de la información administrativa es un proceso bien delimitado, en el cual los actores involucrados son conscientes de la tarea que tienen que realizar. Sin embargo, este proceso no está definido en ningún tipo de documento o de política que limite de manera formal el campo de acción del personal del centro.

Por otro lado, la gestión de la información pedagógica se lleva a cabo por el personal docente. En este área, hay una serie de políticas que delimitan los documentos a los que tiene acceso cada individuo o que tareas tiene que. Sin embargo, el cómo realizar otra parte de esta gestión queda en manos de los propios profesores y profesoras que pueden decidir, por ejemplo, si las pruebas de los alumnos se almacenan en la nube o en formato físico o si la entrega de trabajos se realiza de forma presencial o de forma telemática.

Para un análisis formal sobre la situación inicial del Sistema de Información del centro se han evaluado los aspectos obligatorios a tener en cuenta según la normativa ISO 27000. En esta evaluación se clasificarán los diferentes aspectos de la siguiente manera:

Valoración	Descripción
L0 – No implementado	No se lleva a cabo el control de seguridad en los sistemas de información.
L1 – Inicial / Ad-hoc	Procedimientos existentes, pero sin un proceso formal definido. Su éxito depende de esfuerzos personales.
L2 – Reproducible pero intuitivo	Existe un método de trabajo, pero sin comunicación formal, depende del conocimiento del propio individuo y no hay formación del personal.
L3 – Proceso definido	El proceso se lleva a cabo conforme a la documentación especificada que ha sido administrada por la organización.
L4 – Gestionado y medible	Se puede realizar un seguimiento de la evolución del proceso a través de datos estadísticos.
L5 – Optimizado	Los procesos están implementados según un procedimiento documentado que es medido periódicamente y están en constante mejora
N/A – No Aplica	O bien es un aspecto que no tiene cabida dentro del contexto de la organización o bien su gestión es externa a la propia organización.

Tabla 6. Leyenda para la evaluación inicial del SGSI
Fuente: ISO/IEC 27001:2013 ISMS Status

Estado Inicial del SGSI	
4. Contexto de la organización	
4.1 Comprensión de la organización y de su contexto	L2 – Reproducible pero intuitivo
4.2 Comprensión de las necesidades y expectativas de las partes interesadas	L1 – Inicial / Ad-hoc
4.3 Determinación del alcance del SGSI	L0 – No implementado
4.4 Sistema de gestión de la seguridad de la información	L0 – No implementado
5. Liderazgo	
5.1 Liderazgo y compromiso	L1 – Inicial / Ad-hoc
5.2 Política	L2 – Reproducible pero intuitivo
5.3 Roles, responsabilidades y autoridades en la organización	L2 – Reproducible pero intuitivo
6. Planificación	
6.1 Acciones para tratar los riesgos y oportunidades	
6.1.1 Consideraciones generales	L1 – Inicial / Ad-hoc
6.1.2 Apreciación de riesgos de seguridad de la información	L0 – No implementado
6.1.3 Tratamiento de los riesgos de la seguridad de la información	L0 – No implementado
6.2 Objetivos de seguridad y planificación para su consecución	L1 – Inicial / Ad-hoc
7. Soporte	
7.1 Recursos	L2 – Reproducible pero intuitivo
7.2 Competencia	L2 – Reproducible pero intuitivo
7.3 Concienciación	L1 – Inicial / Ad-hoc
7.4 Comunicación	L2 – Reproducible pero intuitivo
7.5 Información documentada	
7.5.1 Consideraciones generales	L0 – No implementado
7.5.2 Creación y actualización	L0 – No implementado
7.5.3 Control de la información documentada	L0 – No implementado
8. Operación	
8.1 Planificación y control operacional	L2 – Reproducible pero intuitivo
8.2 Apreciación de los riesgos de seguridad de la información	L0 – No implementado
8.3 Tratamiento de los riesgos de seguridad de la información	L0 – No implementado

9. Evaluación del desempeño	
9.1 Seguimiento, medición, análisis y evaluación	L0 – No implementado
9.2 Auditoría interna	L0 – No implementado
9.3 Revisión por la dirección	L0 – No implementado

Tabla 7. Análisis del estado inicial del SGSI
Fuente: ISO/IEC 27001:2013 ISMS Status

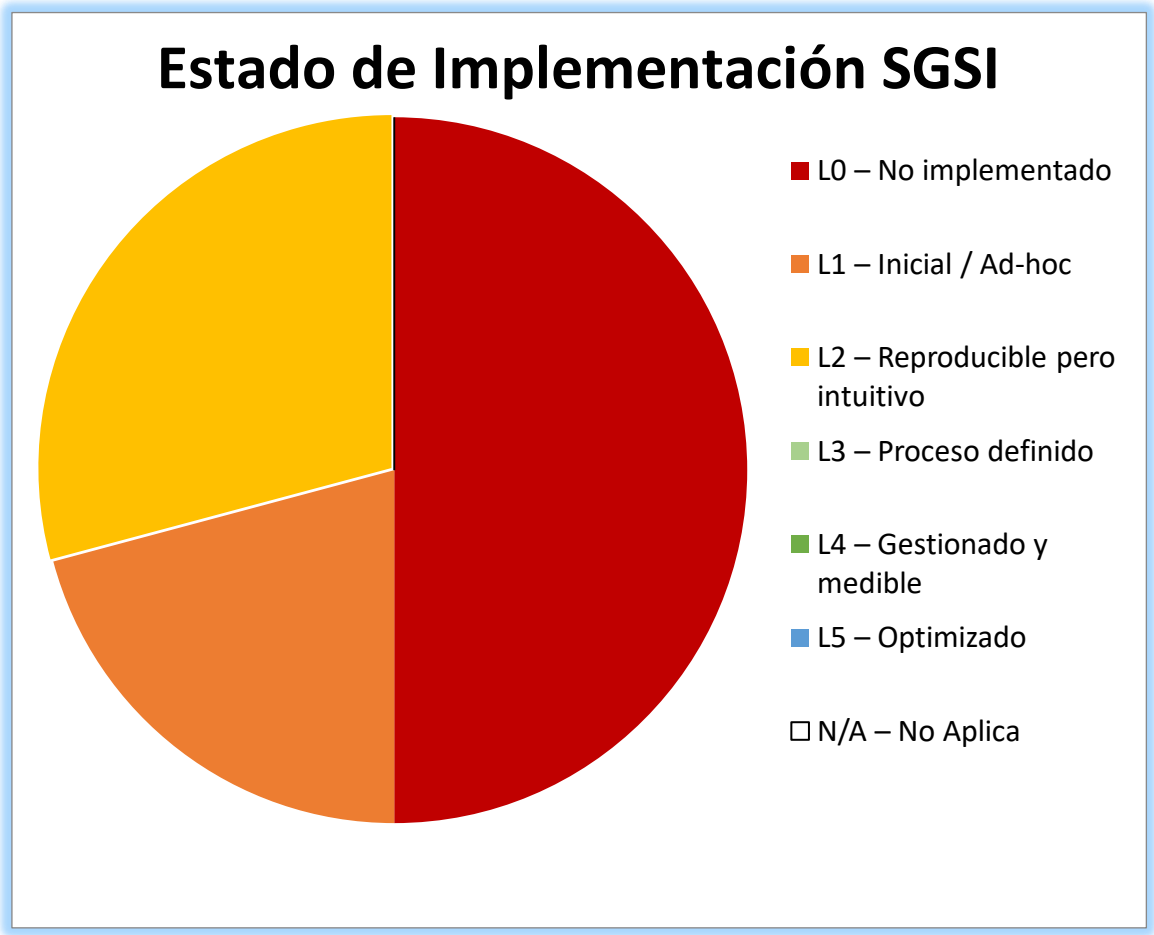

Figura 3. Resumen del estado inicial del SGSI

Habiendo hecho el análisis de la situación actual del centro, desde el contexto hasta el estado inicial del sistema de información, en los siguientes apartados empieza el trabajo orientado a llevar a cabo las medidas necesarias para poner el marcha el Sistema de Gestión de la Seguridad de la Información.

5. Objetivos

En este apartado se van a detallar los objetivos que se pretenden alcanzar con la realización de este proyecto.

El principal objetivo del trabajo es conseguir que el centro escolar estudiado mejore la seguridad de la información que maneja mediante la implantación de un Sistema de Gestión de la Seguridad de la Información. Para ello habrá que desarrollar los siguientes subobjetivos:

1. Estudio del centro. Comprensión de su modelo de negocio, su contexto externo, su estructura organizativa y las funciones realizadas por el personal del centro, así como la información que maneja.
2. Elaboración de un catálogo de activos. Listado con todos los elementos relevantes en un SGSI, así como la valoración de los mismos en función de la importancia que tienen para el funcionamiento del centro.
3. Elaboración de un listado de amenazas. Análisis de las amenazas a las que están expuestos los activos del centro.
4. Análisis de riesgos. Estudiar los riesgos a los que están expuestos los activos del centro en función de las amenazas que pueden sufrir, su probabilidad y el daño que pueden ocasionar.
5. Propuesta de salvaguardas. Listado con una serie de salvaguardas que permitan disminuir el riesgo que corren los activos del centro.
6. Creación del plan de seguridad para el colegio. Elaborar un documento con el plan del seguridad y que pueda ser entregado al centro educativo para que estos puedan valorar la seguridad de su Sistema de Información y poder implantar algunas de las medidas propuestas.
7. Colaborar en la implantación de medidas. Una vez entregado el documento al centro, llevar a cabo la implantación de alguna de las medidas propuestas en el plan de seguridad.

6. Propuesta

A continuación, se detallará la propuesta para la implantación del SGSI en el colegio.

Si bien la normativa ISO 27001 establece los requisitos a cumplir de cara a implementar un SGSI, para cumplir estos requisitos es importante seguir una metodología que imponga una serie de procesos y mecanismos a seguir a lo largo del proyecto de implantación. Para la consecución de este trabajo se seguirá la metodología MAGERIT por ser la metodología más utilizada en la implantación de Sistemas de Gestión de la Seguridad de la Información en España.

Según lo establecido por esta metodología, la implantación del SGSI conllevará un análisis previo para realizar un catálogo de activos del centro, identificar las amenazas que pongan en riesgo el valor de los activos y realizar un proceso de evaluación de riesgos.

Tras esto se llevará a cabo un análisis de tratamiento de riesgos en el que se decidirá cuáles de estos son asumibles para el colegio y cuáles han de ser tratados y se llevarán a cabo las medidas necesarias para reducir su riesgo.

7. Catálogo de activos

En el siguiente apartado se va a llevar a cabo la elaboración del catálogo de activos. Esta tarea según está definida en la metodología MAGERIT, consta de 3 subtareas que son: Identificar los activos, identificar las dependencias entre activos y establecer el valor de los mismos.

De cara a identificar los activos del centro se establecen diferentes categorías de activos entre las que se encuentran las siguientes.

Clase de activo	Descripción
[D] Datos / Información	Información generada o manejada por el centro almacenado en diferentes soportes de información.
[S] Servicios	Servicios o funciones prestados por la organización para cubrir una necesidad de los usuarios.
[SW] Software	Aplicaciones informáticas tanto de desarrollo propio como aplicaciones externas que permiten que ciertas tareas se desempeñen a través del equipo informático.
[HW] Hardware	Equipo informático que actúan como soportes de datos o que albergan los servicios informáticos del centro
[COM] Redes de comunicaciones	Redes que actúen como medio de transporte para datos a través de equipos informatizados.
[Media] Soportes de información	Dispositivos, tanto electrónicos como no electrónicos que permiten almacenar información.
[AUX] Equipamiento auxiliar	Equipos o dispositivos hardware que sirvan como soporte para el sistema informático.
[L] Instalaciones	Lugares para almacenar el hardware del sistema de información.
[P] Personal	Personal relacionado con el sistema de información del centro.

Tabla 8. Clases de activos a identificar en el catálogo
Fuente: MAGERIT I

A cada activo se le asignará un valor según una estimación sobre el perjuicio que supondría perderlo, siendo aquellos activos con más valor aquellos que más interesa proteger. Según esto, los activos podrán tener los siguientes 5 niveles de importancia según su valor:

Valor	Descripción
Muy Alto	Daño crítico para el centro
Alto	Daño grave para el centro
Medio	Daño importante para el centro
Bajo	Daño asumible para el centro
Muy Bajo	Daño inexistente para el centro

Tabla 9. Escala de valor de los activos

Además, para cada activo se debe valorar la importancia de las diferentes dimensiones de seguridad en función de cómo de perjudicial sería que esas dimensiones se vieran alteradas. Así es necesario para cada activo valorar la importancia de proteger cada una de las siguientes dimensiones:

Dimensión	Descripción
Confidencialidad	Como de dañino sería que un activo quedase accesible a personal que en circunstancias normales no tiene acceso.
Integridad	Como de problemático sería que un activo estuviese dañado, corrupto o alterado.
Disponibilidad	Cuál sería el perjuicio provocado en caso de que un activo no estuviera disponible en un determinado momento.
Autenticidad	Cuanto daño podría causar el hecho de que la persona que acceda a un servicio no sea quien dice ser o que los datos referentes a una persona no sean realmente de esa persona
Trazabilidad	Cómo de importante es que quede constancia de que personas tienen acceso y acceden a un activo

Tabla 10. Dimensiones de los activos

Por último, para cada activo se identificarán las dependencias existentes con otros activos. La dependencia entre activos indica que si una amenaza afecta a un activo afectará también a todos aquellos que dependan de él, por tanto, permite definir el valor acumulado de un activo como el valor del propio activo sumado al de aquellos que dependen de él.

Así pues, la elaboración del catálogo de activos consistirá en una tarea en la cual se identificarán los elementos que puedan ser importantes para el SI del centro y se procederá a su valoración e identificación de dependencias. Hecho esto, para cada activo se rellenará una ficha con la información recogida que formará el catálogo.

Estas fichas son el método propuesto por la metodología MAGERIT para realizar el catálogo de activos que si bien genera un documento más extenso que utilizando otro método como podría ser plasmar el catálogo de activos en una única tabla o en una lista, aporta más información. Precisamente este formato puede ser el más interesante sobre todo teniendo en cuenta que el público al que va destinado este documento es el personal docente de un centro que no tiene por qué tener ninguna experiencia en este ámbito

A continuación, se muestra un ejemplo de estas tablas y se adjunta el catálogo de activos completo en el Anexo I [2. Catálogo de activos].

[D] Datos					
Código: D.2			**Nombre:** Expedientes académicos		
Descripción: Información relacionada con el expediente académico de los estudiantes como pueden ser calificaciones, asistencia a clases o partes disciplinarios.					
Tipo: Ficheros					
Dependencias					
Activos: SW.2			**Grado:** Alto		
¿Por qué? Todos los datos relacionados con los expedientes académicos de los alumnos deben introducirse en la plataforma de Itaca para que desde la Consellería d'Educació tengan acceso a estos datos					
Valor					
Total	**Confidencialidad**	**Integridad**	**Disponibilidad**	**Autenticidad**	**Trazabilidad**
Muy Alto	Muy Alto	Muy Alto	Medio	Muy Alto	Alto

Figura 4. Ejemplo de ficha del catálogo de activos

8. Listado de amenazas

Una vez se ha desarrollado el catálogo de activos, el siguiente paso para realizar el plan de seguridad de una organización consiste en realizar el listado de amenazas tal y como se va a describir en el siguiente apartado. Para ello se continuará usando la metodología MAGERIT que establece dos tareas principales: La identificación de las amenazas y la valoración de las estas.

Para identificar las amenazas que pueden afectar a los activos de una organización, MAGERIT establece un catálogo de amenazas típicas organizadas según las siguientes categorías:

Categoría de amenaza	Descripción
[N] Desastres naturales	Sucesos que puede ocurrir sin intervención de los seres humanos como causa directa o indirecta.
[I] De origen industrial	Sucesos que pueden ocurrir de forma accidental derivados de la actividad humana de tipo industrial y que pueden darse de forma accidental o deliberada.
[E] Errores y fallos no intencionados	Fallos no intencionales causados de forma directa por la actividad de personas que tienen acceso al sistema de información. Normalmente se producen por error u omisión.
[A] Ataques intencionados	Fallos deliberados causados por la actividad humana con el objetivo o bien de beneficiarse indebidamente o de causar daños a la organización.

Tabla 11. Clases de amenazas según su origen
Fuente: MAGERIT

Las amenazas que pueden afectar a la organización no afectan a todos los activos por igual, es por esto por lo que es necesario identificar, para cada amenaza, a que activos puede afectar y en qué grado de degradación y probabilidad.

Para determinar la probabilidad con la que una amenaza puede afectar a un activo, se estimará cual es la probabilidad de que esta se materialice y para estimar la degradación, se determinará en qué medida el activo perdería su valor en el caso de materializarse dicha amenaza.

Debido a la dificultad de realizar una valoración numérica, para medir tanto la probabilidad como la degradación se utilizarán las siguientes escalas cualitativas

Valor	Abreviatura	Descripción
Muy Alta	MA	A diario
Alta	A	Mensualmente
Media	M	Una vez al año
Baja	B	Cada varios años
Muy Baja	MB	Siglos

Tabla 12. Escala de probabilidad de una amenaza

Valor	Abreviatura	Descripción
Alta	A	Degradación total
Media	M	Degradación perceptible
Baja	B	Degradación inapreciable

Tabla 13. Escala de degradación de una amenaza

Finalizado este proceso, se creará un documento que se adjuntará al plan de seguridad, que posteriormente se entregará al centro educativo, con un listado de las amenazas a las que está expuesto su sistema de información. Este documento estará formado por una serie de fichas que indicarán las amenazas que puede sufrir el centro, la probabilidad que tienen estas de materializarse y los activos a los que pueden afectar, así como el grado en el que el valor de los mismos puede verse perjudicado.

Una de las técnicas más comunes para realizar este catálogo de amenazas es realizar una tabla en la que aparezcan el código de las amenazas que se considera que pueden materializarse, los activos a los que afecta e indicar en qué medida estos pueden producirse. De esta forma se representa en un documento toda la información del listado de amenazas.

Sin embargo, como se mencionó en el apartado Catálogo de Activos [7. Catálogo de activos], teniendo en cuenta que este documento va dirigido a un público no especializado en la implantación de un SGSI, se ha decidido realizar una serie de fichas como la presentada en la Figura5 que contengan la descripción de cada una de las amenazas que, si bien generan un documento más extenso, aportan más información con el objetivo de facilitar su entendimiento.

I.10 Degradación de soportes de información					
Descripción: Errores o averías en los dispositivos de soporte de información debido al paso del tiempo y al uso continuado.					
Probabilidad: Alta Si bien no es algo muy frecuente es inevitable que cada mes o cada varios meses los soportes de almacenamientos electrónicos den algún fallo					
Activos afectados					
Nombre	**Degradación**				
	C	**I**	**D**	**A**	**T**
Media.1 - Discos duros de Administración	-	-	A	-	-
Media.2 - Almacenamiento USB	-	-	M	-	-

Figura 5. Ejemplo de ficha del listado de amenazas

Este es un ejemplo de las fichas utilizadas para la elaboración del listado de amenazas. En estas se describen el código identificador y el nombre de la amenaza, así como una breve descripción de la misma para facilitar la comprensión por parte del centro.

Además, se especifica la probabilidad que tiene de materializarse la amenaza según la escala expuesta anteriormente y los activos a los que puede afectar, así como el grado de degradación causante. En este caso, la amenaza "*Degradación de soportes de información"* afectaría negativamente a los discos duros del centro y los dispositivos de almacenamiento USB, para los cuales, causaría una degradación de nivel alto y medio respectivamente en el ámbito de la disponibilidad de estos activos, no viéndose afectados otras dimensiones como la confidencialidad, la integridad, la autenticidad o la trazabilidad.

El resto de las amenazas que conforman el listado de amenazas completo se adjuntan en el Anexo I [3. Listado de las amenazas].

9. Estimación de riesgos

Habiendo identificado y valorado los activos de la organización, así como las amenazas a los que estos pueden estar expuestos, en este apartado se realizará el cálculo del impacto y la estimación de riesgos.

En primer lugar, se va a analizar el daño que puede causar para la organización una posible amenaza sobre un determinado activo. En este caso, se hablará de impacto potencial, es decir, el impacto que puede producir sin tener en cuenta ningún tipo de contramedidas o salvaguardas.

Es posible calcular el impacto como una relación entre el valor de un determinado activo y la degradación causada por esa amenaza, para ello, se utilizará la relación expuesta a continuación.

		Degradación		
		Baja	**Media**	**Alta**
Valor	**Muy Alto**	Medio	Alto	Muy Alto
	Alto	Bajo	Medio	Alto
	Medio	Muy Bajo	Bajo	Medio
	Bajo	Muy Bajo	Muy Bajo	Bajo
	Muy Bajo	Muy Bajo	Muy Bajo	Muy Bajo

Tabla 14. Matriz para la estimación del impacto potencial
Fuente: MAGERIT

Además del cálculo del impacto potencial, es necesario tener en cuenta que el impacto generado por una amenaza no proviene únicamente de la degradación del activo al que afecta en primera instancia, sino que todos aquellos elementos que dependan del activo afectado también sufrirán una degradación de su valor.

Para tener este factor en cuenta, además del impacto potencial, se realizará una estimación del impacto acumulado, en el que se realizará el mismo proceso pero tomando como valor del activo el más alto entre su propio valor y el valor de los activos que dependan de este.

La segunda tarea a realizar en este apartado consiste en realizar la estimación de riesgos.

De la misma forma que es posible entender el impacto como una relación entre valor y degradación, se puede estimar el riesgo como una relación entre la probabilidad que tiene de materializarse una amenaza y el impacto generado por esta.

Si bien con el impacto se estima como de perjudicial sería para la organización que se materialice una amenaza, el riesgo tiene en cuenta también como de probable es que esa amenaza llegue a producirse y, por tanto, que la organización sufra el impacto estimado.

Para realizar la estimación del riesgo, calcularemos, de la misma forma que en el caso del impacto, tanto el riesgo potencial como el riesgo acumulado a partir de la siguiente relación:

Riesgo		Probabilidad				
		Muy Baja	**Baja**	**Media**	**Alta**	**Muy Alta**
Impacto	**Muy Alto**	Importante	Crítico	Crítico	Crítico	Crítico
	Alto	Apreciable	Importante	Importante	Crítico	Crítico
	Medio	Bajo	Apreciable	Apreciable	Importante	Importante
	Bajo	Asumible	Bajo	Bajo	Apreciable	Apreciable
	Muy Bajo	Asumible	Asumible	Asumible	Bajo	Bajo

Tabla 15. Matriz para la estimación de riesgos
Fuente: MAGERIT

El cálculo de estas dos magnitudes resulta vital para la elaboración de un plan de seguridad, puesto que, de cara a proponer contramedidas y salvaguardas para mitigar los efectos de posibles amenazas, habrá que priorizar aquellas que supongan un mayor riesgo para la organización. Incluso pueden darse situaciones en las que se considere que un determinado riesgo es aceptable y se evite por tanto la utilización de recursos en mitigar ese riesgo. Estos conceptos se desarrollarán con detalle en los siguientes apartados del documento.

La elaboración del proceso de estimación de riesgos conllevará la elaboración de un documento, que se adjuntará en el Anexo I, con una serie de tablas en las que se reflejará el impacto y el riesgo que suponen sobre los diferentes activos del centro todas las amenazas identificadas.

A continuación, se explica y se muestra un ejemplo de una de las tablas expuestas en el Anexo I [4. Estimación de riesgos].

SW.1 - Alexia												
Amenazas	**Impacto Potencial**			**Impacto Acumulado**			**Riesgo Potencial**			**Riesgo Acumulado**		
	C	**I**	**D**	**C**	**I**	**D**	**C**	**I**	**D**	**C**	**I**	**D**
E.1 – Errores de los usuarios	-	-	B	MB	B	B	-	-	M	B	M	M
E.2 – Errores de administrador	-	-	M	MB	B	M	-	-	M	MB	B	M
E.20 – Vulnerabilidad de los programas	-	-	B	M	M	B	-	-	B	M	M	B
A.5 – Suplantación de la identidad	-	-	-	M	M	-	-	-	-	B	B	-
A.6 – Abuso de privilegios de acceso	-	-	B	M	MB	B	-	-	B	M	MB	B
A.11 – Acceso no autorizado	-	-	-	M	M	-	-	-	-	B	B	-
A.24 – Denegación de servicio	-	-	M	-	-	M	-	-	B	-	-	B

Figura 6. Ejemplo de ficha de estimación de riesgos

Esta ficha pertenece al activo de código *SW.1* y nombre *Alexia* y detalla los valores de impacto y riesgo calculados para las diferentes amenazas que puede sufrir este activo.

Para cada amenaza, representadas en las diferentes filas de la ficha, se ha calculado su impacto y riesgo potencial. Para ello se han utilizado las tablas 14 y 15 y también el valor del activo y las degradaciones que puedan causar estas amenazas, valores que se han calculado en los apartados 7 y 8.

Para el cálculo del impacto acumulado, se ha observado qué activos dependen del SW.1 y se ha escogido, para cada dimensión de seguridad, el valor más alto de entre estos activos. Estos valores son los que se han utilizado para calcular el impacto acumulado de las diferentes amenazas y a partir de este, el riesgo acumulado.

Con el objetivo de compactar un poco la ficha de estimación de riesgos, se han sustituido los valores de las escalas de riesgos e impacto expuestas anteriormente. Así pues, las fichas del Anexo I utilizarán la siguiente escala de valores:

Valor	Valor Equivalente	Abreviatura
Crítico	Muy Alto	MA
Importante	Alto	A
Apreciable	Medio	M
Bajo	Bajo	B
Asumible	Muy Bajo	MB

Tabla 16. Valores para la estimación de riesgos

10. Evaluación de salvaguardas

Según la metodología MAGERIT es posible definir salvaguardas como "…aquellos procedimientos o mecanismos tecnológicos que reducen el riesgo de un sistema de información".

En la sección anterior del documento se ha realizado la estimación de riesgos para el centro sin tener en cuenta ningún tipo de salvaguardas. Esto permite identificar cuáles son los activos que están más expuestos a diferentes tipos de amenazas y sobre cuales se debe hacer más hincapié en cuanto a su protección.

Sin embargo, es impensable confiar el buen funcionamiento de ningún tipo de organización a un sistema de información sin salvaguardas puesto que, tal y como se ha analizado en la sección anterior, los riesgos a los que estaría expuesto serían muy altos.

Con el mismo objetivo de reducir el riesgo del centro, es posible identificar dos tipos de salvaguardas según como pretenden cumplir este objetivo. Por un lado, existen las salvaguardas que buscan reducir el impacto, es decir, limitar la degradación causada por una amenaza sobre un activo, mientras que otras salvaguardas se centrarán en reducir la probabilidad de que una amenaza se materialice y así reducir su riesgo.

