Universidad Oberta de Catalunya

Trabajo de Final de Máster

MISTIC

Plan de Implementación de la ISO/IEC 27001:2013

Conecta Bus S.L – Junio 2019

Alumno:
Juan Carlos Najar Rangel

Colaborador Docente:
Antonio José Segovia Henares

Tabla de contenido

Tabla de ilustraciones

Índice de Tablas

0. Definición

0.1. Resumen

La constante evolución tecnológica en la que se encuentra la sociedad ha traído innovaciones en tecnología que han sustituido por completo a las antiguas herramientas análogas, las cuales ya no son los engranajes que mueven a las empresas. Esta evolución ha generado un cambio tanto en todos los modelos de negocio que habíamos conocido, como en la manera de gestionar a las personas.

La digitalización empresarial ha dejado de ser una alternativa para convertirse ya en una obligación si la compañía quiere ser competitiva.

Las nuevas tecnologías han llegado para aumentar las oportunidades de negocio y facilitar el trabajo de las empresas. Sin embargo, a pesar de que la tecnología trae un sinfín de beneficios, no escapa de los riesgos cibernéticos y digitales. Estos riesgos acarrean consecuencias monetarias, pues los ataques son cada vez más sofisticados y recurrentes.

Por eso, es de gran utilidad para las organizaciones la implementación de un SGSI (Sistema de Gestión de Seguridad de la Información) el cual esta fundamentado sobre la norma ISO27001 y establece un proceso sistemático para la protección ante cualquier amenaza que podría llegar a afectar la confidencialidad, integridad o disponibilidad de la información. Este sistema ofrece las mejores practicas y procedimientos que siendo aplicados correctamente en el ámbito empresarial, proporcionan una mejora continua y apropiada para evaluar los riegos a los que nos enfrentarnos diariamente, establecer controles para una mejor protección y defender así nuestro activo mas valioso dentro de la organización, la información.

0.2. Abstract

The constant technological evolution in which society finds itself has brought innovations in technology that have completely replaced the old analogous tools, which are no longer the gears that move companies. This evolution has generated a change in all the business models we had known, as well as in the way people are managed.

Business digitalization is no longer an alternative but an obligation if the company wants to be competitive.

New technologies have come to increase business opportunities and facilitate the work of companies. However, despite the fact that technology brings endless benefits, it does not escape the cyber and digital risks. These risks have monetary consequences, as the attacks are increasingly sophisticated and recurrent.

Therefore, it is very useful for organizations to implement an ISMS (Information Security Management System) which is based on ISO27001 and establishes a systematic process for protection against any threat that could affect the confidentiality, integrity or availability of information. This system offers the best practices and procedures that being applied correctly in the business environment, provide a continuous and appropriate improvement to evaluate the risks we face daily, establish controls for better protection and defend our most valuable asset within the organization, the information.

0.3. Glosario de términos

- **Activo**

Un recurso, procedimiento, sistema u otra cosa que tenga un valor para una organización y por lo tanto deba de ser protegida, los Activos pueden ser bienes físicos tales como equipos de computo y maquinaria, también puede ser la Información y propiedad intelectual.

- **Auditoría**

La verificación independiente de cualquier actividad o proceso.

- **Autenticación**

Procedimiento para comprobar que alguien es quién dice ser cuando accede a un servicio online. Funcionalidad para una comunicación segura.

- **Autorización**

Acción de otorgar el acceso a usuarios, objetos o procesos.

- **Backup**

Copia de seguridad que se realiza sobre la información, con la finalidad de recuperar los datos en el caso de que los sistemas sufran daños o pérdidas accidentales de los datos almacenados.

- **BIA**

Abreviatura de Business Impact Analysis. Se trata de un informe que muestra el costo ocasionado por la interrupción de los procesos críticos de negocio. Permite asignar la criticidad a los procesos de negocio, definir los objetivos de recuperación y determinar un tiempo de recuperación a cada uno de ellos.

- **Bug**

Error o fallo en un programa o sistema de software que desencadena un resultado indeseado.

- **Certificado digital**

Archivo digital generado por una entidad denominada Autoridad Certificadora (CA) que asocia unos datos de identidad a una persona física, organismo o empresa confirmando de esta manera su identidad digital en Internet.

- **Ciberseguridad**

Conjunto de tecnologías, procesos y prácticas diseñados para proteger redes, computadoras, programas y datos de ataques, daños o accesos no autorizados. En un contexto informático, incluye seguridad cibernética y física.

- **Ciclo de Vida de la Seguridad**

Método para iniciar y mantener un plan de seguridad. Consiste en la evaluación del riesgo de la empresa, la planificación de diversas formas de reducir el riesgo de la empresa, la implementación del plan y la supervisión de la actividad comercial para verificar que el plan redujo el riesgo.