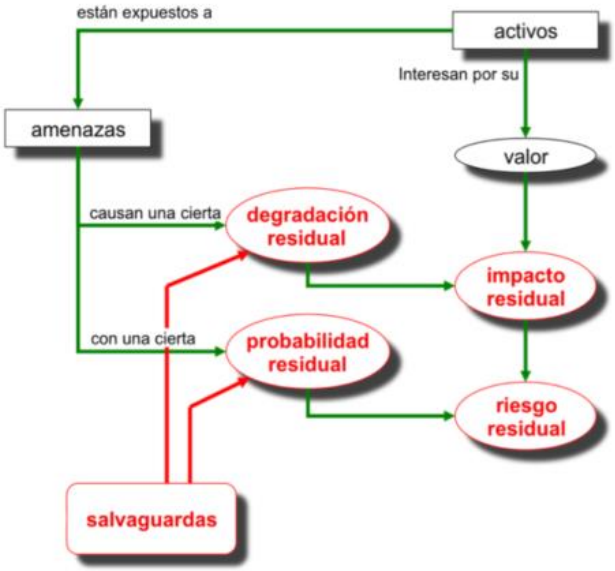

Ilustración 2. Efectos de las salvaguardas sobre el riesgo
Fuente: MAGERIT I

A continuación, se describen los diferentes tipos de salvaguardas existentes según la acción que realizan.

Tipo de Salvaguarda	Descripción	Efecto
[PR] Preventiva	Que busca reducir la probabilidad de que se materialice una amenaza. En caso de que la amenaza se materialice no afecta al impacto.	Reducir probabilidad
[DR] Disuasoria	Que busca reducir la probabilidad de que se produzca un ataque intencionado contra un activo intentando disuadir a los atacantes.	
[EL] Eliminatoria	Que pretende eliminar por completo la posibilidad de que se produzca una amenaza.	
[IM] Minimizadora	Aquellas que buscan limitar el impacto de una amenaza.	Reducir degradación
[CR] Correctiva	Medidas que, una vez se ha producido el daño, intentan repararlo para reducir el impacto.	
[RC] De recuperación	Aquellas que una vez se ha producido el daño, permiten al sistema regresar a un estado previo al incidente para reducir el daño.	
[MN] De monitorización	Salvaguardas que permiten monitorizar la actividad del sistema para poder recabar información a posteriori.	Consolidar el efecto de otras salvaguardas
[DC] De detección	Aquellas que si bien no impiden el ataque permiten una rápida detección y así tomar medidas para minimizar daños.	
[AW] De concienciación	Tareas de formación para evitar que las personas relacionadas con el sistema afecten negativamente a su seguridad.	
[AD] De administración	Procesos relacionados con la administración del sistema que permiten mejorar la seguridad del mismo.	

Tabla 17. Tipos de salvaguardas según su efecto

Para cada tipo de salvaguarda, existen un gran número de posibles salvaguardas que aplicar en la organización. Sin embargo, es importante realizar una selección de aquellas que pueden ser útiles analizando cuáles son los activos y dimensiones que se busca proteger, así como las amenazas frente a las que se está expuesto.

Además, es conveniente realizar una tarea de priorización teniendo en cuenta que conseguir un sistema "seguro" puede resultar más costoso que el valor de los activos a proteger. Así pues, la evaluación de salvaguardas se centrará en proteger los activos más valiosos y reducir los riesgos más elevados, evitando aquellas salvaguardas que, o bien no sean aplicables al sistema del centro, o bien no justifiquen su coste respecto al riesgo que tratan de reducir.

El proceso de evaluación de salvaguardas genera como salida un catálogo de posibles medidas que aplicar en el centro. Este catálogo se ha adjuntado como anexo en el plan de seguridad representado con una serie de tablas que reflejas las diferentes salvaguardas que se pueden aplicar.

A continuación, se detalla una de las tablas del Anexo I – [5. Evaluación de salvaguardas]

Media.2 – Memorias USB												
Amenazas	Salvaguardas	Probabilidad	Dimensiones			Impacto Res.			Riesgo Res.		
			C	I	D	C	I	D	C	I	D
A.7 – Uso no previsto	AW.1 – Elaborar normas del uso de TI	Media	M	M	M	M	B	M	M	B	M
A.15 – Modificación/Destrucción de info.	IM.1 – Cifrado de equipos hardware	Muy Baja	-	M	M	-	B	M	-	MB	B
	PR.3 – Control de acceso lógico	Muy Baja	-	M	M	-	B	M	-	MB	B
A.25 – Robo	PR.2 Control de acceso físico	Muy Baja	A	-	M	A	-	M	M	-	B
	IM.1 – Cifrado de equipos hardware	Baja	B	-	M	B	-	M	B	-	M
E.1 – Errores de los usuarios	AW.1 – Elaborar normas del uso de TI	Media	A	B	M	A	MB	M	A	MB	M
	RC.1 – Copias de seguridad periódicas	Muy Alta	A	B	B	A	MB	B	MA	B	M
E.25 – Pérdida de equipos	PR.2 Control de acceso físico	Muy Baja	A	-	M	A	-	M	M	-	B
	IM.1 – Cifrado de equipos hardware	Baja	B	-	M	B	-	M	B	-	M

Figura 6. Ejemplo de ficha de estimación de riesgos

Cada una de estas tablas se centra en un activo del sistema de información del centro para el cual se han listado todas las amenazas que pueden afectarle, tal y como se analizó en el apartado 8 del documento [8. Listado de amenazas].

Además, para cada una de estas amenazas se han enumerado las posibles salvaguardas que pueden ser aplicadas para reducir su riesgo.

La columna *Probabilidad* hace referencia a la probabilidad que tiene de suceder una amenaza tras aplicar una salvaguarda, mientras que la columna *Dimensiones* se refiere a la degradación que puede causar una amenaza sobre las diferentes dimensiones del activo habiendo aplicado ya la salvaguarda en cuestión. Para poder observar mejor cómo afectaría la implantación de una determinada medida se ha coloreado en morado el valor que ha cambiado con respecto al análisis de amenazas previo a la implantación de la salvaguarda.

Así por ejemplo para la amenaza *E.1 - Errores de los usuarios*, la salvaguarda *AW.1 - Elaborar normas del uso de TI* busca reducir la probabilidad de que se materialice la amenaza y ha bajado su probabilidad de Muy Alta a Media mientras que, para la misma amenaza, la salvaguarda *RC.1 - Copias de seguridad periódicas*, no afecta a la probabilidad de que esta se materialice, pero si disminuye la degradación que produce sobre la disponibilidad del activo de Medio a Bajo.

Por último, sabiendo como afecta cada salvaguarda a cada amenaza se ha calculado el impacto y riesgo residual de una amenaza sobre un activo tal y como se hizo en el apartado anterior, tomando el impacto como una relación de probabilidad y degradación y el riesgo como la relación entre impacto y valor. El riesgo residual es una medida fundamental que se utilizará en la toma de decisiones del siguiente apartado.

11. Gestión de Riesgos

A partir de las medidas de impacto y riesgo calculadas en los apartados anteriores, junto con otros factores como obligaciones legales, imagen pública, relaciones con los clientes u oportunidades de negocio, se realiza la toma de decisiones de cara a la evaluación y el tratamiento de riesgos.

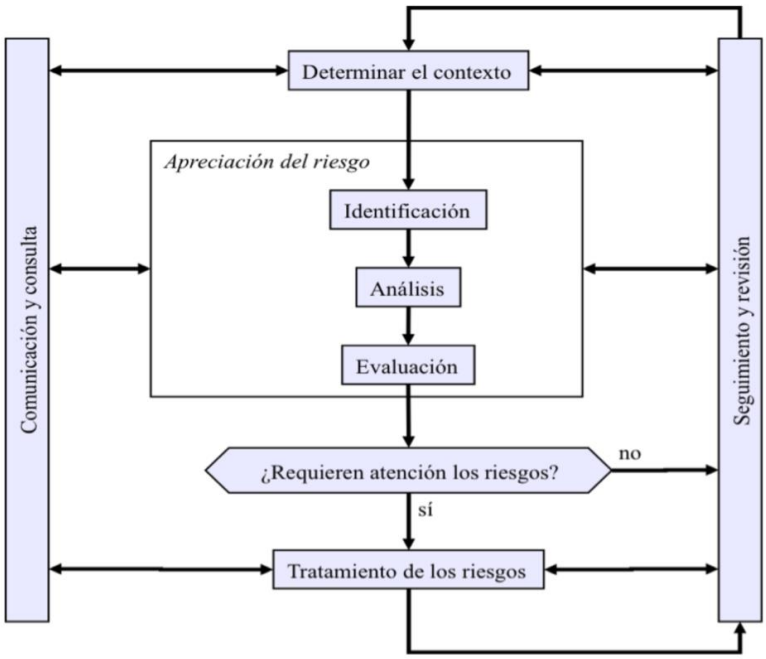

Ilustración 3. Proceso de evaluación de riesgos
Fuente: MAGERIT I

El proceso de evaluación de riesgos definido en MAGERIT consiste en, habiendo identificado los posibles riesgos a los que está expuesto el sistema de información de una organización, valorar cuáles deben ser tratados y cuáles de estos riesgos pueden ser asumidos por la organización en función de si son riesgos críticos, graves, apreciables o asumibles.

Para este proceso habitualmente se establece un umbral de impacto o riesgo aceptable para la organización. De esta forma los riesgos o impactos por debajo del umbral podrán ser asumidos por la organización, independientemente de que estos puedan ser tenidos en cuenta de cara a tomar otras decisiones como la creación de planes de contingencia o la creación de un fondo de emergencia.

Definido este umbral, el proceso consiste en analizar los diferentes riesgos identificados en apartados anteriores y valorar, para cada uno de ellos, si es un riesgo para el que se requiere tratamiento en función de la probabilidad de materialización, el impacto potencial o las

salvaguardas existentes. En caso de que el riesgo no sea aceptable se procederá con el siguiente proceso.

El segundo proceso perteneciente a la Gestión de Riesgos es el Tratamiento de Riesgos. En este proceso se decide cuál es el tratamiento a realizar para evitar los problemas que entrañan un riesgo alto. En este caso se tomarán las medidas necesarias para conseguir uno de los siguientes objetivos.

Tipo de Tratamiento	Descripción
Evitar	Puesta en marcha de medidas para eliminar un riesgo a partir de la eliminación de los elementos que causan el riesgo como pueden ser servicios, activos de información o procesos de la organización.
Mitigar	Medidas enfocadas a reducir el riesgo de forma preventiva, o bien reduciendo la probabilidad de que una amenaza se materialice, o bien reduciendo la degradación que causa esa amenaza sobre los activos.
Compartir	Reorganización de responsabilidades de forma que, si bien no se modifica ni la probabilidad ni los efectos negativos de un riesgo, se externaliza o se comparte su responsabilidad de forma que el impacto no recaiga únicamente sobre la organización.
Asumir	Junto con la decisión de asumir un riesgo habitualmente se ponen en marcha medidas que permitan, en caso de que se materialice una amenaza, poder hacerle frente, por ejemplo, la creación de planes de contingencia y continuidad, la creación de un fondo ante catástrofes o la contratación de un seguro.

Tabla 18. Formas de tratamiento de riesgo

En el tratamiento de riesgos, tal y como ya se ha comentado anteriormente, hay que tener en cuenta que conseguir un sistema casi seguro es muy caro y en la mayoría de las ocasiones el valor de los activos a proteger no compensará el coste de las salvaguardas necesarias. Es por esto por lo que en este proceso es necesario, para las diferentes amenazas, valorar cuáles son las medidas más oportunas teniendo en cuenta el tipo de tratamiento necesario, el valor de los activos a proteger, los valores de impacto y riesgo de una amenaza y el coste de las salvaguardas.

Para ello se realizan habitualmente estudios cuantitativos, en los que se analiza cuál es el coste de una salvaguarda y el dinero que se ahorra la organización con su implantación. Además, se suelen realizar también análisis cualitativos dónde se valora cuáles son los beneficios no económicos que obtiene la organización y el coste de las salvaguardas a implantar. Con esto se valoran los diferentes escenarios y medidas que se pueden poner en marcha y se decide como se han de tratar los riesgos de la organización.

En lo referente al proceso de evaluación y de cara a la aceptación de riesgos, se van a tomar como riesgos asumibles, es decir, aquellos sobre los que no se van a tomar ningún tipo de medida, los riesgos para los que en el apartado [Anexo I - 4. Estimación de riesgos] se haya establecido un riesgo bajo o muy bajo, que indica o bien que la probabilidad de que este se produzca es baja o que el impacto causado a la organización no es especialmente elevado.

Todas aquellas amenazas para las que se haya estimado un riesgo medio se considerarán riesgos apreciables y para estos, si bien no se llevarán a cabo medidas concretas para reducir su riesgo, se tratarán de forma colateral en las salvaguardas de concienciación y serán tenidos en cuenta para la elaboración de planes de contingencia y continuidad.

Por último, todas aquellas amenazas que entrañen un riesgo Alto o Muy Alto se evaluarán como riesgos graves o críticos respectivamente y para ellos se valorarán diferentes escenarios según la implantación de diferentes salvaguardas.

En el anexo de este documento [Anexo I - 6. Gestión de riesgos] se han organizado los riesgos en función de los activos a los que afectan. Para cada uno de estos subapartados, se han analizado los diferentes riesgos identificados en apartados anteriores clasificándolos en aceptables, apreciables, graves y críticos.

Para cada uno de estos riesgos se valora si son asumibles para el centro y en caso de no ser así se proponen varios escenarios aplicando diferentes salvaguardas. Además, se muestra como varía el mapa de riesgos en función de las salvaguardas aplicadas.

En el siguiente apartado de este documento se trabajará en profundidad los planes de seguridad centro teniendo en cuenta las salvaguardas especificadas en este apartado.

12. Plan de seguridad

En el apartado anterior se ha llevado a cabo el proceso de gestión de riesgos donde se han evaluado qué salvaguardas son necesarias para reducir los riesgos a niveles aceptables para el centro. Con la elección de esas salvaguardas el siguiente paso es crear programas de seguridad para implantar de forma controlada esas salvaguardas, y crear un plan de seguridad para gestionar estos proyectos.

Programas de seguridad

El primer paso en este apartado va a ser la creación de diferentes programas de seguridad.

Tras hacer la gestión de riesgos se conoce cuáles son las principales amenazas que ponen en riesgo el Sistema de Información del colegio y cuáles son las medidas que se deben tomar para reducir estos riesgos. Sin embargo, como se ha comentado a lo largo de todo el trabajo, la seguridad de un Sistema de Información no puede recaer en un conjunto de tareas o procesos independientes. En este apartado se van a crear diferentes programas de seguridad que permitirán implantar de manera organizada y controlada las diferentes salvaguardas propuestas tras el análisis de riesgos.

Para ello, en el [**¡Error! No se encuentra el origen de la referencia.**] se incluirán diferentes fichas para los programas que se vayan a realizar con la información necesaria para que el colegio pueda poner en marcha estos proyectos. En estas fichas se detallará para cada programa de seguridad la siguiente información:

- Identificador y nombre.
- Salvaguardas implementadas en el proyecto.
- Activos del sistema de información afectados.
- Estimación de costes, tanto económicos como de esfuerzo.
- Objetivos del proyecto.
- Descripción del proyecto y tareas que realizar para su puesta en funcionamiento.
- Controles y medidores para medir la efectividad de las medidas implantadas.

Para poder realizar estas fichas es necesario contar con los catálogos de activos y amenazas, además de los resultados del análisis de riesgos expuesto en apartados anteriores, que será el que determine que salvaguardas se deben aplicar en los diferentes programas de seguridad.

Con estas fichas se pretende conseguir que el centro tenga los recursos y la información necesaria para poder poner en marcha las diferentes medidas propuestas, ya sea por el propio personal del centro o por personal ajeno al centro que se dedique específicamente a este sector.

Si bien en el apartado anterior se han identificado todas las salvaguardas que permitirían mejorar la seguridad del Sistema de Información del centro, en estos programas de seguridad no se van a incluir todas las salvaguardas propuestas. La razón es que, aunque se analizará en el siguiente apartado, estos programas de seguridad se organizan para realizarlos en un periodo de tiempo medio (Generalmente unos 2 o 3 años). En el **¡Error! No se encuentra el origen de la r eferencia.** se han descrito los programas de seguridad pensados para poner en marcha en ese periodo y el resto de las medidas propuestas quedarían pendientes para su implantación.

Estos programas de seguridad han sido diseñados para que puedan llevarse a cabo por parte del personal del centro. Precisamente por este hecho, los programas de seguridad diseñados establecen las pautas generales para la implantación de estos proyectos en un tiempo estimado (teniendo en cuenta la carga de trabajo del personal del centro) de forma que puedan llevarse a cabo acciones sencillas que mejoren la seguridad en el centro.

Previsiblemente, por la falta de conocimiento en el ámbito de los profesores del centro, la implantación de estas medidas no tendrá la eficacia que podría. Sin embargo, el establecimiento de métricas y controles previsto en los programas de seguridad permitirán monitorizar y analizar los resultados de estos programas para poder evaluar y mejorar su efectividad.

Plan de seguridad

Definidos los programas de seguridad es necesario organizarlos en un plan de seguridad también llamado plan director.

Un plan director se centra, generalmente, en un plazo de tiempo de unos 2 o 3 años y define los programas de seguridad y las medidas a tomar en ese plazo, en este caso el plan de seguridad se ha diseñado para los próximos dos años. El objetivo es definir en esos 2 años como se van a organizar los programas de seguridad propuestos en el apartado anterior. Para ello se tendrá en cuenta la duración y el coste de los programas, la urgencia de implantación (Teniendo en cuenta si el riesgo que buscan mitigar es más o menos crítico), la capacidad del personal…

Teniendo en cuenta que el centro no cuenta con personal específico para implantar estos programas, se ha estructurado el plan de seguridad de forma que no se trabaje en la implantación de dos programas de forma paralela para intentar reducir el esfuerzo realizado por

el profesorado. Así, la puesta en marcha de los diferentes programas de seguridad se llevará a cabo por parte de los responsables de cada programa en el tiempo establecido con una carga de trabajo de 2 horas semanales correspondientes a las horas de trabajo complementario del profesorado.

Se ha estructurado el plan de seguridad de forma que los primeros proyectos estén enfocados a los activos con mayor riesgo y posponiendo los programas con mayor coste para que el centro tenga capacidad para ahorrar ese dinero.

Así, el plan director estructura los proyectos a realizar en los próximos 2 años de la siguiente forma:

1er año (2020):

- DOC02 - Creación de políticas TI
- REC01 - Gestión de Backup
- PRE01 - Control de acceso lógico
- PRE03 - Gestión de la seguridad en Internet

2º año (2020):

- DOC01 - Formalizar procedimientos
- DOC03 - Crear plan de contingencia
- PRE02 - Gestión de la seguridad hardware

A continuación, se adjunta el cronograma planificado para la elaboración del plan de seguridad teniendo en cuenta los meses de trabajo en dos cursos escolares.

		Curso 2019/2020												Curso 2020/2021											
Programas de seguridad	Tiempo	S	O	N	D	E	F	M	A	M	J	J	A	S	O	N	D	E	F	M	A	M	J	J	A
DOC01 - Formalizar procedimientos	4 meses																								
DOC02 - Creación de políticas TI	4 meses																								
DOC03 - Crear plan de contingencia	4 meses																								
REC01 - Gestión de Backup	2 meses																								
PRE01 - Control de acceso lógico	3 meses																								
PRE02 - Gestión de la seguridad Hardware	3 meses																								
PRE03 – Gestión de la seguridad en Internet	3 meses																								

Tabla 19. Cronograma del plan de seguridad

Estado final del SGSI

Con el objetivo de valorar como de seguro será el Sistema de Información del centro después de realizar este plan de seguridad, se va a evaluar el estado del SGSI como ya se hizo en el apartado [4.3 Estado inicial del Sistema de Información].

El objetivo es, a través de un análisis formal y siguiendo las métricas propuestas por la normativa ISO 27000 valorar el grado de implantación del SGSI y valorar como ha cambiado con respecto al estado inicial. A continuación, se adjuntan los resultados de este análisis.

Valoración	Descripción
L0 – No implementado	No se lleva a cabo el control de seguridad en los sistemas de información.
L1 – Inicial / Ad-hoc	Procedimientos existentes, pero sin un proceso formal definido. Su éxito depende de esfuerzos personales.
L2 – Reproducible pero intuitivo	Existe un método de trabajo, pero sin comunicación formal, depende del conocimiento del propio individuo y no hay formación del personal.
L3 – Proceso definido	El proceso se lleva a cabo conforme a la documentación especificada que ha sido administrada por la organización.
L4 – Gestionado y medible	Se puede realizar un seguimiento de la evolución del proceso a través de datos estadísticos.
L5 – Optimizado	Los procesos están implementados según un procedimiento documentado que es medido periódicamente y están en constante mejora
N/A – No Aplica	O bien es un aspecto que no tiene cabida dentro del contexto de la organización o bien su gestión es externa a la propia organización.

Tabla 20. Leyenda para la evaluación final del SGSI

Estado final del SGSI	
4. Contexto de la organización	
4.1 Comprensión de la organización y de su contexto	L3 – Proceso definido
oc4.2 Comprensión de las necesidades y expectativas de las partes interesadas	L2 – Reproducible pero intuitivo
4.3 Determinación del alcance del SGSI	L2 – Reproducible pero intuitivo
4.4 Sistema de gestión de la seguridad de la información	L3 – Proceso definido
5. Liderazgo	
5.1 Liderazgo y compromiso	L1 – Inicial / Ad-hoc
5.2 Política	L3 – Proceso definido
5.3 Roles, responsabilidades y autoridades en la organización	L4 – Gestionado y medible
6. Planificación	
6.1 Acciones para tratar los riesgos y oportunidades	
6.1.1 Consideraciones generales	L4 – Gestionado y medible
6.1.2 Apreciación de riesgos de seguridad de la información	L4 – Gestionado y medible
6.1.3 Tratamiento de los riesgos de la seguridad de la información	L4 – Gestionado y medible
6.2 Objetivos de seguridad y planificación para su consecución	L4 – Gestionado y medible
7. Soporte	
7.1 Recursos	L2 – Reproducible pero intuitivo
7.2 Competencia	L3 – Proceso definido
7.3 Concienciación	L4 – Gestionado y medible
7.4 Comunicación	L4 – Gestionado y medible
7.5 Información documentada	

7.5.1 Consideraciones generales	L4 – Gestionado y medible
7.5.2 Creación y actualización	L4 – Gestionado y medible
7.5.3 Control de la información documentada	L4 – Gestionado y medible
8. Operación	
8.1 Planificación y control operacional	L3 – Proceso definido
8.2 Apreciación de los riesgos de seguridad de la información	L4 – Gestionado y medible
8.3 Tratamiento de los riesgos de seguridad de la información	L3 – Proceso definido
9. Evaluación del desempeño	
9.1 Seguimiento, medición, análisis y evaluación	L3 – Proceso definido
9.2 Auditoría interna	L0 – No implementado
9.3 Revisión por la dirección	L0 – No implementado

Tabla 21. Análisis del estado final según la ISO 27001

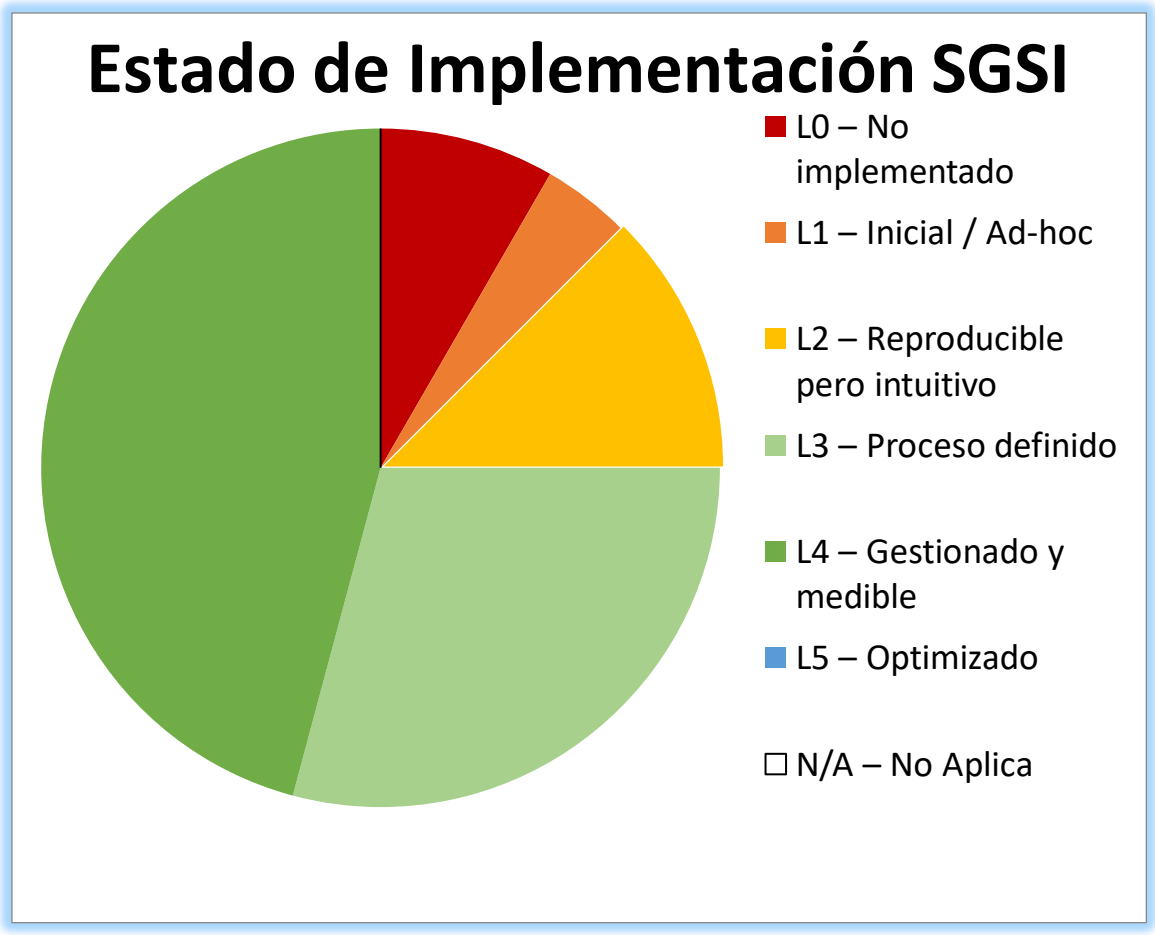

Figura 4. Resumen del estado final según la ISO 27000

Con este gráfico y en comparación al que se realizó previo al estudio del SGSI del centro se pueden observar varias cosas.

En primer lugar, se observa que la mayoría de las cuestiones que antes se definían como “L0 – No implementado” o “L1 – Inicial / Ad-hoc han cambiado. Es lógico que muchas cuestiones, teniendo en cuenta que en el colegio nunca se había realizado ningún proceso para asegurar la información del centro, estuvieran sin implementar o en un estado muy básico, pero a lo largo de este trabajo se ha ido trabajando para cambiar esta situación.

Por otro lado, se puede observar también que mientras que antes no había ninguna cuestión que superara el nivel “L2 – Proceso definido” ahora muchas tienen nivel “L4 – Gestionado y medible”. Esta cuestión se debe a que los niveles superiores a L2 requieren que haya una documentación que defina como se ha realizado el proceso. En el colegio no había nada de documentación que definiera los procesos de gestión interna del centro y por ello se ha hecho mucho énfasis en los programas de seguridad en que se definan estos procesos en diferentes documentos.

Por último, valorando como quedaría el estado del SGSI después de aplicar el plan de seguridad propuesto, no habría ninguna cuestión que llegara al nivel “L5 – Optimizado”. Para llegar a este nivel es necesario no solo tener un proceso definido, organizado y con indicadores que midan su efectividad, sino que se tiene que llevar a cabo un proceso continuo de mejora de estos planes. En este trabajo no se han abordado ese tipo de medidas, sino que se ha centrado en cosas más concretas y sencillas para que pudiera abordar el personal del centro para mejorar en la medida de lo posible la seguridad de la información del colegio.

13. Conclusiones y trabajo futuro

El presente trabajo surge de la idea de intentar ampliar mis conocimientos en seguridad informática y aplicar los conocimientos adquiridos a lo largo del grado de Ingeniería Informática en una empresa que no estuviera específicamente relacionada con el sector. A partir de ahí surge la idea de trabajar con el centro escolar donde cursé la educación secundaria para implantar un Sistema de Gestión de la Seguridad de la Información. Todo ello según lo recogido en la normativa ISO 27000 y siguiendo la metodología MAGERIT.

Los objetivos del trabajo se estructuraban en 3 bloques: Hacer un análisis de la situación actual del centro con relación a su Sistema de Información, diseñar un plan de seguridad para mejorar la seguridad de la información del centro y colaborar con el colegio en la implantación de alguna de las medidas propuestas.

Con respecto al objetivo de analizar la situación del centro, se ha hecho un estudio analítico basado en el marco de trabajo propuesto por la metodología MAGERIT que ha permitido obtener una visión general de los activos importantes para el sistema de información del centro, las amenazas a los que están expuestos y el riesgo que estas suponen y finalmente la identificación de las salvaguardas aplicables para afrontar esta situación

Con respecto al segundo boque de objetivos, se han diseñado 7 programas de seguridad que buscan reducir, en función de diferentes estrategias, el riesgo al que está expuesto el sistema de información aportando las pautas para que el personal del centro pueda poner en marcha estos planes y mejorar la seguridad de la información del colegio.

Como trabajo futuro inmediato, queda por un lado presentar los resultados de este trabajo al colegio para que puedan empezar a trabajar y a poner en marcha el plan de seguridad propuesto y por otro participar en la implantación de los programas de seguridad. Para eso, y según lo marcado por uno de los objetivos de este trabajo, mi intención es colaborar con el colegio en la creación de las políticas sobre el uso de las TI o bien en el propio desarrollo del documento que recoja estas políticas, o bien participando con alumnos y profesores en las actividades de concienciación sobre esta cuestión.

Como trabajo a largo plazo queda ampliar lo expuesto en el trabajo para acabar de cubrir todos los riesgos identificados y que no se han cubierto con lo recogido en el plan de seguridad además de evaluar la eficiencia de las medidas propuestas para optimizar el Sistema de Gestión de la Seguridad de la Información del colegio.

A modo de reflexión, considero que probablemente para una organización de este ámbito, como es en este caso un centro educativo concertado de tamaño pequeño, no sea interesante el llevar a cabo grandes esfuerzos para conseguir una certificación ISO para la seguridad de la información como es la ISO 27000 abordada en este trabajo. En primer lugar, porque esto requiere un gran esfuerzo por parte de la organización del centro y en segundo lugar porque probablemente tener o no esta certificación no es un hecho diferencial para el éxito del colegio.

Sin embargo, me parece vital que en este tipo de organizaciones se realicen esfuerzos para garantizar la seguridad de su información, independientemente de que estos esfuerzos vayan acompañados o no de un reconocimiento o certificación. Por un lado, porque a nivel legal según lo establecido en el Reglamento General de Protección de Datos, la información es un activo muy a tener en cuenta y que habitualmente está muy desprotegido, lo cual puede conllevar problemas jurídicos. Y, en segundo lugar, porque la realización de actividades como las efectuadas a lo largo de este trabajo permiten mejorar la gestión interna de una organización, evitar problemas derivados de una mala gestión de riesgos o llevar a cabo medidas que permitan al personal de una organización mejorar su desempeño en su actividad laboral. Con lo cual, tanto si el esfuerzo realizado conlleva la obtención de un reconocimiento como si no, si se obtienen beneficios importantes de este esfuerzo.

Referencias[1]

1. European Commission (2018). *Digital Economy and Society Index Report 2018*. https://ec.europa.eu/digital-single-market/en/integration-digital-technology
2. Bankia (Ed.) (2017*). Informe Bankia Índicex 2016: La digitalización de las empresas en España.* https://kblsolutions.es/wp-content/uploads/2018/05/Informe-Bankia-Indicex-2016.pdf
3. ISO/IEC 27000 family – Information security management systems https://www.iso.org/isoiec-27001-information-security.html
4. María Jesús Recio. Responsable de Calidad de Servicios de Indra. (2012). *De la seguridad informática a la seguridad de la información*. https://www.aec.es/c/document_library/get_file?uuid=e25028ca-cb3b-4ffd-ada0-4ce2efa86f80&groupId=10128
5. Asociación Española de Normalización y Certificación (2014). *Normativa ISO/IEC 27000* http://www.iso27000.es/iso27000.html
6. Asociación Española de Normalización y Certificación (2017). UNE-EN ISO/IEC 27002
7. Asociación Española de Normalización y Certificación (2008). *UNE 71504:2008 – Metodología de análisis y gestión de riesgos para los sistemas de información.* https://www.une.org/encuentra-tu-norma/busca-tu-norma/norma/?c=N0041430
8. Ministerio de Hacienda y Administraciones Públicas (2012*). MAGERIT. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro I.* https://www.ccn-cert.cni.es/documentos-publicos/1789-magerit-libro-i-metodo/file.html
9. International Organization for Standarization (2018). *ISO31000:2018 – Sistemas de Gestión de Riesgos y Seguridad* https://www.iso.org/iso-31000-risk-management.html
10. Departament d'educació de la Generalitat de Catalunya. *Sitio web oficial de la plataforma Agora* https://agora.xtec.cat/moodle/moodle/

[1] Las referencias presentadas en este trabajo han sido comprobadas a fecha de 14/05/2019

11. Consejería de educación de la Junta de Andalucía. *Sistema de información para la gestión de los Centros de enseñanza en la junta de Andalucía (SÉNECA-PASSEN)* https://administracionelectronica.gob.es/pae_Home/dam/jcr:7497eea1-1766-481c-9bcf-f845aa446080/sistema_de_informacion_para_la_gestion.pdfADKk5RrZGQjejbdb
12. Consellería d'Educació de la Generalitat Valenciana. *Sitio web oficial de la plataforma Itaca* http://www.ceice.gva.es/webitaca/es/index.asp
13. Consellería d'Educació de la Generalitat Valenciana. *Guía de utilización del módulo Docent 2* http://www.ceice.gva.es/webitaca/docs/moduls/modul_docent2.pdf
14. Educaria. *Sitio web oficial de Alexia – Suite educativa* www.alexiaeducaria.com/
15. Parlamento Europeo (2016). *Reglamento General de Protección de datos* https://www.boe.es/doue/2016/119/L00001-00088.pdf
16. Gobierno de España (2014). *Boletín oficial del estado – Ley de propiedad intelectual.* https://www.boe.es/boe/dias/2014/11/05/pdfs/BOE-A-2014-11404.pdf
17. Gobierno de España (2019). *Boletín oficial del estado*.

Anexo I – Análisis de Seguridad

1. Introducción y objetivos del plan de seguridad

Hoy en día vivimos en una sociedad digital, estamos permanentemente conectados con acceso a Internet desde prácticamente cualquier dispositivo y aunque esto nos ofrece un amplio abanico de posibilidades, no siempre estamos preparados para hacer frente a esta realidad.

Están a la orden del día las noticias sobre brechas de seguridad, robo de datos o pérdidas de información y muchas de estas situaciones vienen provocadas debido a un mal uso de las tecnologías de información o al desconocimiento sobre estas.

Un Plan Director de Seguridad está formado por una serie de procesos que permiten reducir los riesgos a los que está expuesta una organización.

El objetivo de este documento es analizar los activos de los que consta el centro, valorar las amenazas a los que están expuestos y realizar una valoración de riesgo, para posteriormente proponer una serie de medidas o salvaguardas que permitan reducir el riesgo al que está expuesto el sistema de información del colegio. Con los resultados del análisis realizado en este documento posteriormente se creará un Plan de Seguridad, para afianzar la seguridad de la información del centro.

Además, con el propósito de ver la situación inicial del centro con respecto a la elaboración de un plan de seguridad, se ha realizado un análisis del estado inicial del centro evaluando los aspectos obligatorios a tener en cuenta según la normativa ISO 27000. En esta evaluación se han clasificado los diferentes aspectos de las siguiente manera:

Valoración	Descripción
L0 – No implementado	No se lleva a cabo el control de seguridad en los sistemas de información.
L1 – Inicial / Ad-hoc	Procedimientos existentes, pero sin un proceso formal definido. Su éxito depende de esfuerzos personales.
L2 – Reproducible pero intuitivo	Existe un método de trabajo, pero sin comunicación formal, depende del conocimiento del propio individuo y no hay formación del personal.
L3 – Proceso definido	El proceso se lleva a cabo conforme a la documentación especificada que ha sido administrada por la organización.
L4 – Gestionado y medible	Se puede realizar un seguimiento de la evolución del proceso a través de datos estadísticos.
L5 – Optimizado	Los procesos están implementados según un procedimiento documentado que es medido periódicamente y están en constante mejora
N/A – No Aplica	O bien es un aspecto que no tiene cabida dentro del contexto de la organización o bien su gestión es externa a la propia organización.

Tabla 1. Leyenda para la evaluación inicial del SGSI

A continuación, se presentan los resultados de este análisis inicial del centro con los requerimientos evaluados y su nivel de implantación.

Estado Inicial del SGSI	
4. Contexto de la organización	
4.1 Comprensión de la organización y de su contexto	L2 – Reproducible pero intuitivo
4.2 Comprensión de las necesidades y expectativas de las partes interesadas	L1 – Inicial / Ad-hoc
4.3 Determinación del alcance del SGSI	L0 – No implementado
4.4 Sistema de gestión de la seguridad de la información	L0 – No implementado
5. Liderazgo	
5.1 Liderazgo y compromiso	L1 – Inicial / Ad-hoc
5.2 Política	L2 – Reproducible pero intuitivo
5.3 Roles, responsabilidades y autoridades en la organización	L2 – Reproducible pero intuitivo
6. Planificación	
6.1 Acciones para tratar los riesgos y oportunidades	
6.1.1 Consideraciones generales	L1 – Inicial / Ad-hoc
6.1.2 Apreciación de riesgos de seguridad de la información	L0 – No implementado
6.1.3 Tratamiento de los riesgos de la seguridad de la información	L0 – No implementado
6.2 Objetivos de seguridad y planificación para su consecución	L1 – Inicial / Ad-hoc
7. Soporte	
7.1 Recursos	L2 – Reproducible pero intuitivo
7.2 Competencia	L2 – Reproducible pero intuitivo
7.3 Concienciación	L1 – Inicial / Ad-hoc
7.4 Comunicación	L2 – Reproducible pero intuitivo
7.5 Información documentada	
7.5.1 Consideraciones generales	L0 – No implementado
7.5.2 Creación y actualización	L0 – No implementado
7.5.3 Control de la información documentada	L0 – No implementado
8. Operación	
8.1 Planificación y control operacional	L2 – Reproducible pero intuitivo
8.2 Apreciación de los riesgos de seguridad de la información	L0 – No implementado
8.3 Tratamiento de los riesgos de seguridad de la información	L0 – No implementado
9. Evaluación del desempeño	
9.1 Seguimiento, medición, análisis y evaluación	L0 – No implementado
9.2 Auditoría interna	L0 – No implementado
9.3 Revisión por la dirección	L0 – No implementado

Tabla 2. Análisis del estado inicial del SGSI

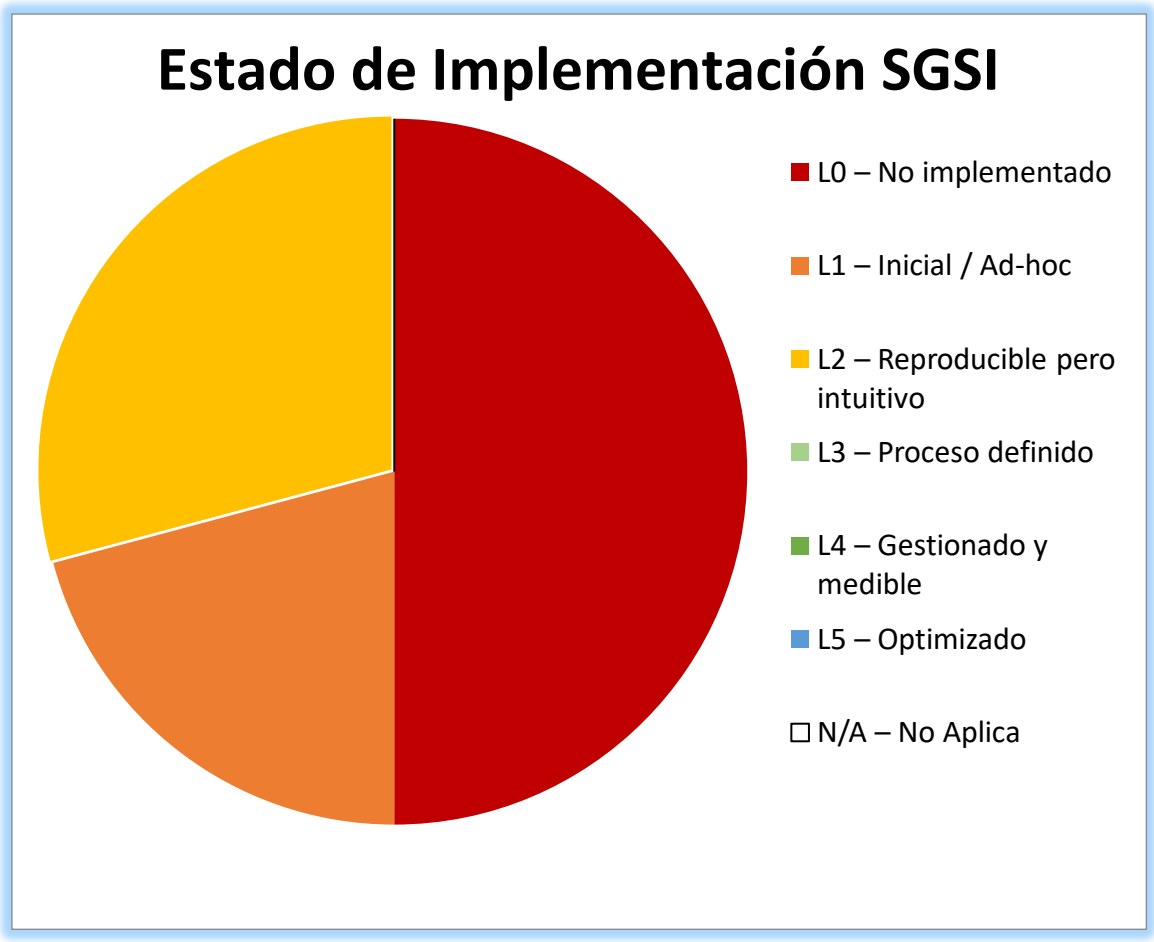

Figura 1. Resumen del estado inicial del SGSI

Debido a que en el centro actualmente no se ha realizado ningún esfuerzo para implantar un SGSI es normal que la mayoría de las cuestiones a evaluar presentan un nivel de implementación muy bajo. El objetivo de este proyecto es cambiar esta situación y que el esfuerzo realizado se refleje en un conjunto de procesos implementados y medidos que permitan mejorar la seguridad de la información del centro.

2. Catálogo de activos

En el ámbito de los sistemas de información, la UNE 71504, define un activo como "*Componente o funcionalidad de un sistema de información que tiene algún valor para la organización y es susceptible de ser atacado deliberada o accidentalmente*".

Para la gestión de la seguridad de la información resulta vital realizar un catálogo con los activos a proteger en una organización. Para esto se han de identificar todos los activos del colegio, valorar las dependencias que existen entre los mismos y asignar a cada activo un valor que está relacionado con el grado de perjuicio que conllevaría perder ese activo.

A continuación, se desarrolla en diferentes fichas el catálogo de activos del centro.

<table>
<tr><th colspan="6">[D] Datos</th></tr>
<tr><td colspan="3">Código: D.1</td><td colspan="3">Nombre: Datos de matrícula</td></tr>
<tr><td colspan="6">Descripción: Información generada por el centro a través del proceso de matrícula.</td></tr>
<tr><td colspan="6">Tipo: Ficheros</td></tr>
<tr><th colspan="6">Dependencias</th></tr>
<tr><td colspan="3">Activos: SW.2</td><td colspan="3">Grado: Muy Alto</td></tr>
<tr><td colspan="6">¿Por qué? Todos los datos de matrícula, una vez finalizado el periodo de matrícula deben introducirse en la plataforma de Itaca para que desde la Consellería d'Educació tengan acceso a estos datos.</td></tr>
<tr><td colspan="3">Activos: Media.1</td><td colspan="3">Grado: Alto</td></tr>
<tr><td colspan="6">¿Por qué? Todos los datos de matrícula, además de ser introducidos en la plataforma de Itaca se almacenan en los discos duros de administración incluso antes de introducirse en la plataforma online.</td></tr>
<tr><th colspan="6">Valor</th></tr>
<tr><th>Total</th><th>Confidencialidad</th><th>Integridad</th><th>Disponibilidad</th><th>Autenticidad</th><th>Trazabilidad</th></tr>
<tr><td>Muy Alto</td><td>Muy Alto</td><td>Muy Alto</td><td>Medio</td><td>Muy Alto</td><td>Alto</td></tr>
</table>

[D] Datos					
Código: D.2			**Nombre:** Expedientes académicos		
Descripción: Información relacionada con el expediente académico de los estudiantes como pueden ser calificaciones, asistencia a clases o partes disciplinarios.					
Tipo: Ficheros					
Dependencias					
Activos: SW.2			**Grado:** Alto		
¿Por qué? Todos los datos relacionados con los expedientes académicos de los alumnos deben introducirse en la plataforma de Itaca para que desde la Consellería d'Educació tengan acceso a estos datos.					
Valor					
Total	**Confidencialidad**	**Integridad**	**Disponibilidad**	**Autenticidad**	**Trazabilidad**
Muy Alto	Muy Alto	Muy Alto	Medio	Muy Alto	Alto

[D] Datos					
Código: D.3			**Nombre:** Material pedagógico		
Descripción: Material del personal docente necesario para la realización de las clases como presentaciones, vídeos, tutoriales o libros.					
Tipo: Ficheros					
Dependencias					
Activos: Media.3, Media.2, Media.4			**Grado:** Bajo		
¿Por qué? Los profesores pueden decidir de forma personal almacenar su material docente en alguna plataforma de almacenamiento en la nube o con un dispositivo USB.					
Activos: HW.4			**Grado:** Bajo		
¿Por qué? Algunas asignaturas están planteadas para que parte de la asignatura se trabaje con Chromebook para utilizar herramientas TIC en algunas lecciones.					
Valor					
Total	**Confidencialidad**	**Integridad**	**Disponibilidad**	**Autenticidad**	**Trazabilidad**
Bajo	Muy Bajo	Muy Bajo	Bajo	Muy Bajo	Bajo

[D] Datos					
Código: D.4			**Nombre:** Copias de seguridad		
Descripción: Copias de seguridad realizadas automáticamente cada tres horas de los datos almacenados en el servidor de secretaría que se vuelcan a un disco duro externo.					
Tipo: Backup					
Dependencias					
Activos: Media.1			**Grado:** Muy Alto		
¿Por qué? Las copias de seguridad únicamente se almacenan en discos duros externos así que la disponibilidad de estas copias de seguridad depende enteramente del buen funcionamiento de estos discos duros.					
Valor					
Total	**Confidencialidad**	**Integridad**	**Disponibilidad**	**Autenticidad**	**Trazabilidad**
Alto	Muy Alto	Muy Alto	Medio	Medio	Medio

[D] Datos					
Código: D.5			**Nombre:** Programación General Anual		
Descripción: Documento de gestión interna que define el conjunto de actuaciones y proyectos que llevar a cabo en el centro a lo largo del año.					
Tipo: Datos de gestión interna					
Dependencias					
Activos: SW.2			**Grado:** Medio		
¿Por qué? El colegio está obligado a publicar su programación general anual en la plataforma Itaca para que desde Consellería d'Educació tengan acceso a este documento.					
Activos: Media.4			**Grado:** Medio		
¿Por qué? El colegio está obligado a almacenar una copia impresa de esta documento en las instalaciones del centro.					
Valor					
Total	**Confidencialidad**	**Integridad**	**Disponibilidad**	**Autenticidad**	**Trazabilidad**
Alto	Muy Bajo	Alto	Bajo	Alto	Muy Bajo

[D] Datos					
Código: D.6			**Nombre:** Comunicación con familias		
Descripción: Documentos generados a partir de la comunicación con familias por correo electrónico o tutorías virtuales.					
Tipo: Datos de gestión interna					
Dependencias					
Activos: SW.1			**Grado:** Alto		
¿Por qué? Toda la comunicación virtual con las familias se realiza a través de la plataforma Alexia.					
Valor					
Total	**Confidencialidad**	**Integridad**	**Disponibilidad**	**Autenticidad**	**Trazabilidad**
Medio	Medio	Medio	Bajo	Medio	Muy Bajo

[S] Servicios					
Código: S.1			**Nombre:** Servicio Web		
Descripción: Página web creada por el departamento de TIC con información general sobre el centro.					
Tipo: Anónimo, WWW					
Dependencias					
Activos: HW.1			**Grado:** Muy Alto		
¿Por qué? La página web está almacenada en un servidor web contratado a una empresa externa al centro.					
Valor					
Total	**Confidencialidad**	**Integridad**	**Disponibilidad**	**Autenticidad**	**Trazabilidad**
Bajo	N/A	N/A	Medio	Muy Bajo	Muy Bajo

[S] Servicios					
Código: S.2			**Nombre:** Servicio de correo electrónico		
Descripción: Servicio de correo electrónico proporcionado por el colegio para que los alumnos tengan un usuario con el que acceder a la plataforma educativa de Google.					
Tipo: Interno, Email					
Dependencias					
Activos:			**Grado:**		
¿Por qué?					
Valor					
Total	**Confidencialidad**	**Integridad**	**Disponibilidad**	**Autenticidad**	**Trazabilidad**
Alto	N/A	N/A	Muy Alto	Muy Alto	Muy Alto

[S] Servicios					
Código: S.3			**Nombre:** Classroom online		
Descripción: Plataforma para la docencia online dónde el profesorado puede subir material y los alumnos acceder a este contenido.					
Tipo: Interno, Almacenamiento de ficheros.					
Dependencias					
Activos:			**Grado:**		
¿Por qué?					
Valor					
Total	**Confidencialidad**	**Integridad**	**Disponibilidad**	**Autenticidad**	**Trazabilidad**
Muy Alto	N/A	N/A	Muy Alto	Alto	Alto

[SW] Software					
Código: SW.1			**Nombre:** Alexia		
Descripción: Herramienta privada para la gestión de la información administrativa del centro, la información pedagógica y la comunicación con las familias. En proceso de migración. Ahora únicamente se usa como herramienta para la comunicación con las familias.					
Tipo: Desarrollo a medida, Servidor de aplicaciones					
Dependencias					
Activos: COM.2, COM.3			**Grado:** Muy Alto		
¿Por qué? Para el uso de Alexia, como plataforma web es necesario conexión a Internet o bien a través de red WiFi o a través de red ADSL					
Valor					
Total	**Confidencialidad**	**Integridad**	**Disponibilidad**	**Autenticidad**	**Trazabilidad**
Alto	N/A	N/A	Alto	Muy Alto	Muy Alto

[SW] Software					
Código: SW.2			**Nombre:** Itaca		
Descripción: Herramienta creada por la Consellería d'Educació para la gestión de la información administrativa del centro. Todos los datos de la gestión interna del centro deben estar almacenados en esta plataforma para que desde la Generalitat Valenciana tengan acceso a ellos.					
Tipo: Servidor de aplicaciones					
Dependencias					
Activos: COM.2, COM.3			**Grado:** Muy Alto		
¿Por qué? Para el uso de Itaca, como plataforma web es necesario conexión a Internet o bien a través de la red WiFi o a través de la red ADSL					
Valor					
Total	**Confidencialidad**	**Integridad**	**Disponibilidad**	**Autenticidad**	**Trazabilidad**
Muy Alto	N/A	N/A	Alto	Muy Alto	Muy Alto

[SW] Software					
Código: SW.3			**Nombre:** Aplicaciones ofimática		
Descripción: Aplicaciones con licencia, o de código abierto, para ofimática básica como OpenOffice o la suite ofimática de Microsoft					
Tipo: Ofimática					
Dependencias					
Activos:			**Grado:**		
¿Por qué?					
Valor					
Total	**Confidencialidad**	**Integridad**	**Disponibilidad**	**Autenticidad**	**Trazabilidad**
Medio	N/A	N/A	Medio	Muy Bajo	Muy Bajo

[SW] Software					
Código: SW.4			**Nombre:** Cliente de correo electrónico		
Descripción: Clientes de correo electrónico para el profesorado que permite la comunicación con las familias de los alumnos.					
Tipo: Cliente de correo					
Dependencias					
Activos: COM.2, COM.3			**Grado:** Muy Alto		
¿Por qué? Para el uso de un cliente de correo web es necesario conexión a Internet o bien a través de la red WiFi o a través de la red ADSL.					
Valor					
Total	**Confidencialidad**	**Integridad**	**Disponibilidad**	**Autenticidad**	**Trazabilidad**
Medio	N/A	N/A	Bajo	Muy Alto	Muy Alto

[SW] Software					
Código: SW.5			**Nombre:** Aplicación de antivirus		
Descripción: Aplicación de antivirus freeware para los ordenadores del centro.					
Tipo: Antivirus					
Dependencias					
Activos:			**Grado:**		
¿Por qué?					
Valor					
Total	**Confidencialidad**	**Integridad**	**Disponibilidad**	**Autenticidad**	**Trazabilidad**
Bajo	N/A	N/A	Bajo	Muy Bajo	Muy Bajo

[HW] Hardware					
Código: HW.1			**Nombre:** Servidor Web		
Descripción: Servidor donde se almacena la página web del colegio. No está físicamente en el colegio, sino que está contratado a una empresa que proporciona este servicio.					
Ubicación: Externo a las instalaciones del centro					
Tipo:					
Dependencias					
Activos:			**Grado:**		
¿Por qué?					
Valor					
Total	**Confidencialidad**	**Integridad**	**Disponibilidad**	**Autenticidad**	**Trazabilidad**
Bajo	N/A	N/A	Bajo	N/A	N/A

[HW] Hardware					
Código: HW.2			**Nombre:** Ordenadores para alumnado		
Descripción: Ordenadores personales situados en las aulas de informática para las clases de informática utilizados por los alumnos.					
Ubicación: Aulas de informática					
Tipo: PC					
Dependencias					
Activos: COM.2, COM.3			**Grado:** Medio		
¿Por qué? La mayoría de las ocasiones en las que los alumnos trabajan con ordenadores es para tener acceso a internet, y por tanto dependen de las redes de acceso a Internet.					
Activos: HW.7			**Grado: Medio**		
¿Por qué? El acceso a internet de los ordenadores de los alumnos se realiza a través del Switch.					
Valor					
Total	**Confidencialidad**	**Integridad**	**Disponibilidad**	**Autenticidad**	**Trazabilidad**
Bajo	N/A	N/A	Bajo	N/A	N/A

[HW] Hardware					
Código: HW.3			**Nombre:** Ordenadores para profesorado		
Descripción: Ordenadores portátiles para profesorado que utilizan tanto el equipo directivo como los jefes de estudio del centro para acceder a Alexia e Itaca.					
Ubicación: Secretaría, dirección y salas de profesores					
Tipo: PC					
Dependencias					
Activos: COM.2, COM.3			**Grado:** Medio		
¿Por qué? La mayoría de las ocasiones en los que el profesorado utiliza ordenadores es para tener acceso a internet, y por tanto dependen de las redes de acceso a Internet.					
Valor					
Total	**Confidencialidad**	**Integridad**	**Disponibilidad**	**Autenticidad**	**Trazabilidad**
Alto	N/A	N/A	Alto	N/A	N/A

[HW] Hardware					
Código: HW.4			**Nombre:** Chromebook		
Descripción: Ordenadores Chromebook utilizados por alumnos en algunas clases para trabajar con la suite educativa de Google.					
Ubicación: Aulas					
Tipo: PC					
Dependencias					
Activos: COM.2, COM.3			**Grado:** Alto		
¿Por qué? Prácticamente todas las ocasiones en las que los alumnos trabajan con ordenadores es para tener acceso a internet, y por tanto dependen de las redes de acceso a Internet.					
Valor					
Total	**Confidencialidad**	**Integridad**	**Disponibilidad**	**Autenticidad**	**Trazabilidad**
Bajo	N/A	N/A	Bajo	N/A	N/A

[HW] Hardware					
Código: HW.5			**Nombre:** Impresoras		
Descripción: Impresoras utilizadas tanto por el equipo administrativo como por el personal docente.					
Ubicación: Secretaría, dirección y salas de profesores					
Tipo: Periféricos, Medios de impresión, Escáneres					
Dependencias					
Activos:			**Grado:**		
¿Por qué?					
Valor					
Total	**Confidencialidad**	**Integridad**	**Disponibilidad**	**Autenticidad**	**Trazabilidad**
Alto	N/A	N/A	Alto	N/A	N/A

[HW] Hardware					
Código: HW.6			**Nombre:** Repetidores WiFi		
Descripción: Dispositivos utilizados para amplificar la señal WiFi por todo el colegio..					
Ubicación: Situados en las salas de profesores de cada planta					
Tipo: Soporte de red, Modem					
Dependencias					
Activos:			**Grado:**		
¿Por qué?					
Valor					
Total	**Confidencialidad**	**Integridad**	**Disponibilidad**	**Autenticidad**	**Trazabilidad**
Muy Alto	N/A	N/A	Muy Alto	N/A	N/A

[HW] Hardware					
Código: HW.7			**Nombre:** Swtich		
Descripción: Dispositivos Swtich utilizados en las aulas de informática para dar red a todos los ordenadores del aula.					
Ubicación: Aula de informática					
Tipo: Soporte de red, Conmutador					
Dependencias					
Activos:			**Grado:**		
¿Por qué?					
Valor					
Total	**Confidencialidad**	**Integridad**	**Disponibilidad**	**Autenticidad**	**Trazabilidad**
Alto	N/A	N/A	Alto	N/A	N/A

[HW] Hardware					
Código: HW.8			**Nombre:** Modem		
Descripción: Dispositivo que proporciona acceso a Internet.					
Ubicación: Secretaría					
Tipo: Soporte de red, Modem					
Dependencias					
Activos:			**Grado:**		
¿Por qué?					
Valor					
Total	**Confidencialidad**	**Integridad**	**Disponibilidad**	**Autenticidad**	**Trazabilidad**
Alto	N/A	N/A	Alto	N/A	N/A

[HW] Hardware					
Código: HW.9			**Nombre:** Ordenadores personales profesorado		
Descripción: Ordenadores portátiles personales del personal docente que utilicen tanto para la labor docente como para almacenar y gestionar datos docentes y administrativos.					
Ubicación:					
Tipo: PC					
Dependencias					
Activos: COM.2, COM.3			**Grado:** Medio		
¿Por qué? En muchas ocasiones, aunque los datos estén almacenados en el ordenador luego este actúa solo como plataforma intermedia antes de subir estos datos a las plataformas “oficiales” como Itaca o Alexia y para ello necesitan acceso a Internet.					
Valor					
Total	**Confidencialidad**	**Integridad**	**Disponibilidad**	**Autenticidad**	**Trazabilidad**
Alto	N/A	N/A	Alto	N/A	N/A

[COM] Redes de comunicaciones					
Código: COM.1			**Nombre:** Red telefónica		
Descripción: Conexión con la red telefónica con un teléfono fijo en la secretaría y un teléfono móvil en dirección.					
Ubicación: Secretaría y dirección					
Tipo: Red telefónica					
Dependencias					
Activos:			**Grado:**		
¿Por qué?					
Valor					
Total	**Confidencialidad**	**Integridad**	**Disponibilidad**	**Autenticidad**	**Trazabilidad**
Medio	N/A	N/A	Medio	N/A	N/A

[COM] Redes de comunicaciones					
Código: COM.2			**Nombre:** Red WiFi		
Descripción: Red WiFi usada por dirección, administración, profesorado y alumnado.					
Ubicación: Secretaría					
Tipo: WiFi					
Dependencias					
Activos: HW.6			**Grado:** Muy Alto		
¿Por qué? Para que la red WiFi sea accesible desde las diferentes aulas y salas del centro es necesario el uso de repetidores WiFi.					
Activos: HW.8			**Grado:** Muy Alto		
¿Por qué? Para tener acceso a la red WiFi es indispensable el buen funcionamiento del módem para que proporcione acceso a Internet.					
Valor					
Total	**Confidencialidad**	**Integridad**	**Disponibilidad**	**Autenticidad**	**Trazabilidad**
Muy Alto	N/A	N/A	Muy Alto	N/A	N/A

[COM] Redes de comunicaciones					
Código: COM.3			**Nombre:** Red ADSL		
Descripción: Conexión ADSL para proporcionar acceso a Internet en los ordenadores de las aulas de informática.					
Ubicación: Aulas de informática					
Tipo: Red ADSL					
Dependencias					
Activos: HW.8			**Grado:** Muy Alto		
¿Por qué? Para tener acceso a la red ADSL es indispensable el buen funcionamiento del modem que proporciona acceso a Internet.					
Valor					
Total	**Confidencialidad**	**Integridad**	**Disponibilidad**	**Autenticidad**	**Trazabilidad**
Bajo	N/A	N/A	Bajo	N/A	N/A

[Media] Soportes de Información					
Código: Media.1			**Nombre:** Discos duros de administración		
Descripción: Los discos duros de los ordenadores de secretaría y administración que almacenan datos de la gestión administrativa del centro.					
Ubicación: Secretaría y administración					
Tipo: Electrónicos, Discos					
Dependencias					
Activos:			**Grado:**		
¿Por qué?					
Valor					
Total	**Confidencialidad**	**Integridad**	**Disponibilidad**	**Autenticidad**	**Trazabilidad**
Alto	N/A	N/A	Alto	N/A	N/A

[Media] Soportes de Información					
Código: Media.2			**Nombre:** Memorias USB		
Descripción: Dispositivos de almacenamiento externo usados por los profesores con información pedagógica como exámenes, calificaciones o expedientes. Se usa como paso intermedio antes de volcar esta información a Itaca.					
Ubicación:					
Tipo: Electrónicos, USB					
Dependencias					
Activos:			**Activos:**		
¿Por qué?					
Valor					
Total	**Confidencialidad**	**Integridad**	**Disponibilidad**	**Autenticidad**	**Trazabilidad**
Alto	N/A	N/A	Alto	N/A	N/A

[Media] Soportes de Información					
Código: Media.3			**Nombre:** Almacenamiento en la nube		
Descripción: Almacenamiento en la nube como Drive o Dropbox personal de los profesores con información pedagógica como exámenes, calificaciones o expedientes. Se usa como paso intermedio antes de volcar esta información a Itaca.					
Ubicación:					
Tipo: Electrónicos, Almacenamiento en la nube					
Dependencias					
Activos: COM.2			**Grado:** Muy Alto		
¿Por qué? Para tener acceso a los servicios de almacenamiento en la nube desde los ordenadores del centro es indispensable el acceso a la red WiFi.					
Valor					
Total	**Confidencialidad**	**Integridad**	**Disponibilidad**	**Autenticidad**	**Trazabilidad**
Alto	N/A	N/A	Medio	N/A	N/A

[Media] Soportes de Información					
Código: Media.4			**Nombre:** Archivadores y carpetas		
Descripción: Almacenamiento físico para almacenar una copia de la programación general anual, expedientes académicos, partes, información de matrícula y versiones impresas de las notas. Si bien de prácticamente todo existe copia digitalizada por legalidad hay documentos que es necesarios tenerlos también en formato físico.					
Ubicación: Secretaría y administración.					
Tipo: No electrónico, Material impreso					
Dependencias					
Activos:			**Grado:**		
¿Por qué?					
Valor					
Total	**Confidencialidad**	**Integridad**	**Disponibilidad**	**Autenticidad**	**Trazabilidad**
Alto	N/A	N/A	Bajo	N/A	N/A

[P] Personal					
Código: P.1			**Nombre:** Personal Docente		
Descripción: Profesorado encargado de la labor educativa del centro, poner notas, comunicación con los padres e introducir datos de sus alumnos en las plataformas de Alexia e Itaca. Únicamente tienen acceso a los datos de sus alumnos.					
Tipo: Usuarios Internos					
Valor					
Total	**Confidencialidad**	**Integridad**	**Disponibilidad**	**Autenticidad**	**Trazabilidad**
Muy Alto	N/A	N/A	Muy Alto	N/A	N/A

[P] Personal					
Código: P.2			**Nombre:** Personal de TIC		
Descripción: Profesores que además de su labor educativa se encargan de la gestión y el mantenimiento de todos los servicios informáticos y electrónicos del centro.					
Tipo: Usuarios internos					
Valor					
Total	**Confidencialidad**	**Integridad**	**Disponibilidad**	**Autenticidad**	**Trazabilidad**
Muy Alto	N/A	N/A	Muy Alto	N/A	N/A

[P] Personal					
Código: P.3			**Nombre:** Personal de orientación		
Descripción: Personal pedagógico que se encarga de la labor de orientación profesional e integración de alumnos con dificultades del aprendizaje. Tienen acceso a toda la información de los alumnos derivados al departamento de orientación.					
Tipo: Usuarios internos					
Valor					
Total	**Confidencialidad**	**Integridad**	**Disponibilidad**	**Autenticidad**	**Trazabilidad**
Medio	N/A	N/A	Medio	N/A	N/A

3. Listado de las amenazas

Una amenaza se puede definir como “Causa potencial de un incidente que puede causar daños a un sistema de información o una organización”.

Si antes se describía los activos de una empresa como los elementos que generan valor en la misma, las amenazas podrían definirse como sucesos que potencialmente pueden afectar negativamente a estos activos reduciendo su valor y causando daño a la organización.

Las amenazas que puedan afectar a una organización pueden tener un origen externo a esta o bien provenir del interior de la propia organización y es posible distinguir amenazas de muy diverso origen, como desastres naturales, acciones llevadas a cabo de forma accidental por personal interno o externo e incluso ataques intencionados contra una organización o empresa.

Una vez se ha desarrollado el catálogo de activos, el siguiente paso para realizar el plan de seguridad de una organización consiste en realizar el listado de amenazas.

Para ello, a continuación, se elaborará un listado con todas las amenazas que pueden afectar negativamente al Sistema de Información del centro mediante un conjunto de fichas. En estas fichas se indicará el nombre y código de la amenaza, una breve descripción de la misma y los activos a los que afecta, así como la probabilidad de que dicha amenaza se materialice y la degradación que causaría en las diferentes dimensiones de los activos.

3.1 Desastres Naturales

N.1 Fuego					
Descripción: Incendios. Posibilidad de que el fuego acabe con recursos del sistema.					
Probabilidad: Muy Baja Nunca ha ocurrido un incidente de este tipo en la historia del centro.					
Activos afectados					
Nombre	**Degradación**				
	C	**I**	**D**	**A**	**T**
HW.2 - Ordenadores Alumnado	-	-	A	-	-
HW.3 - Ordenadores Profesorado	-	-	A	-	-
HW.4 - Chromebook	-	-	A	-	-
HW.5 - Impresoras	-	-	A	-	-
HW.6 - Repetidores Wifi	-	-	A	-	-
HW.7 - Switch	-	-	A	-	-
HW.8 - Modem	-	-	A	-	-
Media.1 - Disco duro de administración	-	-	A	-	-
Media.4 - Archivadores y carpetas	-	-	A	-	-

N.2 Agua					
Descripción: Inundaciones. Posibilidad de que el agua acabe con los recursos del sistema.					
Probabilidad: Muy Baja Nunca ha ocurrido un incidente de este tipo en la historia del centro.					
Activos afectados					
Nombre	**Degradación**				
	C	**I**	**D**	**A**	**T**
HW.2 - Ordenadores Alumnado	-	-	A	-	-
HW.3 - Ordenadores Profesorado	-	-	A	-	-
HW.4 - Chromebook	-	-	A	-	-
HW.5 - Impresoras	-	-	A	-	-
HW.6 - Repetidores Wifi	-	-	A	-	-
HW.7 - Switch	-	-	A	-	-
HW.8 - Modem	-	-	A	-	-
Media.1 - Disco duro de Administración	-	-	A	-	-
Media.4 - Archivadores y carpetas	-	-	A	-	-

3.2 De origen industrial

I.3 Contaminación mecánica					
Descripción: Averías causadas por la acción del polvo, vibraciones, suciedad etc.					
Probabilidad: Alta Todos los meses se producen pequeñas averías en diferentes dispositivos como teclados, monitores, proyectores etc.					
Activos afectados					
Nombre	**Degradación**				
	C	**I**	**D**	**A**	**T**
HW.2 - Ordenadores Alumnado	-	-	M	-	-
HW.3 - Ordenadores Profesorado	-	-	B	-	-
HW.4 - Chromebook	-	-	M	-	-
HW.5 - Impresoras	-	-	M	-	-
Media.1 - Disco duro de Administración	-	-	M	-	-

I.4 Contaminación electromagnética					
Descripción: Averías temporales o permanentes causadas por interferencias de radio, campos magnéticos, luz ultravioleta etc.					
Probabilidad: Baja No se tiene constancia de este tipo de averías.					
Activos afectados					
Nombre	**Degradación**				
	C	**I**	**D**	**A**	**T**
HW.6 - Repetidores Wifi	-	-	B	-	-

I.6 Corte del suministro eléctrico					
Descripción: Cese temporal de la alimentación de energía eléctrica en el sistema.					
Probabilidad: Media No es algo frecuente, pero al año puede darse algún corte eléctrico momentáneo.					
Activos afectados					
Nombre	**Degradación**				
	C	**I**	**D**	**A**	**T**
HW.2 - Ordenadores Alumnado	-	-	M	-	-
HW.3 - Ordenadores Profesorado	-	-	M	-	-
HW.5 - Impresoras	-	-	M	-	-
Media.1 - Discos duros de administración	-	-	A	-	-

I.8 Fallo de servicios de comunicaciones					
Descripción: Cese temporal de la capacidad de transmitir datos de un sitio a otro. Típicamente se debe a la destrucción física de los medios físicos de transporte o por algún error en los mecanismos de conmutación de tráfico.					
Probabilidad: A diario Prácticamente todos los días se da algún momento en el que por fallos del hardware o saturación del servicio los servicios de comunicaciones fallan o disminuyen notablemente su rendimiento.					
Activos afectados					
Nombre	**Degradación**				
	C	**I**	**D**	**A**	**T**
COM.1 - Red Telefónica	-	-	M	-	-
COM.2 - Red WiFi	-	-	M	-	-
COM.3 - Red ADSL	-	-	M	-	-

I.10 Degradación de soportes de información					
Descripción: Errores o averías en los dispositivos de soporte de información debido al paso del tiempo y al uso continuado.					
Probabilidad: Alta Si bien no es algo muy frecuente es inevitable que cada mes o cada varios meses los soportes de almacenamientos electrónicos den algún fallo.					
Activos afectados					
Nombre	**Degradación**				
	C	**I**	**D**	**A**	**T**
Media.1 - Discos duros de Administración	-	-	A	-	-
Media.2 - Almacenamiento USB	-	-	A	-	-

3.3 Errores y fallos no intencionados

E.1 Errores de los usuarios					
Descripción: Equivocaciones de las personas al usar los servicios del centro, acceder a datos etc.					
Probabilidad: Muy Alta Debido al gran número de tareas relacionadas con introducir datos de forma manual en aplicaciones electrónicas este tipo de errores suceden prácticamente a diario.					
Activos afectados					
Nombre	**Degradación**				
	C	**I**	**D**	**A**	**T**
D.1 - Datos de matricula	B	A	B	-	-
D.2 - Expedientes académicos	B	A	B	-	-
S.1 - Servicios Web	B	B	B	-	-
S.2 - Servicio de correo electrónico	M	B	B	-	-
SW.1 - Alexia	B	A	B	-	-
SW.2 - Itaca	B	A	B	-	-
Media.1 - Discos duros de Administración	B	M	M	-	-
Media.2 - Memorias USB	A	B	M	-	-
Media.3 - Almacenamiento en la nube	B	B	B	-	-
Media.4 - Archivadores y carpetas	A	B	A	-	-

E.2 Errores de administrador					
Descripción: Equivocaciones de personas con responsabilidades de instalación y operación.					
Probabilidad: Medio Pese a ser procesos que están más controlados al año pueden producirse varios de estos errores.					
Activos afectados					
Nombre	**Degradación**				
	C	**I**	**D**	**A**	**T**
D.4 - Copias de seguridad	B	B	A	-	-
S.1 - Servicio Web	-	-	M	-	-
SW.1 - Alexia	B	A	M	-	-
SW.2 - Itaca	B	A	M	-	-
HW.5 - Impresoras	-	-	A	-	-
COM.2 - Red Wifi	-	-	B	-	-

E.7 Deficiencias en la organización					
Descripción: Problemas derivados de no definir para cada situación quién tiene que hacer que y cuando hacerlo.					
Probabilidad: Muy Alta Al no haber procesos definidos, prácticamente todos los días se producen este tipo de situaciones.					
Activos afectados					
Nombre	**Degradación**				
	C	**I**	**D**	**A**	**T**
P.2 - Personal de TIC	-	-	M	-	-
P.1 - Personal Docente	-	-	M	-	-

E.19 Fugas de información					
Descripción: Revelación por indiscreción de información que es, en mayor o menor medida, confidencial.					
Probabilidad: Media No existe constancia de este tipo de situaciones.					
Activos afectados					
Nombre	**Degradación**				
	C	**I**	**D**	**A**	**T**
D.1 - Datos de matrícula	A	-	-	-	-
D.2 - Expediente académico	A	-	-	-	-

E.20 Vulnerabilidades de los programas					
Descripción: Defectos en el código que dan pie a una operación defectuosa sin intención por parte del usuario, pero con consecuencias sobre la integridad de los datos o la capacidad misma de operar.					
Probabilidad: Baja No existe constancia de este tipo de situaciones.					
Activos afectados					
Nombre	**Degradación**				
	C	**I**	**D**	**A**	**T**
SW.2 - Itaca	A	M	B	-	-
SW.1 - Alexia	A	M	B	-	-
SW.4 - Cliente de correo	A	B	M	-	-

E.24 Caída del sistema por falta de equipos					
Descripción: La carencia de recursos suficientes provoca la caída del sistema cuando la carga de trabajo es desmesurada.					
Probabilidad: Baja Debido a la actividad del centro no suelen producirse cargas de trabajo demasiado altas y por tanto no es común este tipo de caídas en el sistema.					
Activos afectados					
Nombre	**Degradación**				
	C	**I**	**D**	**A**	**T**
S.1 - Servicio Web	-	-	M	-	-
HW.5 - Impresoras	-	-	M	-	-
HW.8 - Modem	-	-	B	-	-

E.25 Pérdida de equipos					
Descripción: La pérdida de equipos provoca directamente la carencia de un medio para prestar los servicios.					
Probabilidad: Media Este tipo de hechos son relativamente frecuentes sobre todo con material impreso o de poco valor.					
Activos afectados					
Nombre	**Degradación**				
	C	**I**	**D**	**A**	**T**
HW.4 - Chromebook	B	-	B	-	-
HW.3 - Ordenador Personal Profesorado	M	-	M	-	-
Media.2 - Memorias USB	A	-	M	-	-
Media.4 - Archivadores y carpetas	A	-	A	-	-

3.4 Ataques intencionados

A.5 Suplantación de identidad					
Descripción: Acción en la que un atacante consigue hacerse pasar por un usuario autorizado para conseguir mayores privilegios y acceso a más información y servicios.					
Probabilidad: Muy Baja No se tiene constancia de este tipo de situaciones. Además, debido a la actividad del centro este no es un foco de interés para este tipo de ataques					
Activos afectados					
Nombre	**Degradación**				
	C	**I**	**D**	**A**	**T**
D.1 - Datos de matrícula	M	M	-	-	-
D.2 - Expedientes académicos	M	M	-	-	-
D.4 - Copias de seguridad	A	B	-	-	-
S.2 - Servicio de correo electrónico	A	M	-	-	-
SW.1 - Alexia	A	A	-	-	-
SW.2 - Itaca	A	A	-	-	-
COM.2 - Red Wifi	B	B	-	-	-

A.6 Abuso de privilegios de acceso					
Descripción: Cada usuario disfruta de un nivel de privilegios para desarrollar su labor en el centro. Este ataque se da cuando un usuario abusa de su nivel de privilegios para realizar tareas que no son de su competencia.					
Probabilidad: Baja No se tiene constancia de este tipo de situaciones. Además, debido a la actividad del centro este no es un foco de interés para este tipo de ataques.					
Activos afectados					
Nombre	**Degradación**				
	C	**I**	**D**	**A**	**T**
D.2 - Expedientes académicos	M	M	B	-	-
SW.1 - Alexia	A	B	B	-	-
SW.2 - Itaca	A	B	B	-	-

A.7 Uso no previsto					
Descripción: Utilización de recursos del sistema para fines no previstos, típicamente de interés personal, juegos, consultas personales en internet, programas personales etc.					
Probabilidad: Muy Alta El hecho de que haya dispositivos personales de profesores y que los alumnos tengan acceso a equipos informáticos hace difícil controlar el uso que se le da a estos y por tanto este tipo de situaciones son muy comunes.					
Activos afectados					
Nombre	**Degradación**				
	C	**I**	**D**	**A**	**T**
S.2 - Servicio de correo electrónico	B	B	B	-	-
HW.2 - Ordenadores para alumnado	B	B	B	-	-
HW.3 - Ordenadores para profesorado	B	B	B	-	-
COM.1 - Red telefónica	B	B	B	-	-
COM.2 - Red WiFi	B	B	B	-	-
Media.3 - Memoria USB	M	M	M	-	-

A.11 Acceso no autorizado					
Descripción: El atacante consigue acceder a los recursos del sistema sin tener autorización para ello. Normalmente esto se hace aprovechando un fallo del sistema de identificación y autorización.					
Probabilidad: Muy Baja No se tiene constancia de este tipo de situaciones. Además, debido a la actividad del centro este no es un foco de interés para este tipo de ataques.					
Activos afectados					
Nombre	**Degradación**				
	C	**I**	**D**	**A**	**T**
D.1 - Datos de matrícula	M	B	-	-	-
D.2 - Expedientes académicos	M	M	-	-	-
D.4 - Copias de seguridad	A	B	-	-	-
S.2 - Servicio de correo electrónico	A	M	-	-	-
SW.1 - Alexia	A	A	-	-	-
SW.2 - Itaca	A	A	-	-	-
COM.2 - Red Wifi	B	B	-	-	-

A.14 Interceptación de información					
Descripción: El atacante llega a tener acceso a información que no le corresponde, sin que la información se vea alterada.					
Probabilidad: Muy Baja No se tiene constancia de este tipo de situaciones. Además, debido a la actividad del centro este no es un foco de interés para este tipo de ataques.					
Activos afectados					
Nombre	**Degradación**				
	C	**I**	**D**	**A**	**T**
COM.2 - Red Wifi	B	-	-	-	-

A.15 Modificación/Destrucción de información					
Descripción: Alteración intencional de información con ánimo de obtener un beneficio o causar un perjuicio.					
Probabilidad: Baja No se tiene constancia de este tipo de situaciones. Además, debido a la actividad del centro este no es un foco de interés para este tipo de ataques.					
Activos afectados					
Nombre	**Degradación**				
	C	**I**	**D**	**A**	**T**
D.1 - Datos de matrícula	-	M	B	-	-
D.2 - Expedientes académicos	-	M	B	-	-
D.4 - Copias de seguridad	-	B	B	-	-
S.1 - Servicio Web	-		A	-	-
HW.2 - Ordenadores de alumnado	-	B	B	-	-
HW.3 - Ordenadores de profesorado	-	M	A	-	-
Media.1 - Discos duros de administración	-	A	A	-	-
Media.2 - Memorias USB	-	M	M	-	-
Media.4 - Archivadores y carpetas	-	A	M	-	-

A.23 Manipulación de equipos					
Descripción: Alteración intencionada del funcionamiento de los programas, persiguiendo un beneficio indirecto cuando una persona autorizada lo utiliza.					
Probabilidad: Muy Baja No se tiene constancia de este tipo de situaciones. Además, debido a la actividad del centro este no es un foco de interés para este tipo de ataques.					
Activos afectados					
Nombre	**Degradación**				
	C	**I**	**D**	**A**	**T**
HW.2 - Ordenadores alumnado	B	-	B	-	-
HW.3 - Ordenadores profesorado	M	-	B	-	-

A.24 Denegación de Servicio					
Descripción: Ataque por el cual se somete al sistema a una carga de trabajo excesiva de forma forzada para conseguir que este caiga.					
Probabilidad: Muy Baja No se tiene constancia de este tipo de situaciones. Además, debido a la actividad del centro este no es un foco de interés para este tipo de ataques.					
Activos afectados					
Nombre	**Degradación**				
	C	**I**	**D**	**A**	**T**
SW.2 - Itaca	-	-	M	-	-
SW.1 - Alexia	-	-	M	-	-
S.1 - Servidor Web	-	-	A	-	-

A.25 Robo					
Descripción: Sustracción de equipamiento que puede ser de todo tipo como material hardware, datos impresos o soportes de información					
Probabilidad: Baja Se ha dado algún caso de robo de equipamiento del centro como ordenadores o proyectores, pero es una situación muy poco común					
Activos afectados					
Nombre	**Degradación**				
	C	**I**	**D**	**A**	**T**
HW.3 - Ordenadores profesorado	B	-	A	-	-
HW.4 - Chromebook	B	-	A	-	-
Media.2 - Memorias USB	A	-	M	-	-

A.26 Ataque destructivo					
Descripción: Acciones que pueden ser realizadas por personal interno o ajeno a la organización como vandalismo.					
Probabilidad: Baja Se ha dado algún caso de robo de equipamiento del centro como ordenadores o proyectores, pero es una situación muy poco común					
Activos afectados					
Nombre	**Degradación**				
	C	**I**	**D**	**A**	**T**
HW.3 - Ordenadores profesorado	-	-	A	-	-
HW.2 - Ordenadores alumnado	-	-	B	-	-
HW.4 - Chromebook	-	-	B	-	-
HW.6 - Repetidores Wifi	-	-	A	-	-
HW.7 - Swtich	-	-	A	-	-

4. Estimación de riesgos

Habiendo identificado y valorado los activos del centro, así como las amenazas a los que estos pueden estar expuestos, en este apartado se realizará el cálculo del impacto y la estimación de riesgos.

El impacto puede definirse como el daño que causaría al centro la materialización de una amenaza sobre un determinado activo. Para el cálculo de este impacto no se tienen en cuenta salvaguardas o medidas tomadas para evitar o reducir el daño causado por una amenaza. El impacto puede entenderse como una relación entre valor y degradación.

Por su parte, el riesgo se entiende como el daño probable que puede sufrir el centro a raíz de una amenaza. En este caso se calculará el riesgo como una relación entre el impacto de una amenaza sobre un activo y la probabilidad de que esta se materialice.

Esta estimación de riesgos permitirá identificar cuáles son los elementos a proteger con mayor prioridad en el centro y así evitar costes innecesarios o medidas no efectivas de cara a garantizar la seguridad de la información.

Para realizar esta estimación de riesgos se adjunta un listado con una serie de fichas, en las cuales se determina, para cada activo, que amenazas puede sufrir, el impacto y riesgo potencial de las mismas (es decir, cuanto daño hacen estas amenazas teniendo en cuenta solo ese activo) y el impacto y riesgo acumulado, en el cual se tiene en cuenta el valor de un activo en función de todos los elementos que dependen del mismo.

D.1 – Datos de Matrícula												
Amenazas	**Impacto Potencial**			**Impacto Acumulado**			**Riesgo Potencial**			**Riesgo Acumulado**		
	C	**I**	**D**	**C**	**I**	**D**	**C**	**I**	**D**	**C**	**I**	**D**
E.1 - Errores de los usuarios	M	MA	MB	-	-	-	A	MA	B	-	-	-
E.19 - Fugas de información	MA	-	-	-	-	-	MA	-	-	-	-	-
A.5 – Suplantación de identidad	A	A	-	-	-	-	M	M	-	-	-	-
A.11 – Acceso no autorizado	A	M	-	-	-	-	M	B	-	-	-	-
A.15 – Modificación/Destrucción de info.	-	A	MB	-	-	-	-	A	MB	-	-	-

D.2 – Expedientes académicos												
Amenazas	**Impacto Potencial**			**Impacto Acumulado**			**Riesgo Potencial**			**Riesgo Acumulado**		
	C	**I**	**D**	**C**	**I**	**D**	**C**	**I**	**D**	**C**	**I**	**D**
E.1 - Errores de usuarios	A	MA	MB	-	-	-	MA	MA	B	-	-	-
E.19 – Fugas de información	MA	-	-	-	-	-	MA	-	-	-	-	-
A.5 – Suplantación de identidad	A	A	-	-	-	-	M	M	-	-	-	-
A.11 – Acceso no autorizado	A	A	-	-	-	-	M	M	-	-	-	-
A.15 – Modificación/Destrucción de info.	-	A	M	-	-	-	-	A	M	-	-	-

D.4 – Copias de seguridad												
Amenazas	**Impacto Potencial**			**Impacto Acumulado**			**Riesgo Potencial**			**Riesgo Acumulado**		
	C	**I**	**D**	**C**	**I**	**D**	**C**	**I**	**D**	**C**	**I**	**D**
E.2 – Errores de administrador	M	M	MA	-	-	-	M	M	MA	-	-	-
A.11 – Acceso no autorizado	MA	M	-	-	-	-	A	B	-	-	-	-
A.15 – Modificación/Destrucción de info.	-	M	MB	-	-	-	-	M	MB	-	-	-

COM.1 – Red telefónica												
Amenazas	**Impacto Potencial**			**Impacto Acumulado**			**Riesgo Potencial**			**Riesgo Acumulado**		
	C	**I**	**D**	**C**	**I**	**D**	**C**	**I**	**D**	**C**	**I**	**D**
I.8 – Fallo de servicios de comunicaciones	-	-	B	-	-	-	-	-	M	-	-	-
A.7 – Uso no previsto	-	-	MB	-	-	-	-	-	B	-	-	-

COM.2 – Red WiFi												
Amenazas	**Impacto Potencial**			**Impacto Acumulado**			**Riesgo Potencial**			**Riesgo Acumulado**		
	C	**I**	**D**	**C**	**I**	**D**	**C**	**I**	**D**	**C**	**I**	**D**
I.8 – Fallo de servicios de comunicaciones	-	-	A	-	-	A	-	-	MA	-	-	MA
A.5 – Suplantación de identidad	M	-	-	-	-	-	M	-	-	-	-	-
A.7 – Uso no previsto	-	-	M	-	-	M	-	-	A	-	-	A
E.2 – Errores de administrador	-	-	M	-	-	M	-	-	M	-	-	M

COM.3 – Red ADSL												
Amenazas	**Impacto Potencial**			**Impacto Acumulado**			**Riesgo Potencial**			**Riesgo Acumulado**		
	C	**I**	**D**	**C**	**I**	**D**	**C**	**I**	**D**	**C**	**I**	**D**
I.8 – Fallo de servicios de comunicaciones	-	-	MB	-	-	A	-	-	B	-	-	MA

HW.1 – Servidor Web												
Amenazas	**Impacto Potencial**			**Impacto Acumulado**			**Riesgo Potencial**			**Riesgo Acumulado**		
	C	**I**	**D**	**C**	**I**	**D**	**C**	**I**	**D**	**C**	**I**	**D**
A.24 – Denegación de servicio	-	-	B	-	-	M	-	-	MB	-	-	B

HW.2 – Ordenadores para alumnado												
Amenazas	**Impacto Potencial**			**Impacto Acumulado**			**Riesgo Potencial**			**Riesgo Acumulado**		
	C	**I**	**D**	**C**	**I**	**D**	**C**	**I**	**D**	**C**	**I**	**D**
N.1 – Fuego	-	-	B	-	-	-	-	-	MB	-	-	-
N.2 - Agua	-	-	B	-	-	-	-	-	MB	-	-	-
I.3 – Contaminación mecánica	-	-	MB	-	-	-	-	-	B	-	-	-
I.6 – Corte suministro eléctrico	-	-	M	-	-	-	-	-	M	-	-	-
A.7 – Uso no previsto	-	-	MB	-	-	-	-	-	MB	-	-	-
A.15 – Modificación/Destrucción de info.	-	-	MB	-	-	-	-	-	MB	-	-	-
A.23 – Manipulación de equipos	-	-	MB	-	-	-	-	-	MB	-	-	-
A.26 – Ataque destructivo	-	-	MB	-	-	-	-	-	MB	-	-	-

HW.3 – Ordenadores para profesorado												
Amenazas	**Impacto Potencial**			**Impacto Acumulado**			**Riesgo Potencial**			**Riesgo Acumulado**		
	C	**I**	**D**	**C**	**I**	**D**	**C**	**I**	**D**	**C**	**I**	**D**
N.1 – Fuego	-	-	A	-	-	-	-	-	M	-	-	-
N.2 - Agua	-	-	A	-	-	-	-	-	M	-	-	-
I.3 – Contaminación mecánica	-	-	B	-	-	-	-	-	M	-	-	-
I.6 – Corte suministro eléctrico	-	-	M	-	-	-	-	-	M	-	-	-
A.7 – Uso no previsto	-	-	B	-	-	-	-	-	B	-	-	-
A.15 – Modificación/Destrucción de info.	-	-	A	-	-	-	-	-	M	-	-	-
A.23 – Manipulación de equipos	-	-	B	-	-	-	-	-	MB	-	-	-
A.26 – Ataque destructivo	-	-	A	-	-	-	-	-	M	-	-	-

HW.4 - Chromebook												
Amenazas	**Impacto Potencial**			**Impacto Acumulado**			**Riesgo Potencial**			**Riesgo Acumulado**		
	C	**I**	**D**	**C**	**I**	**D**	**C**	**I**	**D**	**C**	**I**	**D**
N.1 – Fuego	-	-	B	-	-	-	-	-	MB	-	-	-
N.2 - Agua	-	-	B	-	-	-	-	-	MB	-	-	-
I.3 – Contaminación mecánica	-	-	MB	-	-	-	-	-	B	-	-	-
E.25 – Pérdida de equipos	-	-	MB	-	-	-	-	-	MB	-	-	-
A.25 – Robo	-	-	B	-	-	-	-	-	MB	-	-	-
A.26 – Ataque destructivo	-	-	MB	-	-	-	-	-	MB	-	-	-

HW.5 - Impresoras												
Amenazas	**Impacto Potencial**			**Impacto Acumulado**			**Riesgo Potencial**			**Riesgo Acumulado**		
	C	**I**	**D**	**C**	**I**	**D**	**C**	**I**	**D**	**C**	**I**	**D**
N.1 - Fuego	-	-	A	-	-	-	-	-	M	-	-	-
N.2 - Agua	-	-	A	-	-	-	-	-	M	-	-	-
I.3 – Contaminación mecánica	-	-	M	-	-	-	-	-	A	-	-	-

HW.6 – Repetidores WiFi												
Amenazas	**Impacto Potencial**			**Impacto Acumulado**			**Riesgo Potencial**			**Riesgo Acumulado**		
	C	**I**	**D**	**C**	**I**	**D**	**C**	**I**	**D**	**C**	**I**	**D**
I.4 Contaminación electromagnética	-	-	M	-	-	M	-	-	M	-	-	M
A.26 – Ataque destructivo	-	-	MA	-	-	MA	-	-	A	-	-	A
N.1 – Fuego	-	-	MA	-	-	MA	-	-	A	-	-	A
N.2 - Agua	-	-	MA	-	-	MA	-	-	A	-	-	A

HW.7 - Switch												
Amenazas	**Impacto Potencial**			**Impacto Acumulado**			**Riesgo Potencial**			**Riesgo Acumulado**		
	C	**I**	**D**	**C**	**I**	**D**	**C**	**I**	**D**	**C**	**I**	**D**
N.1 – Fuego	-	-	A	-	-	A	-	-	M	-	-	M
N.2 – Agua	-	-	A	-	-	A	-	-	M	-	-	M
A.26 – Ataque destructivo	-	-	A	-	-	A	-	-	M	-	-	M

HW.8 - Modem												
Amenazas	**Impacto Potencial**			**Impacto Acumulado**			**Riesgo Potencial**			**Riesgo Acumulado**		
	C	**I**	**D**	**C**	**I**	**D**	**C**	**I**	**D**	**C**	**I**	**D**
N.1 – Fuego	-	-	A	-	-	MA	-	-	M	-	-	A
N.2 – Agua	-	-	A	-	-	MA	-	-	M	-	-	A
E.24 – Caída del sistema falta de equipos	-	-	B	-	-	M	-	-	MB	-	-	B

HW.9 – Ordenadores personales del profesorado												
Amenazas	**Impacto Potencial**			**Impacto Acumulado**			**Riesgo Potencial**			**Riesgo Acumulado**		
	C	**I**	**D**	**C**	**I**	**D**	**C**	**I**	**D**	**C**	**I**	**D**
E.25 – Pérdida de equipos	-	-	M	-	-	-	-	-	M	-	-	-
A.25 - Robo	-	-	M	-	-	-	-	-	B	-	-	-

Media.1 – Discos duros de administración												
Amenazas	**Impacto Potencial**			**Impacto Acumulado**			**Riesgo Potencial**			**Riesgo Acumulado**		
	C	**I**	**D**	**C**	**I**	**D**	**C**	**I**	**D**	**C**	**I**	**D**
N.1 – Fuego	-	-	A	-	-	A	-	-	M	-	-	M
N.2 – Agua	-	-	A	-	-	A	-	-	M	-	-	M
I.3 – Contaminación mecánica	-	-	M	-	-	M	-	-	A	-	-	A
I.6 Corte suministro eléctrico	-	-	A	-	-	A	-	-	A	-	-	A
I.10 Degradación soportes de información	-	-	A	-	-	A	-	-	MA	-	-	MA
E.1 – Errores de los usuarios	-	-	M	M	M	M	-	-	A	A	A	A
A.15 – Modificación/Destrucción de info.	-	-	A	A	A	A	-	-	M	M	M	M

Media.2 – Memorias USB												
Amenazas	**Impacto Potencial**			**Impacto Acumulado**			**Riesgo Potencial**			**Riesgo Acumulado**		
	C	**I**	**D**	**C**	**I**	**D**	**C**	**I**	**D**	**C**	**I**	**D**
A.7 – Uso no previsto	-	-	M	MB	MB	M	-	-	M	MB	MB	M
E.1 – Errores de los usuarios	-	-	M	MB	MB	M	-	-	M	B	B	A
E.25 – Pérdida de equipos	-	-	M	M	-	M	-	-	M	M	-	M
A.15 – Modificación/Destrucción de info.	-	-	M	-	MB	M	-	-	B	-	MB	B
A.25 - Robo	-	-	M	M	-	M	-	-	B	B	-	B
I.10 – Degradación en soportes de info.	-	-	M	-	-	M	-	-	M	-	-	M

Media.3 – Archivadores y carpetas												
Amenazas	**Impacto Potencial**			**Impacto Acumulado**			**Riesgo Potencial**			**Riesgo Acumulado**		
	C	**I**	**D**	**C**	**I**	**D**	**C**	**I**	**D**	**C**	**I**	**D**
N.1 – Fuego	-	-	B	-	-	B	-	-	MB	-	-	MB
N.2 – Agua	-	-	B	-	-	B	-	-	MB	-	-	MB
E.1 – Errores de los usuarios	-	-	B	MB	MB	B	-	-	M	B	B	M
E.25 – Pérdida de equipos	-	-	B	MB	-	B	-	-	M	B	-	M
A.15 – Modificación/Destrucción de info.	-	-	MB	-	MB	MB	-	-	MB	-	MB	MB

Media.4 – Almacenamiento en la nube												
Amenazas	**Impacto Potencial**			**Impacto Acumulado**			**Riesgo Potencial**			**Riesgo Acumulado**		
	C	**I**	**D**	**C**	**I**	**D**	**C**	**I**	**D**	**C**	**I**	**D**
E.1 – Errores de los usuarios	-	-	MB	MB	MB	MB	-	-	B	B	B	B

P.1 – Personal Docente												
Amenazas	**Impacto Potencial**			**Impacto Acumulado**			**Riesgo Potencial**			**Riesgo Acumulado**		
	C	**I**	**D**	**C**	**I**	**D**	**C**	**I**	**D**	**C**	**I**	**D**
E.7 – Deficiencias en la organización	-	-	A	-	-	-	-	-	A	-	-	-

P.2 – Personal de TIC												
Amenazas	**Impacto Potencial**			**Impacto Acumulado**			**Riesgo Potencial**			**Riesgo Acumulado**		
	C	**I**	**D**	**C**	**I**	**D**	**C**	**I**	**D**	**C**	**I**	**D**
E.7 – Deficiencias en la organización	-	-	MA	-	-	-	-	-	MA	-	-	-

S.1 – Servicio web												
Amenazas	**Impacto Potencial**			**Impacto Acumulado**			**Riesgo Potencial**			**Riesgo Acumulado**		
	C	**I**	**D**	**C**	**I**	**D**	**C**	**I**	**D**	**C**	**I**	**D**
E.1 – Errores de los usuarios	-	-	MB	-	-	-	-	-	B	-	-	-
E.2 – Errores de administrador	-	-	B	-	-	-	-	-	B	-	-	-
E.24 – Caída del sistema por falta equipos	-	-	M	-	-	-	-	-	B	-	-	-
A.15 – Modificación/Destrucción de info.	-	-	MB	-	-	-	-	-	MB	-	-	-

S.2 – Servicio de correo electrónico												
Amenazas	**Impacto Potencial**			**Impacto Acumulado**			**Riesgo Potencial**			**Riesgo Acumulado**		
	C	**I**	**D**	**C**	**I**	**D**	**C**	**I**	**D**	**C**	**I**	**D**
E.1 – Errores de los usuarios	-	-	M	-	-	-	-	-	B	-	-	-
E.20 – Vulnerabilidad de los programas	-	-	M	-	-	-	-	-	B	-	-	-
A.7 – Uso no previsto	-	-	M	-	-	-	-	-	B	-	-	-

SW.1 - Alexia												
Amenazas	**Impacto Potencial**			**Impacto Acumulado**			**Riesgo Potencial**			**Riesgo Acumulado**		
	C	**I**	**D**	**C**	**I**	**D**	**C**	**I**	**D**	**C**	**I**	**D**
E.1 – Errores de los usuarios	-	-	B	MB	B	B	-	-	M	B	M	M
E.2 – Errores de administrador	-	-	M	MB	B	M	-	-	M	MB	B	M
E.20 – Vulnerabilidad de los programas	-	-	B	M	M	B	-	-	B	M	M	B
A.5 – Suplantación de la identidad	-	-	-	M	M	-	-	-	-	B	B	-
A.6 – Abuso de privilegios de acceso	-	-	B	M	MB	B	-	-	B	M	MB	B
A.11 – Acceso no autorizado	-	-	-	M	M	-	-	-	-	B	B	-
A.24 – Denegación de servicio	-	-	M	-	-	M	-	-	B	-	-	B

SW.2 - Itaca												
Amenazas	**Impacto Potencial**			**Impacto Acumulado**			**Riesgo Potencial**			**Riesgo Acumulado**		
	C	**I**	**D**	**C**	**I**	**D**	**C**	**I**	**D**	**C**	**I**	**D**
E.1 – Errores de los usuarios	-	-	B	M	MA	B	-	-	M	A	MA	M
E.2 – Errores de administrador	-	-	M	M	MA	M	-	-	M	M	MA	M
E.20 – Vulnerabilidad de los programas	-	-	B	MA	A	M	-	-	B	MA	A	M
A.5 – Suplantación de la identidad	-	-	-	MA	MA	-	-	-	-	A	A	-
A.6 – Abuso de privilegios de acceso	-	-	B	A	M	B	-	-	B	A	M	B
A.11 – Acceso no autorizado	-	-	-	MA	MA	-	-	-	-	A	A	-
A.24 – Denegación de servicio	-	-	M	-	-	A	-	-	M	-	-	A

5. Evaluación de salvaguardas

En la sección anterior del documento se ha realizado la estimación de riesgos para el centro sin tener en cuenta ningún tipo de salvaguardas. Esto permite identificar los activos que están más expuestos a diferentes tipos de amenazas y sobre cuáles se debe hacer más hincapié en cuanto a su protección.

En este apartado se va a realizar un catálogo de las posibles salvaguardas que puede aplicar el centro para asegurar el valor de sus activos contra las amenazas identificadas en el apartado 3. Listado de las amenazas.

Para ello se han realizado una serie de fichas donde se han identificado todas las posibles salvaguardas que poner en marcha, identificando además cuál sería el efecto provocado por la salvaguarda y las amenazas a las que afectaría disminuyendo su riesgo. Para ello se ha coloreado en morado los valores modificados por el efecto de la salvaguarda, en relación con los calculados en el apartado anterior.

Para cada tipo de salvaguarda existen un gran número de posibles medidas que aplicar en el centro, sin embargo, es importante realizar una selección de aquellas que pueden ser útiles para el centro teniendo en cuenta cuáles son los activos y las dimensiones que buscamos proteger, en tanto que una salvaguarda puede afectar de manera diferente a varias dimensiones, y cuáles son las amenazas frente a las que se está expuesto.

Además, es conveniente realizar una tarea de priorización teniendo en cuenta que conseguir un sistema “seguro” puede resultar más costoso que el valor de los activos de la organización. Así pues, la evaluación de salvaguardas se centrará en proteger los activos más valiosos y reducir los riesgos más elevados evitando aquellas salvaguardas que, o bien no sean aplicables al sistema del centro, o bien no justifiquen su coste respecto al riesgo que tratan de reducir.

En este apartado se identificarán todas las posibles salvaguardas a implantar en el centro mientras que esta priorización se llevará a cabo en las siguientes secciones del documento.

D.1 – Datos de Matrícula												
Amenazas	**Salvaguardas**	**Probabilidad**	**Dimensiones**			**Impacto Res.**			**Riesgo Res.**		
			C	**I**	**D**	**C**	**I**	**D**	**C**	**I**	**D**
E.1 - Errores de los usuarios	CR.1 – Cuentas de administración	Muy Alta	B	**B**	B	M	**M**	MB	A	**A**	MB
	AD.1 – Formalización de procedimientos	**Media**	B	A	B	M	MA	MB	**M**	**A**	**MB**
	RC.1 – Copias de seguridad periódicas	Muy Alta	B	**B**	**MB**	M	**M**	**MB**	A	**A**	**MB**
E.19 – Fugas de información	AW.1 – Elaborar normas del uso de TI	**Baja**	A	-	-	MA	-	-	**M**	-	-
	AW.2 – Formación sobre aplicación RGPD	**Baja**	A	-	-	MA	-	-	**M**	-	-
	IM.1 – Cifrado de equipos hardware	Media	**B**	-	-	**M**	-	-	**M**	-	-
	PR.7 – Formateo periódico de equipos	Media	**B**	-	-	**M**	-	-	**M**	-	-
A.5 – Suplantación de identidad	PR.1 – Uso de claves y certificados para conexiones inalámbricas	**Muy Baja**	A	B	-	MA	M	-	**M**	**MB**	-
	PR.3 – Control de acceso lógico	**Muy Baja**	A	B	-	MA	M	-	**M**	**MB**	-
	PR.4 – Implantación contraseñas seguras	**Muy Baja**	A	B	-	MA	M	-	**M**	**MB**	-
A.11 – Acceso no autorizado	IM.1 – Cifrado de equipos hardware	Muy Baja	**B**	B	-	**M**	M	-	**MB**	MB	-
	PR.1 – Uso de claves y certificados para conexiones inalámbricas	**Muy Baja**	M	B	-	A	M	-	**B**	**MB**	-
	PR.3 – Control de acceso lógico	**Muy Baja**	M	B	-	A	M	-	**B**	**MB**	-
	PR.4 – Implantación contraseñas seguras	**Muy Baja**	M	B	-	A	M	-	**B**	**MB**	-
A.15 – Modificación/Destrucción de info.	IM.1 – Cifrado de equipos hardware	Baja	-	M	**B**	-	A	**MB**	-	M	**MB**
	PR.3 – Control de acceso lógico	**Muy Baja**	-	M	B	-	A	MB	-	**B**	**MB**
	PR.4 – Implantación contraseñas seguras	**Muy Baja**	-	M	B	-	A	MB	-	**B**	**MB**
	RC.1 – Copias de seguridad periódicas	Baja	-	**M**	**B**	-	**A**	**MB**	-	**M**	**MB**
	RC.3 – Plantes de contingencia y continuidad	Baja	-	**M**	**B**	-	**A**	**MB**	-	**M**	**MB**

D.2 – Expedientes académicos												
Amenazas	**Salvaguardas**	**Probabilidad**	**Dimensiones**			**Impacto Res.**			**Riesgo Res.**		
			C	**I**	**D**	**C**	**I**	**D**	**C**	**I**	**D**
E.1 - Errores de los usuarios	CR.1 – Cuentas de administración	Muy Alta	B	**B**	B	M	**M**	MB	A	**A**	B
	AD.1 – Formalización de procedimientos	**Media**	B	A	B	M	MA	MB	**M**	**MA**	**MB**
	RC.1 – Copias de seguridad periódicas	Muy Alta	B	**B**	**B**	M	**M**	**MB**	A	**A**	**B**
E.19 – Fugas de información	AW.1 – Elaborar normas del uso de TI	**Baja**	A	-	-	MA	-	-	**MA**	-	-
	AW.2 – Formación sobre aplicación RGPD	**Baja**	A	-	-	MA	-	-	**MA**	-	-
	IM.1 – Cifrado de equipos hardware	Media	B	-	-	**M**	-	-	**M**	-	-
	PR.7 – Formateo periódico de equipos	Media	B	-	-	**M**	-	-	**M**	-	-
A.5 – Suplantación de identidad	PR.1 – Uso de claves y certificados para conexiones inalámbricas	**Muy Baja**	A	B	-	MA	M	-	**A**	**B**	-
	PR.3 – Control de acceso lógico	**Muy Baja**	A	B	-	MA	M	-	**A**	**B**	-
	PR.4 – Implantación contraseñas seguras	**Muy Baja**	A	B	-	MA	M	-	**A**	**B**	-
	IM.1 – Cifrado de equipos hardware	Muy Baja	B	B	-	**M**	M	-	**B**	B	-
A.11 – Acceso no autorizado	PR.1 – Uso de claves y certificados para conexiones inalámbricas	**Muy Baja**	M	B	-	A	M	-	**M**	**B**	-
	PR.3 – Control de acceso lógico	**Muy Baja**	M	B	-	A	M	-	**M**	**B**	-
	PR.4 – Implantación contraseñas seguras	**Muy Baja**	M	B	-	A	M	-	**M**	**B**	-
	IM.1 – Cifrado de equipos hardware	Baja	-	M	**B**	-	A	**MB**	-	A	**MB**
A.15 – Modificación/Destrucción de info.	PR.3 – Control de acceso lógico	**Muy Baja**	-	M	B	-	A	MB	-	**A**	**MB**
	PR.4 – Implantación contraseñas seguras	**Muy Baja**	-	M	B	-	A	MB	-	**A**	**MB**
	RC.1 – Copias de seguridad periódicas	Baja	-	**M**	**B**	-	**A**	**MB**	-	**A**	**MB**
	RC.3 – Plantes de contingencia y continuidad	Baja	-	**M**	**B**	-	**A**	**MB**	-	**A**	**MB**
	CR.1 – Cuentas de administración	Muy Alta	B	B	B	M	M	MB	A	A	MB

D.4 – Copias de seguridad												
Amenazas	**Salvaguardas**	**Probabilidad**	**Dimensiones**			**Impacto Res.**			**Riesgo Res.**		
			C	**I**	**D**	**C**	**I**	**D**	**C**	**I**	**D**
E.2 – Errores de administrador	AD.1 – Formalización de procedimientos	**Baja**	B	B	A	M	M	M	**M**	**M**	**M**
	AW.1 – Elaborar normas del uso de TI	**Baja**	B	B	A	M	M	M	**M**	**M**	**M**
	RC.2 – Guardar registros de configuración	Media	B	B	A	M	M	M	M	M	M
	RC.3 – Plantes de contingencia y continuidad	Media	B	B	A	M	M	M	M	M	M
A.11 – Acceso no autorizado	IM.1 – Cifrado de equipos hardware	Muy Baja	B	B	-	**M**	M	-	**B**	B	-
	PR.3 – Control de acceso lógico	**Muy Baja**	M	B	-	**A**	M	-	**M**	**B**	-
A.15 – Modificación/Destrucción de info.	PR.3 – Control de acceso lógico	**Muy Baja**	-	B	B	-	M	MB	-	**B**	**MB**
	RC.3 – Plantes de contingencia y continuidad	Baja	-	B	B	-	**M**	**MB**	-	**M**	**M**

-

COM.1 – Red telefónica											
Amenazas	**Salvaguardas**	**Probabilidad**	**Dimensiones**			**Impacto Res.**			**Riesgo Res.**		
			C	**I**	**D**	**C**	**I**	**D**	**C**	**I**	**D**
I.8 – Fallo de servicios de comunicaciones	RC.3 – Plantes de contingencia y continuidad	Muy Alta	-	-	**B**	-	-	-	-	-	-
A.7 – Uso no previsto	AW.1 – Elaborar normas del uso de TI	**Media**	B	B	B	MB	-	-	**MB**	-	-

COM.2 – Red WiFi												
Amenazas	**Salvaguardas**	**Probabilidad**	**Dimensiones**			**Impacto Res.**			**Riesgo Res.**		
			C	**I**	**D**	**C**	**I**	**D**	**C**	**I**	**D**
I.8 – Fallo de servicios de comunicaciones	RC.3 – Plantes de contingencia y continuidad	Muy Alta	-	-	**B**	-	-	**M**	-	-	**A**
A.5 – Suplantación de identidad	PR.1 – Uso de claves y certificados para conexiones inalámbricas	**Muy Baja**	B	B	-	M	-	-	**B**	-	-
	PR.3 – Control de acceso lógico	**Muy Baja**	B	B	-	M	-	-	**B**	-	-
A.7 – Uso no previsto	AW.1 – Elaborar normas del uso de TI	**Media**	B	B	-	M	-	-	**M**	-	-
	EL.1 – Mecanismos capar servicios web	**Baja**	B	B	-	M	-	-	**M**	-	-
E.2 – Errores de administrador	AD.1 – Formalización de procedimientos	**Baja**	B	-	-	M	-	-	**M**	-	-
	RC.2 – Guardar registros de configuración	Medio	**B**	-	**B**	**M**	-	**M**	**M**	-	**M**

COM.3 – Red ADSL											
Amenazas	**Salvaguardas**	**Probabilidad**	**Dimensiones**			**Impacto Res.**			**Riesgo Res.**		
			C	**I**	**D**	**C**	**I**	**D**	**C**	**I**	**D**
I.8 – Fallo de servicios de comunicaciones	RC.3 – Plantes de contingencia y continuidad	Muy Alta	-	-	**B**	-	-	**MB**	-	-	**B**

HW.2 – Ordenadores para alumnado												
Amenazas	**Salvaguardas**	**Probabilidad**	**Dimensiones**			**Impacto Res.**			**Riesgo Res.**		
			C	**I**	**D**	**C**	**I**	**D**	**C**	**I**	**D**
N.1 – Fuego	IM.4 – Uso y mantenimiento extintores	**Muy Baja**	-	-	A	-	-	B	-	-	**MB**
	PR.5 – Instalar sistemas contra incendios	**Muy Baja**	-	-	A	-	-	B	-	-	**MB**
I.3 – Contaminación mecánica	PR.6 – Mantenimiento periódico del hardware	**Baja**	-	-	M	-	-	MB	-	-	**MB**
	RC.1 – Copias de seguridad periódicas	Alta	-	-	**B**	-	-	**MB**	-	-	**B**
	RC.2 – Guardar registros de configuración	Alta	-	-	**B**	-	-	**MB**	-	-	**B**
I.6 – Corte suministro eléctrico	IM.2 – Equipo contra corte eléctrico	**Muy Bajo**	-	-	B	-	-	MB	-	-	**MB**
	RC.1 – Copias de seguridad periódicas	Baja	-	-	**B**	-	-	**MB**	-	-	**MB**
	RC.3 – Plantes de contingencia y continuidad	Baja	-	-	**B**	-	-	**MB**	-	-	**MB**
A.7 – Uso no previsto	AW.1 – Elaborar normas del uso de TI	**Alta**	B	B	B	-	-	MB	-	-	**B**
	EL.1 – Mecanismos capar servicios web	**Baja**	B	B	B	-	-	MB	-	-	**MB**
A.15 – Modificación/Destrucción de info.	IM.1 – Cifrado de equipos hardware	Baja	-	**B**	B	-	-	**MB**	-	-	**MB**
	PR.3 – Control de acceso lógico	**Muy Baja**	-	B	B	-	-	MB	-	-	**MB**
	RC.1 – Copias de seguridad periódicas	Baja	-	B	**B**	-	-	**MB**	-	-	**MB**
A.23 – Manipulación de equipos	PR.2 Control de acceso físico	**Muy Baja**	B	-	B	-	-	MB	-	-	**MB**

HW.3 – Ordenadores para profesorado												
Amenazas	**Salvaguardas**	**Probabilidad**	**Dimensiones**			**Impacto Res.**			**Riesgo Res.**		
			C	**I**	**D**	**C**	**I**	**D**	**C**	**I**	**D**
N.1 – Fuego	IM.4 – Uso y mantenimiento extintores	**Muy Baja**	-	-	A	-	-	A	-	-	**M**
	PR.5 – Instalar sistemas contra incendios	**Muy Baja**	-	-	A	-	-	A	-	-	**M**
	RC.1 – Copias de seguridad periódicas	Muy Baja	-	-	**M**	-	-	**M**	-	-	**B**
	RC.3 – Plantes de contingencia y continuidad	Muy Baja	-	-	**M**	-	-	**M**	-	-	**B**
I.3 – Contaminación mecánica	PR.6 – Mantenimiento periódico del hardware	**Baja**	-	-	M	-	-	M	-	-	**B**
	RC.1 – Copias de seguridad periódicas	Alta	-	-	**B**	-	-	**B**	-	-	**M**
	RC.2 – Guardar registros de configuración	Alta	-	-	**B**	-	-	**B**	-	-	**M**
I.6 – Corte suministro eléctrico	IM.2 – Equipo contra corte eléctrico	**Muy Baja**	-	-	M	-	-	M	-	-	**B**
	RC.1 – Copias de seguridad periódicas	Baja	-	-	**B**	-	-	**B**	-	-	**B**
	RC.3 – Plantes de contingencia y continuidad	Baja	-	-	**B**	-	-	**B**	-	-	**B**
A.7 – Uso no previsto	AW.1 – Elaborar normas del uso de TI	**Media**	B	B	B	-	-	B	-	-	**B**
	EL.1 – Mecanismos capar servicios web	**Baja**	B	B	B	-	-	B	-	-	**B**
A.15 – Modificación/Destrucción de info.	IM.1 – Cifrado de equipos hardware	Baja	-	**B**	A	-	-	A	-	-	A
	PR.3 – Control de acceso lógico	**Muy Baja**	-	M	A	-	-	A	-	-	**M**
	RC.1 – Copias de seguridad periódicas	Baja	-	**B**	**B**	-	-	**B**	-	-	**B**
A.23 – Manipulación de equipos	PR.2 Control de acceso físico	**Muy Baja**	M	-	B	-	-	B	-	-	**MB**

HW.4 – Chromebook												
Amenazas	**Salvaguardas**	**Probabilidad**	**Dimensiones**			**Impacto Res.**			**Riesgo Res.**		
			C	**I**	**D**	**C**	**I**	**D**	**C**	**I**	**D**
N.1 – Fuego	IM.4 – Uso y mantenimiento extintores	**Muy Baja**	-	-	A	-	-	B	-	-	**MB**
	PR.5 – Instalar sistemas contra incendios	**Muy Baja**	-	-	A	-	-	B	-	-	**MB**
	RC.1 – Copias de seguridad periódicas	Muy Baja	-	-	**M**	-	-	**MB**	-	-	**MB**
	RC.3 – Plantes de contingencia y continuidad	Muy Baja	-	-	**M**	-	-	**MB**	-	-	**MB**
I.3 – Contaminación mecánica	PR.6 – Mantenimiento periódico del hardware	**Baja**	-	-	M	-	-	MB	-	-	**MB**
	RC.1 – Copias de seguridad periódicas	Alta	-	-	**B**	-	-	**MB**	-	-	**B**
	RC.2 – Guardar registros de configuración	Alta	-	-	**B**	-	-	**MB**	-	-	**B**
E.25 – Pérdida de equipos	PR.2 Control de acceso físico	**Baja**	B	-	M	-	-	B	-	-	**B**
A.25 - Robo	PR.2 Control de acceso físico	**Muy Baja**	B	-	A	-	-	M	-	-	**B**

HW.5 - Impresoras											
Amenazas	**Salvaguardas**	**Probabilidad**	**Dimensiones**			**Impacto Res.**			**Riesgo Res.**		
			C	**I**	**D**	**C**	**I**	**D**	**C**	**I**	**D**
N.1 – Fuego	IM.4 – Uso y mantenimiento extintores	**Muy Baja**	-	-	A	-	-	A	-	-	**M**
	PR.5 – Instalar sistemas contra incendios	**Muy Baja**	-	-	A	-	-	A	-	-	**M**
	RC.3 – Plantes de contingencia y continuidad	Muy Baja	-	-	**M**	-	-	**M**	-	-	**B**
I.3 – Contaminación mecánica	PR.6 – Mantenimiento periódico del hardware	**Baja**	-	-	M	-	-	M	-	-	**M**
	RC.2 – Guardar registros de configuración	Alta	-	-	**B**	-	-	**B**	-	-	**M**

HW.6 – Repetidores WiFi											
Amenazas	**Salvaguardas**	**Probabilidad**	**Dimensiones**			**Impacto Res.**			**Riesgo Res.**		
			C	**I**	**D**	**C**	**I**	**D**	**C**	**I**	**D**
N.1 – Fuego	IM.4 – Uso y mantenimiento extintores	**Muy Baja**	-	-	A	-	-	MA	-	-	**A**
	PR.5 – Instalar sistemas contra incendios	**Muy Baja**	-	-	A	-	-	MA	-	-	**A**
	RC.3 – Plantes de contingencia y continuidad	Muy Baja	-	-	**M**	-	-	**A**	-	-	**M**

HW.7 - Switch											
Amenazas	**Salvaguardas**	**Probabilidad**	**Dimensiones**			**Impacto Res.**			**Riesgo Res.**		
			C	**I**	**D**	**C**	**I**	**D**	**C**	**I**	**D**
N.1 – Fuego	IM.4 – Uso y mantenimiento extintores	**Muy Baja**	-	-	A	-	-	A	-	-	**M**
	PR.5 – Instalar sistemas contra incendios	**Muy Baja**	-	-	A	-	-	A	-	-	**M**
	RC.3 – Plantes de contingencia y continuidad	Muy Baja	-	-	**M**	-	-	**M**	-	-	**B**

HW.8 - Modem											
Amenazas	**Salvaguardas**	**Probabilidad**	**Dimensiones**			**Impacto Res.**			**Riesgo Res.**		
			C	**I**	**D**	**C**	**I**	**D**	**C**	**I**	**D**
N.1 – Fuego	IM.4 – Uso y mantenimiento extintores	**Muy Baja**	-	-	A	-	-	A	-	-	**M**
	PR.5 – Instalar sistemas contra incendios	**Muy Baja**	-	-	A	-	-	A	-	-	**M**
	RC.3 – Plantes de contingencia y continuidad	Muy Baja	-	-	**M**	-	-	**M**	-	-	**B**

Media.1 – Discos duros de administración												
Amenazas	**Salvaguardas**	**Probabilidad**	**Dimensiones**			**Impacto Res.**			**Riesgo Res.**		
			C	**I**	**D**	**C**	**I**	**D**	**C**	**I**	**D**
N.1 – Fuego	IM.4 – Uso y mantenimiento extintores	**Muy Baja**	-	-	A	-	-	A	-	-	**M**
	PR.5 – Instalar sistemas contra incendios	**Muy Baja**	-	-	A	-	-	A	-	-	**M**
	RC.1 – Copias de seguridad periódicas	Muy Baja	-	-	**M**	-	-	**M**	-	-	**B**
	RC.3 – Plantes de contingencia y continuidad	Muy Baja	-	-	**M**	-	-	**M**	-	-	**B**
I.3 – Contaminación mecánica	PR.6 – Mantenimiento periódico del hardware	**Baja**	-	-	M	-	-	M	-	-	**M**
	RC.1 – Copias de seguridad periódicas	Alta	-	-	**B**	-	-	**B**	-	-	**M**
	RC.2 – Guardar registros de configuración	Alta	-	-	**B**	-	-	**B**	-	-	**M**
I.6 – Corte suministro eléctrico	IM.2 – Equipo contra corte eléctrico	**Muy Baja**	-	-	A	-	-	A	-	-	**M**
	RC.1 – Copias de seguridad periódicas	Baja	-	-	**M**	-	-	**M**	-	-	**M**
	RC.3 – Plantes de contingencia y continuidad	Baja	-	-	**M**	-	-	**M**	-	-	**M**
E.1 – Errores de los usuarios	AD.1 – Formalización de procedimientos	**Media**	B	M	M	B	M	M	**B**	**M**	**M**
	RC.1 – Copias de seguridad periódicas	Muy Alta	B	**B**	**B**	B	**B**	**B**	M	**M**	**M**
	RC.2 – Guardar registros de configuración	Muy Alta	B	**B**	**B**	B	**B**	**B**	M	**M**	**M**
	RC.3 – Plantes de contingencia y continuidad	Muy Alta	B	**B**	**B**	B	**B**	**B**	M	**M**	**M**
A.15 – Modificación/Destrucción de info.	IM.1 – Cifrado de equipos hardware	Baja	-	**M**	**M**	-	-	**M**	-	-	**M**
	PR.3 – Control de acceso lógico	**Muy Baja**	-	A	A	-	-	A	-	-	**M**
	RC.1 – Copias de seguridad periódicas	Baja	-	**B**	**B**	-	-	**B**	-	-	**B**
	RC.3 – Plantes de contingencia y continuidad	Baja	-	**B**	**B**	-	-	**B**	-	-	**B**

Media.2 – Memorias USB												
Amenazas	**Salvaguardas**	**Probabilidad**	**Dimensiones**			**Impacto Res.**			**Riesgo Res.**		
			C	**I**	**D**	**C**	**I**	**D**	**C**	**I**	**D**
A.7 – Uso no previsto	AW.1 – Elaborar normas del uso de TI	**Media**	M	M	M	M	B	M	**M**	**B**	**M**
A.15 – Modificación/Destrucción de info.	IM.1 – Cifrado de equipos hardware	**Muy Baja**	-	M	M	-	B	M	-	**MB**	**B**
	PR.3 – Control de acceso lógico	**Muy Baja**	-	M	M	-	B	M	-	**MB**	**B**
A.25 – Robo	PR.2 Control de acceso físico	**Muy Baja**	A	-	M	A	-	M	**M**	-	**B**
	IM.1 – Cifrado de equipos hardware	Baja	**B**	-	M	**B**	-	M	**B**	-	M
E.1 – Errores de los usuarios	AW.1 – Elaborar normas del uso de TI	**Media**	A	B	M	A	MB	M	**A**	**MB**	**M**
	RC.1 – Copias de seguridad periódicas	Muy Alta	A	B	**B**	A	MB	**B**	MA	B	**M**
E.25 – Pérdida de equipos	PR.2 Control de acceso físico	**Muy Baja**	A	-	M	A	-	M	**M**	-	**B**
	IM.1 – Cifrado de equipos hardware	Baja	**B**	-	M	**B**	-	M	**B**	-	M

Media.3 – Archivadores y carpetas												
Amenazas	**Salvaguardas**	**Probabilidad**	**Dimensiones**			**Impacto Res.**			**Riesgo Res.**		
			C	**I**	**D**	**C**	**I**	**D**	**C**	**I**	**D**
N.1 – Fuego	IM.4 – Uso y mantenimiento extintores	**Muy Baja**	-	-	A	-	-	M	-	-	**B**
	PR.5 – Instalar sistemas contra incendios	**Muy Baja**	-	-	A	-	-	M	-	-	**B**
	RC.1 – Copias de seguridad periódicas	Muy Baja	-	-	**B**	-	-	**MB**	-	-	**MB**
	RC.3 – Plantes de contingencia y continuidad	Muy Baja	-	-	**B**	-	-	**MB**	-	-	**MB**
E.1 – Errores de los usuarios	AD.1 – Formalización de procedimientos	**Media**	A	B	A	M	MB	M	**M**	**MB**	**M**
	RC.3 – Plantes de contingencia y continuidad	Muy Alta	**B**	**B**	**B**	**MB**	**MB**	**MB**	**B**	**B**	**B**
E.25 – Pérdida de equipos	PR.2 Control de acceso físico	**Baja**	A	-	A	M	-	M	**M**	-	**M**
A.15 – Modificación/Destrucción de info.	RC.1 – Copias de seguridad periódicas	Baja	-	**B**	**B**	-	**MB**	**MB**	-	**MB**	**MB**
	RC.3 – Plantes de contingencia y continuidad	Baja	-	**B**	**B**	-	**MB**	**MB**	-	**MB**	**MB**

Media.4 – Almacenamiento en la nube											
Amenazas	**Salvaguardas**	**Probabilidad**	**Dimensiones**			**Impacto Res.**			**Riesgo Res.**		
			C	**I**	**D**	**C**	**I**	**D**	**C**	**I**	**D**
E.1 – Errores de los usuarios	AD.1 – Formalización de procedimientos	**Media**	B	B	B	MB	MB	MB	**MB**	**MB**	**MB**
	AW.1 – Elaborar normas del uso de TI	**Media**	B	B	B	MB	MB	MB	**MB**	**MB**	**MB**
	AW.2 – Formación sobre aplicación RGPD	**Media**	B	B	B	MB	MB	MB	**MB**	**MB**	**MB**
	RC.3 – Plantes de contingencia y continuidad	Muy Alta	B	**MB**	**MB**	MB	**MB**	**MB**	B	**B**	**B**

P.1 – Personal Docente												
Amenazas	**Salvaguardas**	**Probabilidad**	**Dimensiones**			**Impacto Res.**			**Riesgo Res.**		
			C	**I**	**D**	**C**	**I**	**D**	**C**	**I**	**D**
AE.7 – Deficiencias en la organización	AD.1 – Formalización de procedimientos	**Baja**	-	-	M	-	-	A	-	-	**M**
	AD.3 – Formalización de responsabilidades	**Baja**	-	-	M	-	-	A	-	-	**M**
	AW.1 – Elaborar normas del uso de TI	**Baja**	-	-	M	-	-	A	-	-	**M**

P.2 – Personal de TIC											
Amenazas	**Salvaguardas**	**Probabilidad**	**Dimensiones**			**Impacto Res.**			**Riesgo Res.**		
			C	**I**	**D**	**C**	**I**	**D**	**C**	**I**	**D**
E.7 – Deficiencias en la organización	AD.1 – Formalización de procedimientos	**Baja**	-	-	A	-	-	MA			**A**
	AD.3 – Formalización de responsabilidades	**Baja**	-	-	A	-	-	MA			**A**
	AW.1 – Elaborar normas del uso de TI	**Baja**	-	-	A	-	-	MA			**A**

S.1 – Servicio Web											
Amenazas	**Salvaguardas**	**Probabilidad**	**Dimensiones**			**Impacto Res.**			**Riesgo Res.**		
			C	**I**	**D**	**C**	**I**	**D**	**C**	**I**	**D**
E.1 – Errores de los usuarios	CR.1 – Cuentas de administración	Muy Alta	B	**B**	**B**	-	-	**MB**	-	-	**B**
	RC.2 – Guardar registros de configuración	Muy Alta	B	**B**	**B**	-	-	**MB**	-	-	**B**
	RC.3 – Plantes de contingencia y continuidad	Muy Alta	B	**B**	**B**	-	-	**MB**	-	-	**B**
E.2 – Errores de administrador	AD.1 – Formalización de procedimientos	**Baja**	-	-	M	-	-	B	-	-	**B**
	RC.2 – Guardar registros de configuración	Media	-	-	**B**	-	-	**MB**	-	-	**MB**
	RC.3 – Plantes de contingencia y continuidad	Media	-	-	**B**	-	-	**MB**	-	-	**MB**

SW.1 - Alexia												
Amenazas	**Salvaguardas**	**Probabilidad**	**Dimensiones**			**Impacto Res.**			**Riesgo Res.**		
			C	**I**	**D**	**C**	**I**	**D**	**C**	**I**	**D**
E.1 – Errores de los usuarios	CR.1 – Cuentas de administración	Muy Alta	B	**B**	B	MB	**B**	B	B	**M**	M
	AD.1 – Formalización de procedimientos	**Baja**	B	A	B	MB	A	B	**MB**	**A**	**B**
	AW.1 – Elaborar normas del uso de TI	**Media**	B	A	B	MB	A	B	**MB**	**A**	**B**
	AW.2 – Formación sobre aplicación RGPD	**Media**	B	A	B	MB	A	B	**MB**	**A**	**B**
	RC.3 – Plantes de contingencia y continuidad	Muy Alta	B	**B**	**B**	MB	**B**	**B**	B	**M**	**M**
E.2 – Errores de administrador	AD.1 – Formalización de procedimientos	**Muy Baja**	B	A	M	MB	A	M	**MB**	**M**	**B**
	AW.1 – Elaborar normas del uso de TI	**Baja**	B	A	M	MB	A	M	**MB**	**A**	**M**
	AW.2 – Formación sobre aplicación RGPD	**Baja**	B	A	M	MB	A	M	**MB**	**A**	**M**
	RC.2 – Guardar registros de configuración	Media	B	**B**	**B**	MB	**B**	**B**	MB	**B**	**B**
	RC.3 – Plantes de contingencia y continuidad	Media	B	**B**	**B**	MB	**B**	**B**	MB	**B**	**B**
E.20 – Vulnerabilidad de los programas	IM.3 – Instalación de antivirus	**Muy Baja**	A	M	B	M	M	B	**B**	**B**	**MB**
A.5 – Suplantación de identidad	CR.1 – Cuentas de administración	Muy Baja	A	**B**	-	M	B	-	B	MB	-
	PR.3 – Control de acceso lógico	**Muy Baja**	A	A	-	M	A	-	**B**	**M**	-
A.11 – Acceso no autorizado	PR.1 – Uso de claves y certificados para conexiones inalámbricas	**Muy Baja**	A	A	-	M	A	-	**B**	**M**	-
	PR.4 – Implantación contraseñas seguras	**Muy Baja**	A	A	-	M	A	-	**B**	**M**	-

SW.2 - Itaca												
Amenazas	**Salvaguardas**	**Probabilidad**	**Dimensiones**			**Impacto Res.**			**Riesgo Res.**		
			C	**I**	**D**	**C**	**I**	**D**	**C**	**I**	**D**
E.1 – Errores de los usuarios	CR.1 – Cuentas de administración	Muy Alta	B	**B**	B	MB	**B**	B	B	**M**	M
	AD.1 – Formalización de procedimientos	**Baja**	B	A	B	MB	A	B	**MB**	**A**	**B**
	AW.1 – Elaborar normas del uso de TI	**Media**	B	A	B	MB	A	B	**MB**	**A**	**B**
	AW.2 – Formación sobre aplicación RGPD	**Media**	B	A	B	MB	A	B	**MB**	**A**	**B**
	RC.3 – Plantes de contingencia y continuidad	Muy Alta	B	**B**	**B**	MB	**B**	**B**	B	**M**	**M**
E.2 – Errores de administrador	AD.1 – Formalización de procedimientos	**Muy Baja**	B	A	M	MB	A	M	**MB**	**M**	**B**
	AW.1 – Elaborar normas del uso de TI	**Baja**	B	A	M	MB	A	M	**MB**	**A**	**M**
	AW.2 – Formación sobre aplicación RGPD	**Baja**	B	A	M	MB	A	M	**MB**	**A**	**M**
	RC.2 – Guardar registros de configuración	Media	B	**B**	**B**	MB	**B**	**B**	MB	**B**	**B**
	RC.3 – Plantes de contingencia y continuidad	Media	B	**B**	**B**	MB	**B**	**B**	MB	**B**	**B**
E.20 – Vulnerabilidad de los programas	IM.3 – Instalación de antivirus	**Muy Baja**	A	M	B	M	M	B	**B**	**B**	**MB**
A.5 – Suplantación de identidad	CR.1 – Cuentas de administración	Muy Baja	A	**B**	-	M	**B**	-	**B**	MB	-
	PR.3 – Control de acceso lógico	**Muy Baja**	A	A	-	M	A	-	**B**	**M**	-
A.11 – Acceso no autorizado	PR.1 – Uso de claves y certificados para conexiones inalámbricas	**Muy Baja**	A	A	-	M	A	-	**B**	**M**	-
	PR.4 – Implantación contraseñas seguras	Muy Baja	A	A	-	M	A	-	B	M	-

6. Gestión de riesgos

En este apartado se va a realizar un análisis de riesgos a partir de las medidas de impacto y riesgos calculados en apartados anteriores. El objetivo de este apartado es decidir qué riesgos son asumibles o aceptables por parte de la organización y qué riesgos han de ser tratados por suponer un riesgo grave o crítico para el centro.

Para ello, el primer paso es establecer un umbral de aceptación de forma que los riesgos que no superen ese umbral sean aceptados por el colegio. En este caso se va a tomar como riesgos asumibles, es decir, riesgos sobre los que no se van a tomar ningún tipo de medidas, aquellas amenazas para las que se haya establecido un riesgo Bajo o Muy Bajo, que indica que o bien que la probabilidad de que esta se produzca es baja, o que el impacto causado al colegio no es especialmente elevado.

Todas aquellas amenazas para las que se haya estimado un riesgo Medio se considerarán riesgos apreciables, y para estos, si bien no se llevarán a cabo medidas concretar para reducir su riesgo, se tratarán de forma colateral en las salvaguardas de concienciación y serán tenidos en cuenta para la elaboración de planes de contingencia y continuidad.

Por último, todas aquellas amenazas que entrañen un riesgo Alto o Muy Alto se evaluarán como riesgos graves o críticos y para ellos se valorarán diferentes escenarios según la implantación de diferentes salvaguardas.

A continuación, se van a analizar las diferentes amenazas que ponen en riesgo el Sistema de Información del colegio y cuáles son las diferentes salvaguardas que se pueden aplicar. En los siguientes subapartados se van a estudiar, por bloques según los diferentes tipos de activos del centro, las amenazas a las que están expuestos estos activos y que superan los umbrales de aceptación. Después para cada uno de estos bloques se plantearán diferentes escenarios con diferentes salvaguardas y se decidirá cuál es el escenario más conveniente en función del coste, la efectividad y la necesidad de dichas salvaguardas.

6.1 Datos

Según lo visto en el capítulo de estimación de riesgos para los activos “Datos de matrícula” y “Expedientes académicos” las amenazas “Suplantación de identidad” y “Acceso no autorizado” generan el riesgo indicado en la siguiente tabla que, si bien es apreciable, es asumible para el centro teniendo en cuenta que se tratará de forma colateral en los planes de contingencia.

Amenazas	Impacto Potencial			Riesgo Potencial		
	C	I	D	C	I	D
A.5 – Suplantación de identidad	A	A	-	M	M	-
A.11 – Acceso no autorizado	A	M	-	M	B	-

En lo referente a los riesgos que deben ser tratados, las siguientes amenazas de los bloques de “Errores” o “Ataques intencionados” generan un riesgo “Alto” o “Muy Alto” principalmente en las dimensiones de confidencialidad e integridad.

Amenazas	Impacto Potencial			Riesgo Potencial		
	C	I	D	C	I	D
E.1 - Errores de los usuarios	M	MA	MB	A	MA	B
E.2 – Errores de administrador	M	M	MA	M	M	MA
E.19 - Fugas de información	MA	-	-	MA	-	-
A.5 – Suplantación de identidad	MA	M	-	A	B	-
A.11 – Acceso no autorizado	MA	M	-	A	B	-
A.15 – Modificación/Destrucción de info.	-	A	M	-	A	M

Tal y como se ha detallado en el análisis de salvaguardas, la medida “AD.1 – Formalización de procedimientos” permite mitigar los riesgos relacionados con los errores de usuarios y errores de administración reduciendo la probabilidad de que estos ocurran. Además, la elaboración de copias de seguridad periódicas permite mitigar los riesgos relacionados con los errores de usuarios y la modificación y destrucción de información. Por último, las salvaguardas de concienciación como “AW.1 – Elaborar normas de uso de las TI” o “AW.2 – Formación sobre el RGPD” permitirían mitigar los riesgos de que se produjeran fugas de información y la implantación de controles de acceso lógico sobre los elementos informáticos, así como la implantación de un sistema de contraseñas seguras ayudaría a mitigar los riesgos relacionados con las amenazas “A.5 – Suplantación de identidad” y “A.11 – Acceso no autorizado”.

También cabe mencionar las medidas “RC2 – Guardar registros de configuración” y “RC3 – Creación de planes de contingencia” que permitirían reducir los riesgos relacionados con los errores de usuarios y la modificación y destrucción de información. Si bien son medidas más costosas de implantar (En esfuerzo del personal, no tanto en términos económicos) supondrían

reducir en gran medida los riesgos relacionados con activos muy valiosos y por tanto se llevará a cabo su implantación.

Por último, la medida "IM.1 – Cifrado de equipos hardware" permitiría reducir los riesgos relacionados con las fugas de información y el acceso no autorizado. Sin embargo, teniendo en cuenta que el coste de implantación de esta salvaguarda también es elevado y es una medida complementaria a otras de las salvaguardas que ya se han mencionado no se llevará a cabo la implantación de esta medida.

Con la implantación de estas salvaguardas, el mapa de los riesgos que antes eran "Importantes" o "Críticos" quedaría de la siguiente manera.

Amenazas	Impacto Potencial			Riesgo Potencial		
	C	I	D	C	I	D
E.1 - Errores de los usuarios	M	**M**	MB	**B**	**B**	**MB**
E.2 – Errores de administrador	M	M	**A**	M	M	MA
E.19 - Fugas de información	MA	-	-	**M**	-	-
A.5 – Suplantación de identidad	MA	M	-	**B**	**MB**	-
A.11 – Acceso no autorizado	MA	M	-	**M**	**MB**	-
A.15 – Modificación/Destrucción de info.	-	A	M	-	**M**	**MB**

6.2 Redes de comunicaciones

En lo referente a las redes de comunicaciones, según lo visto en el análisis de riesgos, la red telefónica se ve afectada por la amenaza "A.7 – Uso no previsto", sin embargo, genera un riesgo Bajo que se podría considerar como aceptable, como se puede ver en la siguiente tabla. Precisamente por la poca probabilidad de que esto ocurra y por el bajo impacto que supondría se asumirá este riesgo.

Amenazas	Impacto Potencial			Riesgo Potencial		
	C	I	D	C	I	D
A.7 – Uso no previsto	-	-	MB	-	-	B

Por otro lado, existen riesgos medios relacionados con los errores de administrador en la red WiFi y los fallos en el servicio de comunicación para la red telefónica. Con respecto a la segunda el buen funcionamiento del servicio telefónico debe estar asegurado por el proveedor del servicio, así que ese riesgo es compartido entre el colegio y la compañía telefónica. Por su parte el riesgo de errores de administrador en la red WiFi, pese a ser un riesgo que por su impacto podría ser asumible, puede tratarse sin un gran coste guardando los registros de la configuración de la red, por esto se abordará la implantación de esta medida. De esta forma la tabla de riesgos apreciables quedaría de la siguiente manera.

Amenazas	Impacto Potencial			Riesgo Potencial		
	C	I	D	C	I	D
I.8 – Fallo de servicios de comunicaciones	-	-	B	-	-	M
E.2 – Errores de administrador	-	-	**B**	-	-	**B**

A continuación, se incluye una tabla con las amenazas que producen riesgos “Altos” o “Muy Altos” en diferentes activos del bloque de “Redes de Comunicación”.

Amenazas	Impacto Potencial			Riesgo Potencial		
	C	I	D	C	I	D
I.8 – Fallo de servicios de comunicaciones	-	-	A	-	-	MA
A.7 – Uso no previsto	-	-	M	-	-	A

En primer lugar, existe la posibilidad de que ocurriera un fallo en los servicios de comunicaciones, que si antes no era excesivamente perjudicial en la red telefónica, para la red ADSL o la red WiFi supondría un daño importante para el colegio, no tanto por el valor de la propia red, sino el impacto a la disponibilidad de otros activos que dependen de estas redes. Para evitar estos fallos por un lado se pueden tomar medidas para proteger los diferentes elementos de la red (Que se analizarán posteriormente), y por otro se debe trabajar en establecer planes de contingencia y continuidad para aquellos casos en los que se produzca esta amenaza.

Y, en segundo lugar, el uso no previsto de las redes WiFi puede afectar negativamente a su disponibilidad causando un riesgo “Alto” para el centro. Para evitar esta situación es importante establecer una normas básicas del uso de las TI como medida de concienciación en el centro. Para intentar eliminar la posibilidad de que se produzca esta amenaza se implantará la salvaguarda “EL.1 – Mecanismos para capar servicios web” que permitan implantar un proxy que impida el uso de algunos servicios o el acceso a diferentes páginas web y evitar así el uso indebido de la red WiFi.

Con esto el mapa de riesgos “Críticos” para las redes de comunicaciones quedaría de la siguiente manera.

Amenazas	Impacto Potencial			Riesgo Potencial		
	C	I	D	C	I	D
I.8 – Fallo de servicios de comunicaciones	-	-	**M**	-	-	**M**
A.7 – Uso no previsto	-	-	M	-	-	**B**

6.3 Hardware

Tal y como se analizó en el apartado de gestión de riesgos, a continuación, se adjunta una tabla con las amenazas que suponen riesgos “Bajos” o “Muy Bajos” para algunos de los activos del colegio.

Amenazas	Impacto Potencial			Riesgo Potencial		
	C	I	D	C	I	D
A.24 - Denegación de servicio	-	-	M	-	-	B
A.7 – Uso no previsto	-	-	B	-	-	B
A.23 – Manipulación de equipos	-	-	B	-	-	MB
A.25 – Robo	-	-	B	-	-	B
E.25 – Pérdida de equipos	-	-	MB	-	-	MB

Estás amenazas suponen un riesgo muy bajo para el colegio y por tanto es más eficiente asumir el riesgo que implantar salvaguardas para proteger los activos afectados.

Con respecto a las amenazas que suponen un riesgo medio se adjunta la siguiente tabla. En ella podemos observar como fuentes de estos riesgos, por un lado, los ataques intencionados para la modificación o destrucción de información que si bien supondrían un impacto considerable para el colegio son muy improbables, y por otro lado las averías como el corte del suministro eléctrico o la contaminación electromagnética. Para evitar los riesgos producidos por averías se podrían tomar medidas como la implantación de hardware específico. Teniendo en cuenta que el riesgo no es especialmente elevado sería recomendable implantar esta medida con recursos que no sean especialmente costosos como regletas con protección contra sobrecargas eléctricas y evitar inversiones más costosas. De cara a evitar ataques intencionados que busquen modificar o borrar información a través de los elementos hardware se podría implantar mecanismos de cifrado o de control lógico para los elementos hardware, pero su elevado coste lo hace una medida no rentable.

Amenazas	Impacto Potencial			Riesgo Potencial		
	C	I	D	C	I	D
I.6 – Corte del suministro eléctrico	-	-	M	-	-	M
A.15 – Modificación/Destrucción de info.	-	-	A	-	-	M
I.4 – Contaminación electromagnética	-	-	M	-	-	M

Por último, se adjunta una tabla con las amenazas que producen riesgos “Altos” o “Muy Altos”.

Amenazas	Impacto Potencial			Riesgo Potencial		
	C	I	D	C	I	D
N.1 – Fuego	-	-	MA	-	-	A
A.26 – Ataque destructivo	-	-	MA	-	-	A
I.3 – Contaminación mecánica	-	-	M	-	-	A

Estas son las amenazas que suponen mayor riesgo para los activos del centro, por un lado, los daños causados por un posible incendio que si bien tienen una probabilidad muy baja supondrían un gran coste económico para el colegio. Por otro lado, los efectos causados por una persona que decida dañar intencionadamente los elementos hardware del colegio que también supondrían un gran coste económico en concepto de reparación o sustitución. Y finalmente los efectos causados por el uso normal de estos aparatos que por el propio uso acaban sufriendo diferentes averías.

Para mitigar los efectos de la contaminación mecánica se puede realizar un mantenimiento periódico de los equipos hardware del colegio para intentar que estas averías sucedan lo menos frecuentemente posible. Además, es importante llevar a cabo una gestión planificada de las copias de seguridad que se realizan de aquellos equipos que almacenan información sensible o que no se encuentra en otras plataformas para así, reducir los daños causados en caso de avería de esos equipos.

Para evitar los daños producidos por un posible incendio es vital la implantación de sistemas contra incendios y mantenimiento periódico del mismo, salvaguarda que ya está implantada en el centro, así que sería conveniente realizar esfuerzos en diseñas planes de contingencia y continuidad en caso de que ocurra una amenaza de este tipo.

Por último, con respecto a la amenaza de un ataque destructivo por parte de personal del centro o ajeno podría llevarse a cabo la implantación de medidas de control de acceso físico. Sin embargo, estas medidas tienen un coste muy elevado y la probabilidad de estos ataques es baja, así pues, se definirá un plan de actuación como mecanismo de continuidad en caso de que se produzca esta amenaza.

Con esto la tabla con los riesgos residuales con respecto a los actuales riesgos críticos para los activos de hardware del centro quedaría de la siguiente manera.

Amenazas	Impacto Potencial			Riesgo Potencial		
	C	I	D	C	I	D
N.1 – Fuego	-	-	M	-	-	M
A.26 – Ataque destructivo	-	-	M	-	-	M
I.3 – Contaminación mecánica	-	-	M	-	-	B

6.4 Soportes de información

Tal y como se puede ver en la siguiente tabla, las amenazas "Uso no previsto", "Robo" y "Pérdida de equipos" provocan diferentes riesgos bajos para los soportes de información del colegio. Esto se debe principalmente a que el impacto de estas amenazas es bastante bajo. Es por esto por lo que se tomarán estos riesgos como "Asumibles".

Amenazas	Impacto Potencial			Riesgo Potencial		
	C	I	D	C	I	D
A.7 – Uso no previsto	MB	MB	M	MB	MB	M
A.25 – Robo	M	-	M	B	-	B
E.25 – Pérdida de equipos	MB	-	B	B	-	M

En lo referente a aquellas amenazas que suponen riesgos de nivel "Medio" encontramos por un lado los riesgos causados por las amenazas de "Fuego" y un ataque de "Modificación y destrucción de datos". Estas amenazas si bien producen unos daños importantes, son muy poco probables y por tanto su riesgo no es demasiado elevado, así que únicamente se tendrán en cuenta en los planes de contingencia y continuidad.

Por su parte las amenazas "Uso no previsto" y "Pérdida de equipos" suponen un riesgo apreciable para la disponibilidad de los activos "M2 – Memorias USB" y "M3 – Material impreso" respectivamente. Para evitar el mal uso de las memorias USB es recomendable llevar a cabo medidas de concienciación y para mitigar los efectos de la perdida de los activos relacionados con el material impreso es importante tener esos datos duplicados en plataformas digitales.

Amenazas	Impacto Potencial			Riesgo Potencial		
	C	I	D	C	I	D
N.1 – Fuego	-	-	M	-	-	M
A.15 – Modificación/Destrucción de info.	A	A	A	M	M	M
A.7 – Uso no previsto	MB	MB	M	MB	MB	M
E.25 – Pérdida de equipos	M	-	M	M	-	M

Por último, en la siguiente tabla se listan las amenazas que suponen un riesgo más importante para los soportes de información del centro.

Amenazas	Impacto Potencial			Riesgo Potencial		
	C	I	D	C	I	D
I.3 – Contaminación mecánica	-	-	M	-	-	A
I.6 – Corte de suministro eléctrico	-	-	A	-	-	A
I.10 – Degradación soportes de información	-	-	A	-	-	MA
E.1 – Errores de los usuarios	A	A	A	A	A	A

En primer lugar, cabe destacar que el activo que genera un mayor riesgo en este bloque son los "Discos duros de administración" debido a que almacenan información muy relevante para el funcionamiento del centro que no está duplicada en otros soportes.

Para mitigar gran parte del riesgo derivado de las amenazas que pertenecen al bloque de averías industriales, es importante implementar un procedimiento de copias de seguridad periódicas que permita, en caso de que se produzca uno de estos errores no perder los datos. Además, el mantenimiento periódico del material hardware o la compra de material específico (Equipamiento de soporte de alimentación ininterrumpida o regletas con protección para sobrecarga eléctrica …), si bien son medidas algo más costosas permitirían reducir en gran medida estos riesgos.

Finalmente, en lo referente a los errores cometidos por los usuarios, las medidas más útiles para mitigar el riesgo, además de las ya citadas copias de seguridad, son la formalización de procesos a realizar por los usuarios y la realización de planes de contingencia y continuidad.

De esta forma el mapa de los riesgos residuales quedaría así.

Amenazas	Impacto Potencial			Riesgo Potencial		
	C	I	D	C	I	D
I.3 – Contaminación mecánica	-	-	M	-	-	M
I.6 – Corte de suministro eléctrico	-	-	M	-	-	B
I.10 – Degradación soportes de información	-	-	M	-	-	M
E.1 – Errores de los usuarios	M	M	B	M	M	B

6.5 Personal

Con respecto a los activos del bloque de personal, únicamente se ha identificado una amenaza, concretamente "E.7 – Deficiencias en la organización". Esta amenaza afecta a la disponibilidad del personal debido a que, por culpa de la falta de procedimientos definidos o por la inoperatividad de la estructura del personal, se dediquen mas esfuerzos de los necesarios para las tareas habituales del personal del colegio.

Amenazas	Impacto Potencial			Riesgo Potencial		
	C	I	D	C	I	D
E.7 – Deficiencias en la organización	-	-	A	-	-	A

Para mitigar los efectos de esta amenaza, las salvaguardas pasan por un lado por formalizar los procedimientos que tiene que realizar el personal y crear una documentación asociada a esos procedimientos, y por otro lado por formalizar las responsabilidades que debe acarrear cada individuo.

Con estas medidas se busca evitar que se produzcan estas deficiencias en la organización que afectan negativamente al rendimiento del personal del centro. El riesgo se reduciría de la siguiente manera.

Amenazas	Impacto Potencial			Riesgo Potencial		
	C	I	D	C	I	D
E.7 – Deficiencias en la organización	-	-	M	-	-	B

6.6 Servicios

Este es el bloque de activos que supone menos riesgo para el centro, principalmente porque el valor de los activos es muy bajo y la probabilidad de que se materialicen las amenazas es también baja. A continuación, se incluye una tabla con los riesgos de este bloque.

Amenazas	Impacto Potencial			Riesgo Potencial		
	C	I	D	C	I	D
E.1 – Errores de los usuarios	-	-	MB	-	-	B
E.2 – Errores de administrador	-	-	B	-	-	B
A.15 – Modificación/destrucción de info	-	-	MB	-	-	MB
E.20 – Vulnerabilidad de los programas	-	-	M	-	-	B
A.7 – Uso no previsto	-	-	M	-	-	B

Todos los riesgos que afectan a este bloque de activos son de niveles "Bajo" o "Muy Bajos" y son perfectamente asumibles para el colegio.

6.7 Software

En este bloque se describen las amenazas y riesgo que afectan a los activos software entre los que destacan los programas de Itaca y Alexia.

Debido al gran valor de estos activos la mayoría de las amenazas generan riesgos altos. Analizando en primer lugar los riesgos más bajos, las amenazas "Abuso de privilegios de acceso" y "Denegación de servicio" riesgos "Bajos" en Integridad y Disponibilidad y riesgo "Medio" en Disponibilidad respectivamente. Teniendo en cuenta que los programas Itaca y Alexia son externos al centro, la responsabilidad de dar respuestas ante ataques, junto al hecho de que no son riesgos excesivamente altos hace que sean asumibles por parte del centro.

Por parte de los riesgos "Medios" que afectan a la disponibilidad para las diferentes amenazas relacionadas con errores, la principal medida a llevar a cabo pasa por formalizar los diferentes procedimientos que hay que realizar con este software. Esto permitiría disminuir el número de errores y así mitigar el riesgo. Igualmente es necesario, debido al alto valor de los activos afectados, definir los planes de contingencia y continuidad para estas amenazas.

Amenazas	**Impacto Potencial**			**Riesgo Potencial**		
	C	**I**	**D**	**C**	**I**	**D**
A.6 – Abuso de privilegios de acceso	A	M	B	A	B	B
A.24 - Denegación de servicio	-	-	A	-	-	M
E.1 – Errores de los usuarios	M	MA	B	A	MA	M
E.2 – Errores de administrador	M	MA	M	M	MA	M
E.20 – Vulnerabilidad de los programas	MA	A	M	MA	A	M

Finalmente, los riesgos más elevados para este bloque de activos se adjuntan en la siguiente tabla.

Amenazas	**Impacto Potencial**			**Riesgo Potencial**		
	C	**I**	**D**	**C**	**I**	**D**
E.1 – Errores de los usuarios	M	A	B	A	MA	M
E.2 – Errores de administrador	M	A	M	M	MA	M
A.5 – Suplantación de identidad	MA	A	-	A	A	-
A.11 – Acceso no autorizado	MA	MA	-	A	A	-
E.20 – Vulnerabilidad de los programas	MA	A	M	MA	A	M

Tal y como se ha mencionado antes, las amenazas “E.1 – Errores de los usuarios” y “E.2 – Errores de administrador” generan un riesgo “Alto” para la confidencialidad y la integridad de estos activos y la principal manera de mitigar este riesgo es la formalización de los procedimientos a realizar.

Por su parte para mitigar los riesgos de la amenaza “A.5 – Suplantación de identidad” sería conveniente implantar controles de acceso lógico para el acceso a este software. Puesto que el software es de terceros, la responsabilidad de implantar estas medidas en el propio software no son responsabilidad del colegio. Sin embargo, si existen es responsabilidad del centro utilizarlas correctamente y si no reclamarlo a las empresas desarrolladores.

Finalmente, en cuanto a la amenaza “A.11 – Acceso no autorizado” las principales salvaguardas que permitirían mitigar los riesgos derivados de esta amenaza serían, por un lado la implantación de contraseñas seguras para el acceso a este software, y por otro lado el uso de claves y certificados para las conexiones inalámbricas que permitan acceder a este software.

Con la aplicación de estas medidas se permitiría reducir los riesgos de este bloque para que quedaran de la siguiente manera.

Amenazas	**Impacto Potencial**			**Riesgo Potencial**		
	C	**I**	**D**	**C**	**I**	**D**
E.1 – Errores de los usuarios	M	**B**	B	**B**	**M**	M
E.2 – Errores de administrador	**MB**	A	M	**MB**	**M**	**B**
A.5 – Suplantación de identidad	**M**	A	-	**B**	**B**	-
A.11 – Acceso no autorizado	**M**	**A**	-	**M**	**M**	-

6.8 Conclusión

En este apartado, y con el objetivo de resumir los resultados del proceso de gestión de riesgos, se van a listar las salvaguardas a aplicar para cada uno de los bloques de activos analizados previamente.

Para ello, en las siguientes tablas se definen, para cada bloque las salvaguardas a aplicar según lo analizado a lo largo de este apartado.

Datos	
AD.1 – Formalización de procedimientos del centro	AW.2 – Formación sobre el RGPD
RC.1 –Realización de copias de seguridad regulares	RC.2 – Guardar registros de configuración
AW.1 – Elaborar normas básicas sobre el uso de las TI	RC.3 – Planes de contingencia y continuidad

Redes de comunicaciones	
AW.1 – Elaborar normas básicas sobre el uso de las TI	RC.3 – Planes de contingencia y continuidad
PR.2 – Mecanismos de control de acceso físico	EL.1 – Mecanismos para capar servicios web

Hardware	
PR.6 – Mantenimiento periódico	RC.3 – Planes de contingencia y continuidad
RC.1 – Realización de copias de seguridad regulares	PR.3 – Control de acceso físico

Soportes de información	
IM.2 – Instalación de equipo contra corte eléctrico	RC.2 – Copias de seguridad periódicas
AD.1 – Formalización de procedimientos del centro	PR.6 – Mantenimiento periódico

Personal	
AD.3 – Formalización de responsabilidades	AD.1 – Formalización de procedimientos

Software	
AD.1 – Formalización de procedimientos del centro	PR.4 – Implementar directivas de contraseña segura
PR.3 – Mecanismos de control de acceso lógico	PR.1 – Certificados para WiFi

Una vez identificadas cuáles son las salvaguardas que permitirían reducir el riesgo de los activos del centro a valores asumibles, se desarrollarán en los programas y planes de seguridad desarrollados en los siguientes apartados.

7. Programas de seguridad

En este apartado se van a crear diferentes programas de seguridad que permitirán implantar de manera organizada y controlada las diferentes salvaguardas propuestas tras el análisis de riesgos.

Para ello, a continuación, se incluyen diferentes fichas para los proyectos que se vayan a realizar con la información necesaria para que el colegio pueda poner en marcha estos proyectos. En estas fichas se detallará para cada proyecto de seguridad la siguiente información:

- Identificador y nombre.
- Salvaguardas implementadas en el proyecto.
- Activos del sistema de información afectados.
- Estimación de costes, tanto económicos como de esfuerzo.
- Objetivos del proyecto.
- Descripción del proyecto y tareas que realizar para su puesta en funcionamiento.
- Controles y medidores para medir la efectividad de las medidas implantadas.

Con estas fichas se pretende conseguir que el centro tenga los recursos y la información necesaria para poder poner en marcha las diferentes medidas propuestas, ya sea por el propio personal del centro o por personal ajeno al centro que se dedique específicamente a este sector.

Entendiendo que el centro no tiene la capacidad, ni en algunos casos la necesidad, de invertir un gran número de horas de trabajo ni de recursos en la implantación de estos programas de seguridad estos se han realizado para conllevar el menor gasto posible.

Así para cada proyecto se ha establecido el tiempo de implantación aproximado teniendo en cuenta un trabajo de 2 horas semanales por parte de los responsables asignados. Estas horas se corresponderán con las horas correspondientes a las horas complementarias de la jornada de los profesores.

ID:	DOC01
Nombre Programa:	Formalización de procedimientos y responsabilidades
Detalles	

Salvaguardas aplicadas

AD.1 – Formalización de procedimientos del centro
AD.3 – Formalización de responsabilidades del personal

Activos afectados

D.1 – Datos de matrícula
D.2 – Expedientes académicos
D.4 – Copias de seguridad
Media.1 – Discos duros de administración
Media.3 – Archivadores y carpetas
Media.4 – Almacenamiento en la nube
P.1 – Personal Docente
P.2 – Personal de TIC
SW.1 - Alexia
SW.2 - Itaca

Costes

Tiempo de implantación:	4 meses (96 horas)
Recursos necesarios:	2 horas de trabajo semanales por parte de un responsable de dirección, un responsable del departamento de TIC y un responsable del departamento de administración
Coste Total:	Utilizando las horas correspondientes a las horas complementarias de la jornada de los profesores el coste dependerá del salario/hora de los responsables del proyecto

Objetivos

- Conseguir que todos los procesos desarrollados por el personal del centro estén definidos y documentados.
- Evitar que la transmisión del “know-how” o conocimiento sobre el funcionamiento del centro dependa del buen hacer de su personal.
- Mejorar la organización del personal definiendo y formalizando las responsabilidades de los diferentes puestos y departamentos.

Descripción

La idea de este programa es elaborar una serie de documentos donde se recoja todo el conocimiento sobre el funcionamiento del centro. De esta forma, quedarán definidos qué

procesos relacionados con los activos de información objeto de tratamiento, debe saber realizar el personal del centro y cómo se deben realizar.

En estos documentos se deben recoger los procedimientos que deben realizar de forma habitual profesores y personal de administración en relación con el sistema de información del centro. Algunos de los procedimientos susceptibles de ser recogidos en estos documentos serían: La gestión de expedientes académicos en la plataforma de Itaca, gestión de la información del banco de libros, gestión del comedor, actividades extraescolares…

Además, en este programa se abordará la tarea de definir los roles y las responsabilidades que tiene el personal del centro en función de su puesto, departamento etc.

Así, se creará un documento escrito dónde se recogerá el organigrama del centro con los diferentes puestos, departamentos y comisiones y se especificará cuáles son las tareas que tienen que realizar los miembros de cada departamento. Esto permitiría mejorar la organización del centro y delimitar las responsabilidades del personal.

Controles

Puesto que el resultado de este programa es un documento de gestión interna lo primero que se ha de controlar es que después de realizar este documento no quede desactualizado, para ello cuando se produzcan cambios en el organigrama del centro o se modifiquen los procedimientos actuales (Por ejemplo, en el momento en que se migren diferentes elementos de la gestión del centro a la plataforma Itaca) deberán actualizarse estos documentos.

Por otro lado, para comprobar hasta qué punto esta medida ayuda a la gestión interna del personal del centro se deberían establecer encuestas de satisfacción o de evaluación al personal del centro. De esta forma se podría analizar anualmente que procesos no funcionan como deberían o que cuestiones son susceptibles de mejorar.

ID:	DOC02
Nombre Programa:	Creación de políticas de TI
Detalles	

Salvaguardas aplicadas

AW.1 – Elaborar normas básicas sobre el uso de las TI
AW.2 – Formación acerca del nuevo Reglamento General de Protección de Datos

Activos afectados

D.1 – Datos de matrícula
D.2 – Expedientes académicos
D.4 – Copias de seguridad
COM.2 – Red WiFi
HW.2 – Ordenadores para alumnado
HW.3 – Ordenadores para profesorado
Media.2 – Memorias USB
Media.4 – Almacenamiento en la nube
SW.1 – Alexia
SW.2 - Itaca

Costes

Tiempo de implantación:	4 meses (64 horas)
Recursos necesarios:	2 horas de trabajo semanales por parte de un responsable de dirección y un responsable del departamento de TIC
Coste Total:	Utilizando las horas correspondientes a las horas complementarias de la jornada de los profesores el coste dependerá del salario/hora de los responsables del proyecto

Objetivos

- Crear normas para el uso de la tecnología en el colegio para el profesorado y para los alumnos.
- Aprovechar la tecnología para mejorar las tareas diarias del personal del centro.
- Resolver cuestiones referentes a la aplicación del nuevo RGPD en el centro y más concretamente en lo referente a las TI.

Descripción

Con este programa se pretende definir las políticas que deben seguir tanto el personal del centro como los alumnos en lo referente al buen uso de las TI.

A nivel de profesorado, el objetivo sería crear un pequeño documento con normas básicas o buenas prácticas para el uso de las TI en el centro, además de crear material de apoyo (como posters o trípticos) que permitan ayudar a la concienciación. Este documento recogerá las

buenas prácticas a llevar a cabo en temas como: control de acceso, copias de seguridad, seguridad en internet, gestión de dispositivos…

A nivel de alumnado, el objetivo es hacerles conscientes de las normas básicas que deben seguir en el uso de las TI tanto en el colegio como en casa. Así, esta tarea estaría menos enfocada a establecer normas y más a la divulgación de buenas prácticas. Para ello se pueden realizar talleres de formación, posters, trípticos, videos etc.

Para la realización de estas normas o buenas prácticas se seguirá las pautas marcadas por el INCIBE (Instituto Nacional de Ciberseguridad), ya que dispone de una gran cantidad de material enfocado a la creación de políticas de seguridad TI en empresas y el uso responsable de TI para particulares, además de ser el referente a nivel nacional de esta cuestión.

Por otro lado, en este programa de seguridad se abordaría la creación de un documento con las medidas a seguir por el personal del centro para cumplir las normas propuestas en el RGPD. Esto es de vital importancia teniendo en cuenta lo novedoso del Reglamento General de Protección de Datos y al gran control que supone para una organización que trabaja con personas menores de edad. En este documento se abordará el tratamiento de información sobre los alumnos del centro como pueden ser expedientes académicos o información personal. Además, se abordará la gestión de las tecnologías de la información para el cumplimiento de esta normativa.

Controles

Teniendo en cuenta que uno de los objetivos principales es concienciar tanto al personal del centro como a los alumnos los controles tendrán que ir enfocados a si la concienciación es efectiva. Para ello se realizarán encuestas o actividades para valorar el nivel de conocimiento sobre todo para el alumnado del centro.

Por otro lado, para medir si se cumplen o no las normas especificadas por el RGPD se designará un departamento del personal del centro que se responsabilice de velar porque se cumplen las normas impuestas en el documento propuesto en este programa.

ID:	DOC03
Nombre Programa:	Plan de contingencia y continuidad
Detalles	

Salvaguardas aplicadas

RC.3 – Planes de contingencia y continuidad

Activos afectados

Datos	Hardware
Redes de comunicaciones	Software
Servicios	

Costes

Tiempo de implantación:	4 meses (64 horas)
Recursos necesarios:	2 horas de trabajo semanales por parte de un responsable del departamento de TIC y un responsable del departamento de administración
Coste Total:	Utilizando las horas correspondientes a las horas complementarias de la jornada de los profesores el coste dependerá del salario/hora de los responsables del proyecto

Objetivos

- Elaboración de un plan de contingencia y recuperación ante incidentes.
- Definir el método de actuación para minimizar el impacto de las posibles amenazas que afecten al sistema de información del centro.

Descripción

Teniendo en cuenta que un sistema nunca va a estar 100% protegido es importantes definir la estrategia a seguir en caso de que se produzca una incidencia grave para intentar que cause el menor impacto posible.

Para ello se desarrollará un plan de contingencia y continuidad en el cual se organizará el personal del centro en equipos, se establecerán funciones y responsabilidades en caso de incidencia, se definirán los procedimientos de actuación ante incidentes y la estrategia para la vuelta a la normalidad.

La creación de equipos es importante para que, en caso de incidencia, haya una parte de personal encargado de atender esa incidencia mientras que el resto del personal del colegio se dedica a su actividad normal.

Los procedimientos de actuación ante incidentes se definirán para intentar recuperar la actividad normal del centro haciendo uso de copias de seguridad o equipos de respaldo, reanudar y verificar el correcto funcionamiento de los procesos afectados e identificar las causas del incidente.

Controles

Uno de los principales controles a tener en cuenta de cara al plan de contingencia y continuidad está relacionado con tener actualizado el plan. De esta forma cuando se modifique uno de los procedimientos habituales de la gestión del centro, se valorará si requiere hacer modificaciones en el plan de contingencia y continuidad.

Además, otro de los controles más importantes está relacionado con la monitorización de la actividad del centro. Así si un incidente se produce en varias ocasiones será conveniente evaluar si es necesario establecer algún tipo de salvaguarda para evitarlo en futuras ocasiones.

ID:	REC01
Nombre Programa:	Gestión de Backup
Detalles	

Salvaguardas aplicadas

AD.2 – Elaboración de catálogo de versiones de productos
RC.1 – Realización de copias de seguridad regulares
RC.2 – Elaborar registro de configuración

Activos afectados

D.1 – Datos de matrícula
D.2 – Expedientes académicos
D.4 – Copias de seguridad
COM.2 – Red WiFi
HW.2 – Ordenadores para alumnado
HW.3 – Ordenadores para profesorado
HW.4 - Chromebook
Media.1 – Discos duros de administración
Media.2 – Memorias USB
Media.3 – Archivadores y carpetas
S.1 – Servicio Web

Costes

Tiempo de implantación:	2 meses (32 horas)
Recursos necesarios:	2 horas de trabajo semanales por parte del personal del departamento de TIC
Coste Total:	Utilizando las horas correspondientes a las horas complementarias de la jornada de los profesores el coste dependerá del salario/hora de los responsables del proyecto

Objetivos

- Implantar un sistema de copias de seguridad organizado de todos los soportes de información que contienen datos relevantes para el centro.
- Elaborar documentación que permita, en caso de incidente, devolver el sistema al estado previo al incidente.
- Elaborar un catálogo de versiones y configuraciones para poder reconfigurar en poco tiempo el hardware del Sistema de Información del colegio.

Descripción

Este programa envolverá todas las actividades necesarias para que, en caso de incidente, podamos recuperar el estado previo del sistema en el menor tiempo posible.

El primer paso para ello es llevar a cabo la gestión de copias de seguridad del centro. Se realizarán copias de seguridad periódicas para aquellos activos que contienen información importante (Que son para los que en el [Anexo I - 5. Evaluación de salvaguardas] se indicó como recomendable esta medida).

Para la realización de las copias de seguridad se empleará la estrategia "3-2-1". Para los archivos importantes se almacenarán 3 copias: la original y dos copias de seguridad. Estas dos copias de seguridad estarán en formatos de almacenamiento distintos (Discos duros, cintas magnéticas, almacenamiento en la nube…). Y finalmente, no debe haber dos copias de seguridad almacenadas en el mismo lugar, lo ideal es que haya una copia de seguridad fuera del colegio (O bien físicamente en otro lugar, o bien en la nube) y en caso de no ser posible, la segunda copia de seguridad deberá estar en otro edificio del colegio.

Como últimas valoraciones con respecto a las copias de seguridad estas se realizarán periódicamente en función de los datos que se estén manejando (Los discos duros de administración pueden hacer copias de seguridad incrementales cada varias horas, y del servidor web se puede hacer una copia de seguridad completa mensualmente fuera del horario laboral). Además, estas copias de seguridad deberán ser revisadas de forma periódica para asegurar el correcto funcionamiento de estas.

Por otro lado, además de las copias de seguridad se llevará a cabo un registro de los productos software utilizados en los dispositivos del centro donde se indicará el dispositivo que incorpora el producto, el nombre del producto y su versión.

Finalmente se realizará también un registro de configuración con las diferentes opciones de configuración de los diferentes elemento hardware y software del colegio para que, en caso de avería y que haya que reinstalar uno de estos dispositivos se pueda reconfigurar de la misma forma que estaba antes del incidente.

Controles

En lo referente a la gestión de las copias de seguridad periódicamente se deberá hacer el volcado de las copias de seguridad para verificar que pueden restaurarse. Este proceso puede

hacerse una vez al mes para las copias de seguridad que se hagan diariamente o una vez al trimestre para las copias que se hagan mensualmente.

Al final de cada curso se eliminarán de forma segura las copias de seguridad que no sean necesarias y se conservarán las que, bien por ley bien para la propia gestión del colegio, tengan que mantenerse.

ID:	PRE01
Nombre Programa:	Control de acceso lógico
Detalles	

Salvaguardas aplicadas

PR.3 – Control de acceso lógico
PR.4 – Implementar directivas de contraseña segura
IM.1 – Cifrado de equipos hardware

Activos afectados

D.1 – Datos de matrícula
D.2 – Expedientes académicos
D.4 – Copias de seguridad
COM.2 – Red WiFi
HW.2 – Ordenadores para alumnado
HW.3 – Ordenadores para profesorado
Media.2 – Memorias USB
SW.1 - Alexia
SW.2 - Itaca

Costes

Tiempo de implantación:	3 meses (48 horas)
Recursos necesarios:	2 horas de trabajo semanales por parte del personal del departamento de TIC
Coste Total:	Utilizando las horas correspondientes a las horas complementarias de la jornada de los profesores el coste dependerá del salario/hora de los responsables del proyecto

Objetivos

- Establecer mecanismos de control lógico para proteger el acceso a información sensible.
- Implantar en el colegio, una política de contraseñas seguras para proteger los datos de las plataformas informatizadas.

Descripción

Con la realización de este programa se establecerán controles de acceso lógico para los diferentes dispositivos que almacenan información vulnerable o que ofrecen un servicio como pueden ser los ordenadores del profesorado, el ordenador de administración, la red WiFi, memorias USB…

El objetivo es que una persona no autorizada que tenga acceso físico a un dispositivo no pueda acceder a la información que este contiene o impedir en la medida de lo posible que se pueda acceder a los dispositivos del colegio a través de la red.

Para conseguir esto todos los dispositivos físicos que almacenen información deberán tener un control de acceso a partir de usuario y/o contraseña, de esta forma se puede evitar que una persona no autorizada acceda a información que no debería y además queda constancia de que usuarios han accedido a esos dispositivos.

En lo referente a dispositivos de almacenamiento portables, como pueden ser discos duros externos o memorias USB es importante que, si contienen información sensible, estén cifrados y protegidos también por contraseña.

Además, para la gestión de este acceso lógico se implementará una política de contraseñas seguras para el personal del centro que incluya detalles sobre cómo debe ser una contraseña segura, cada cuanto ha de cambiarse una contraseña, como debe almacenarse una contraseña…

Para los servicios proporcionados por el centro (Como el acceso a ordenadores del colegio, plataforma de Alexia, correo corporativo…) estás contraseñas serán proporcionadas por el administrador del servicio.

Controles

Además de evitar que personal no autorizado acceda a los recursos del sistema es importante monitorizar el acceso a estos recursos. De esta forma, el control de acceso lógico debe dejar constancia de que usuarios acceden a que recursos para luego valorar si se ha producido algún incidente y poder tomar medidas al respecto.

ID:	PRE02
Nombre Programa:	Gestión de la seguridad del hardware
Detalles	

Salvaguardas aplicadas

IM.1 – Cifrado de información de los dispositivos hardware
IM.2 – Instalación de equipo contra corte eléctrico
PR.2 – Implantar mecanismos de control de acceso físico
PR.7 – Formateo periódico de los datos almacenados en dispositivos electrónicos

Activos afectados

D.1 – Datos de matrícula
D.2 – Expedientes académicos
D.4 – Copias de seguridad
HW.2 – Ordenadores para alumnado
HW.3 – Ordenadores para profesorado
HW.4 - Chromebook
Media.1 – Discos duros de administración
Media.2 – Memorias USB
Media.3 – Archivadores y carpetas

Costes

Tiempo de implantación:	3 meses (48 horas)
Recursos necesarios:	2 horas de trabajo semanales por parte del personal del departamento de TIC Dispositivo SAI, regletas con protección contra sobretensión y material para el control de acceso físico
Coste Total:	Utilizando las horas correspondientes a las horas complementarias de la jornada de los profesores el coste dependerá del salario/hora de los responsables del proyecto 500€ en material

Objetivos

- Instalación de los mecanismos necesarios para asegurar la integridad física de los activos físicos del colegio.
- Instalación de mecanismos físicos para evitar fugas de información.
- Instalación de equipo contra cortes y sobrecargas eléctricas.

Descripción

El objetivo de este programa es asegurar físicamente los activos hardware del colegio a través de medidas que impidan que personas no autorizadas tengan acceso a ellos, que sufran daños por diferentes incidencias, o que permitan fugas de información.

La primera etapa de este programa consiste en la instalación de mecanismos de control de seguridad físicos para elementos importantes del Sistema de Información del centro como, por ejemplo: instalar cables de seguridad para los ordenadores de las aulas de informática, guardar los elementos de red como switches o módems en armarios de seguridad, almacenar material impreso con datos personales bajo llave…

La segunda etapa consiste en instalar equipamiento que permita, que en caso de corte de luz o de sobrecarga eléctrica no se dañen los equipos informáticos del centro. Para los equipos más importantes y que requieren dar servicio de forma constante, como los ordenadores de administración, se instalará un Sistema de Alimentación Ininterrumpida que dará soporte eléctrico durante un tiempo limitado a los ordenadores. Además, para las aulas de informática donde hay un gran número de equipos se instalarán regletas con protección contra sobrecargas eléctricas para evitar que uno de estos incidentes dañe los ordenadores.

Por último, para eliminar riesgos innecesarios, periódicamente se realizarán formateos de los equipos informáticos del centro. De esta forma, la información necesaria se guardará en diferentes plataformas y la información que se va almacenando de forma residual en los ordenadores se elimine.

Controles

Periódicamente se hará una revisión del estado de los mecanismos instalados según este programa para hacer un mantenimiento en caso de que fuera necesario y evitar averías.

Además, se creará un histórico de los incidentes que afecten a los elementos físicos del sistema de información del colegio. De esta forma se podrá tener un control sobre la efectividad y la necesidad de estas prácticas.

ID:	PRE03
Nombre Programa:	Gestión de la seguridad en Internet
Detalles	

Salvaguardas aplicadas

EL.1 – Implantar mecanismos para capar servicios en la red
IM.3 – Gestión de los antivirus en los equipos informáticos del centro
PR.1 – Usuario, contraseña y certificados para las conexiones inalámbricas

Activos afectados

D.1 – Datos de matrícula
D.2 – Expedientes académicos
COM.2 – Red WiFi
HW.2 – Ordenadores para alumnado
HW.3 – Ordenadores para profesorado
SW.1 – Alexia
SW.2 - Itaca

Costes

Tiempo de implantación:	2 meses (48 horas)
Recursos necesarios:	3 horas de trabajo semanales por parte del personal del departamento de TIC
Coste Total:	Utilizando las horas correspondientes a las horas complementarias de la jornada de los profesores el coste dependerá del salario/hora de los responsables del proyecto

Objetivos

- Minimizar el riesgo al que está expuesto el sistema del centro ante ataques por Internet.
- Evitar que los alumnos del colegio hagan un mal uso del acceso a Internet.

Descripción

Este programa de seguridad está enfocado en dos aspectos diferentes. En primer lugar, defender el sistema de información del colegio de posibles incidentes causados desde el exterior de la red del colegio, y en segundo lugar controlar el acceso a internet desde el centro.

Con respecto a lo primero es importante realizar una configuración segura de la red WiFi. Para ello se modificará periódicamente la clave de la red WiFi, se ocultará el SSID de la empresa para que no sea visible, se asegurará con el uso de cifrado WPA/WPA2… Además de esto, se llevará a cabo la creación de una política antimalware. En esta se trabajarán

cuestiones como la protección antivirus de los ordenadores del colegio, la creación de diferentes perfiles con diferentes permisos en los ordenadores que utilizan los alumnos o definir una política de actualización del software del centro

Por otro lado, enfocado a la cuestión de controlar que hacen los alumnos con su conexión a internet, la conexión de los ordenadores del alumnado se pasará por un servidor proxy. El objetivo de este servidor proxy es evitar que los alumnos puedan acceder a direcciones web que no sean adecuadas o a servicios no relacionados con el ámbito educativo. Además, en los ordenadores de los alumnos se instalará un software de monitorización para realizar un seguimiento de lo que hacen los alumnos con los ordenadores del centro.

Controles

Se creará un histórico de incidencias relacionadas con ataques y virus para analizar si existe alguna vulnerabilidad del sistema de información.

Además, se configurará el servidor proxy para dejar constancia de los movimientos en la red de los diferentes ordenadores del alumnado.

8. Plan de seguridad

Definidos los programas de seguridad es necesario organizarlos en un plan de seguridad también llamado plan director.

Un plan director se centra, generalmente, en un plazo de tiempo de unos 2 o 3 años y define los programas de seguridad y las medidas a tomar en ese plazo, en este caso se establecerá un plan de seguridad a dos años vista. El objetivo es definir en esos 2 años como se van a organizar los programas de seguridad propuestos en el apartado anterior. Para ello se tendrá en cuenta la duración y el coste de los programas, la urgencia de implantación (Teniendo en cuenta si el riesgo que buscan mitigar es más o menos crítico), la capacidad del personal…

Teniendo en cuenta que el centro no cuenta con personal específico para implantar estos programas, se ha estructurado el plan de seguridad de forma que no se trabaje en la implantación de dos programas de forma paralela para intentar reducir el esfuerzo realizado por el profesorado.

Se ha estructurado el plan de seguridad de forma que los primeros proyectos estén enfocados a los activos con mayor riesgo y posponiendo los programas con mayor coste para que el centro tenga capacidad para ahorrar ese dinero.

Así, el plan director estructura los proyectos a realizar en los próximos 2 años de la siguiente forma:

1er año (2020):

- DOC02 - Creación de políticas TI
- REC01 - Gestión de Backup
- PRE01 - Control de acceso lógico
- PRE03 - Gestión de la seguridad en Internet

2º año (2020):

- DOC01 - Formalizar procedimientos
- DOC03 - Crear plan de contingencia
- PRE02 - Gestión de la seguridad hardware

A continuación, se adjunta un cronograma donde se establecen los periodos de trabajo planificados para la realización de los diferentes programas del plan de seguridad.

		Curso 2019/2020												Curso 2020/2021											
Programas de seguridad	Tiempo	S	O	N	D	E	F	M	A	M	J	J	A	S	O	N	D	E	F	M	A	M	J	J	A
DOC01 - Formalizar procedimientos	4 meses																								
DOC02 - Creación de políticas TI	4 meses																								
DOC03 - Crear plan de contingencia	4 meses																								
REC01 - Gestión de Backup	2 meses																								
PRE01 - Control de acceso lógico	3 meses																								
PRE02 - Gestión de la seguridad Hardware	3 meses																								
PRE03 – Gestión de la seguridad en Internet	3 meses																								

Tabla 3. Cronograma del plan de seguridad

9. Estado final del SGSI

Con el objetivo de valorar como de seguro será el Sistema de Información del centro después de realizar este plan de seguridad, se va a evaluar el estado del SGSI como ya se hizo en el apartado [4.3 Estado inicial del Sistema de Información].

El objetivo es, a través de un análisis formal y siguiendo las métricas propuestas por la normativa ISO 27000 valorar el grado de implantación del SGSI y valorar como ha cambiado con respecto al estado inicial. A continuación, se adjuntan los resultados de este análisis.

Valoración	Descripción
L0 – No implementado	No se lleva a cabo el control de seguridad en los sistemas de información.
L1 – Inicial / Ad-hoc	Procedimientos existentes, pero sin un proceso formal definido. Su éxito depende de esfuerzos personales.
L2 – Reproducible pero intuitivo	Existe un método de trabajo, pero sin comunicación formal, depende del conocimiento del propio individuo y no hay formación del personal.
L3 – Proceso definido	El proceso se lleva a cabo conforme a la documentación especificada que ha sido administrada por la organización.
L4 – Gestionado y medible	Se puede realizar un seguimiento de la evolución del proceso a través de datos estadísticos.
L5 – Optimizado	Los procesos están implementados según un procedimiento documentado que es medido periódicamente y están en constante mejora
N/A – No Aplica	O bien es un aspecto que no tiene cabida dentro del contexto de la organización o bien su gestión es externa a la propia organización.

Tabla 4. Leyenda para la evaluación final del SGSI

Estado final del SGSI	
4. Contexto de la organización	
4.1 Comprensión de la organización y de su contexto	L3 – Proceso definido
oc4.2 Comprensión de las necesidades y expectativas de las partes interesadas	L2 – Reproducible pero intuitivo
4.3 Determinación del alcance del SGSI	L2 – Reproducible pero intuitivo
4.4 Sistema de gestión de la seguridad de la información	L3 – Proceso definido
5. Liderazgo	
5.1 Liderazgo y compromiso	L1 – Inicial / Ad-hoc
5.2 Política	L3 – Proceso definido
5.3 Roles, responsabilidades y autoridades en la organización	L4 – Gestionado y medible
6. Planificación	
6.1 Acciones para tratar los riesgos y oportunidades	
6.1.1 Consideraciones generales	L4 – Gestionado y medible
6.1.2 Apreciación de riesgos de seguridad de la información	L4 – Gestionado y medible
6.1.3 Tratamiento de los riesgos de la seguridad de la información	L4 – Gestionado y medible
6.2 Objetivos de seguridad y planificación para su consecución	L4 – Gestionado y medible
7. Soporte	
7.1 Recursos	L2 – Reproducible pero intuitivo
7.2 Competencia	L3 – Proceso definido
7.3 Concienciación	L4 – Gestionado y medible
7.4 Comunicación	L4 – Gestionado y medible
7.5 Información documentada	

7.5.1 Consideraciones generales	L4 – Gestionado y medible
7.5.2 Creación y actualización	L4 – Gestionado y medible
7.5.3 Control de la información documentada	L4 – Gestionado y medible
8. Operación	
8.1 Planificación y control operacional	L3 – Proceso definido
8.2 Apreciación de los riesgos de seguridad de la información	L4 – Gestionado y medible
8.3 Tratamiento de los riesgos de seguridad de la información	L3 – Proceso definido
9. Evaluación del desempeño	
9.1 Seguimiento, medición, análisis y evaluación	L3 – Proceso definido
9.2 Auditoría interna	L0 – No implementado
9.3 Revisión por la dirección	L0 – No implementado

Tabla 5. Análisis del estado final según la ISO 27001

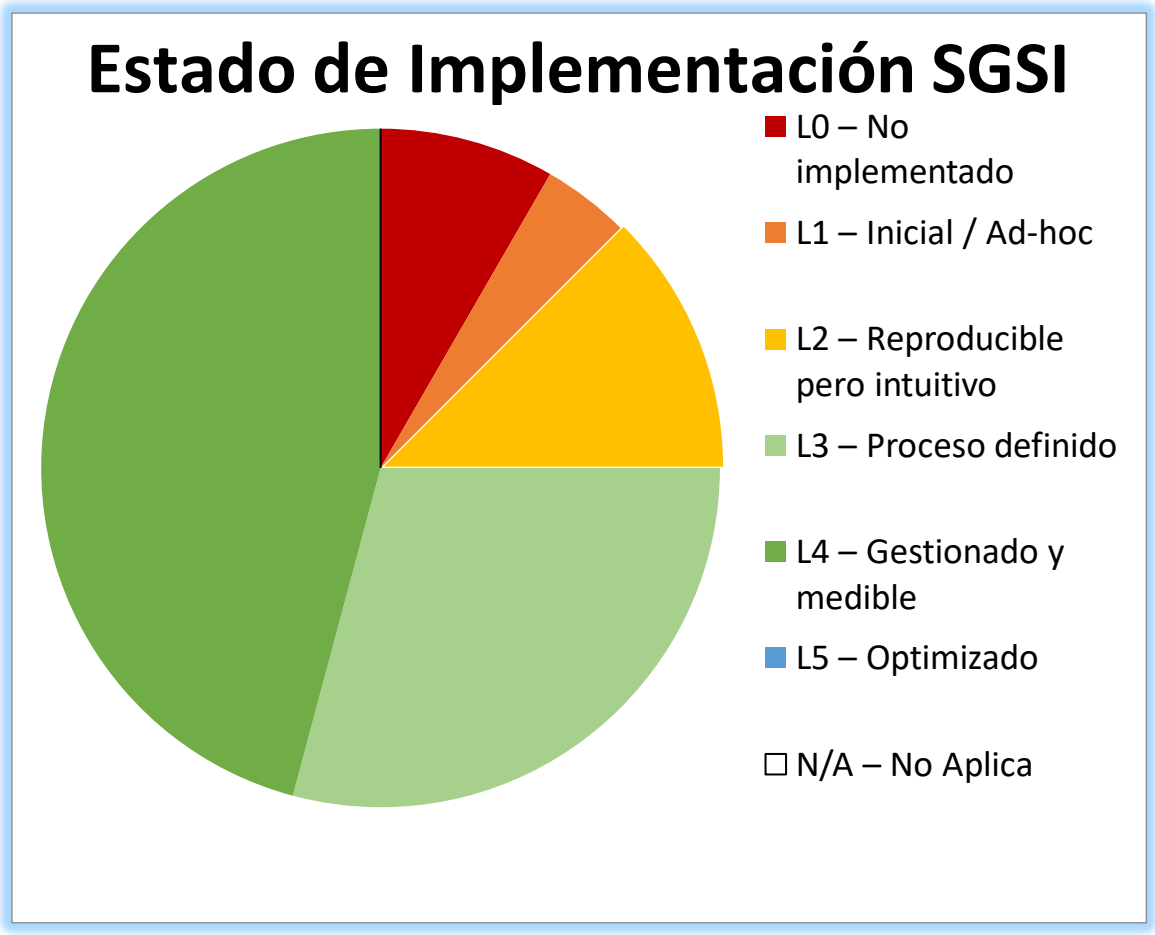

Figura 2. Resumen del estado final según la ISO 27000

Con este gráfico y en comparación al que se realizó previo al estudio del SGSI del centro se pueden observar varias cosas.

En primer lugar, se observa que la mayoría de las cuestiones que antes se definían como “L0 – No implementado” o “L1 – Inicial / Ad-hoc han cambiado. Es lógico que muchas cuestiones, teniendo en cuenta que en el colegio nunca se había realizado ningún proceso para asegurar la información del centro, estuvieran sin implementar o en un estado muy básico, pero a lo largo de este trabajo se han ido realizando.

Por otro lado, se puede observar también que mientras que antes no había ninguna cuestión que superara el nivel “L2 – Proceso definido” ahora muchas tienen nivel “L4 – Gestionado y medible”. Esta cuestión se debe a que los niveles superiores a L2 requieren que haya una documentación que defina como se ha realizado el proceso. En el colegio no había suficiente documentación que definiera los procesos de gestión interna del centro y por ello se ha hecho mucho énfasis en los programas de seguridad para que se definan estos procesos en diferentes documentos.

Por último, valorando como quedaría el estado del SGSI después de aplicar el plan de seguridad propuesto, no habría ninguna cuestión que llegara al nivel “L5 – Optimizado”. Para llegar a este nivel es necesario no solo tener un proceso definido, organizado y con indicadores que midan su efectividad, sino que se tiene que llevar a cabo un proceso continuo de mejora de estos planes. En este trabajo no se han abordado ese tipo de medidas, sino que se ha centrado en cosas más concretas y sencillas para que pudiera abordar el personal del centro para mejorar en la medida de lo posible la seguridad de la información del colegio.