- **Cifrado**

Proceso mediante el cual se toma un mensaje en claro, se le aplica una función matemática, y se obtiene un mensaje codificado.

- **Confidencialidad**

Previene del uso no autorizado o revelación de información, asegurándose que la información es accesible únicamente para aquellos que tengan autorizado su uso.

- **Control de acceso**

Limitar el acceso a objetos de acuerdo con los permisos de acceso del sujeto. El control de acceso puede ser definido por el sistema (Control de accesos obligatorio, MAC) o por el propietario del objeto (Control de accesos discrecional, DAC).

- **Criptografía**

La ciencia de cifrar o descifrar información, tal como puede ser un mensaje privado para proteger su confidencialidad, integridad y / o autenticidad.

- **Denegación de servicio (DoS)**

Estrategia de ataque que consiste en saturar de información a la víctima con información inútil para detener los servicios que ofrece.

- **Disponibilidad**

El proceso de asegurar que los sistemas e información sean accesibles para usuarios autorizados cuando ellos lo requieran.

- **Encriptación**

Método de codificar o encriptar datos para evitar que usuarios no autorizados puedan leerlos o alterarlos. Solo los usuarios con acceso a una contraseña o una clave podrán desencriptar y utilizar los datos. Estos datos pueden ser mensajes, archivos, carpetas o discos.

- **Función Hash**

Una función matemática que crea una representación única de un grupo grande de datos. Las funciones Hash son frecuentemente utilizadas en algoritmos criptográficos y para producir resúmenes de mensajes (Checksums and message digest).

- **Integridad**

Garantiza la exactitud y completitud de la información y los métodos de procesamiento.

- **Intrusión**

Violación intencionada de las políticas de seguridad de un sistema.

- **Política de seguridad**

1. Conjunto de estatutos que describen la filosofía de una organización respecto a la protección de su información y sistemas informáticos. 2. Conjunto de reglas que ponen en práctica los requisitos de seguridad del sistema.

- **Privacidad**

Estar libre de accesos no autorizados.

- **Puerta trasera**

Mecanismo que permite a un atacante entrar y controlar un sistema de forma oculta.

- **Riesgo.**

Amenaza que explota una vulnerabilidad que puede causar daño a uno o más activos.

- **Vulnerabilidad**

Es una debilidad o fallo en un sistema de información que pone en riesgo la seguridad de la información pudiendo permitir que un atacante pueda comprometer la integridad, disponibilidad o confidencialidad de esta.

1. Introducción

1.1. Contexto y justificación del trabajo

Conecta Bus S.L es una empresa ficticia que pertenece al sector del transporte de pasajeros. Su sede central está ubicada en Madrid y desde ahí operan para dar respuesta a las solicitudes de sus clientes.

Conecta Bus S.L siempre ha sido una empresa familiar y desde el año 2008 se encuentra regentada por el hijo del fundador. El nuevo gerente trae muchas ideas renovadas y en un intento de potenciar el negocio, ha sumergido a la compañía en un proceso de digitalización. La dirección de la compañía es consciente de la necesidad de invertir en materia de seguridad de la información para que este proceso de digitalización sea exitoso.

Por este único motivo nace este proyecto, que consiste en la realización de un Plan Director que siente las bases para la correcta implementación de un Sistema de Gestión de Seguridad de la Información. La compañía pretende con este proyecto mejorar el grado de madurez de la compañía en seguridad de la información y establecer los proyectos a ejecutar en los próximos años. La compañía también espera conseguir una inversión inteligente y optimizada en seguridad de la información.

Este proyecto se apoya en el uso de la norma ISO27000 para la implementación del SGSI (Sistema de Gestión de Seguridad de la Información) y la metodología MAGERIT para la realización del análisis de riesgos de la compañía.

1.2. Objetivos del trabajo

Concienciados con la importancia de implementar todos los mecanismos de seguridad posibles para mejorar el grado de madurez en materia de seguridad de la información, Conecta Bus precisa:

- Implementar un Sistema de Gestión de Seguridad de la Información certificado, que permita brindar a sus clientes confianza por el tratamiento de los datos que la empresa gestiona, cumpliendo con la legislación nacional e internacional vigente para la transferencia de datos.
- Garantizar la implementación de controles eficientes que protejan la información reduciendo los riesgos a los que está sometida la empresa a unos niveles aceptables.
- Proteger la información de los clientes.

1.3. Metodología

Este trabajo se apoya en las normas internacionales ISO/IEC 27001, con el apoyo de los controles de la ISO/IEC 27002.

La metodología seguida, ha sido la división por fases que está basada en el Ciclo de Deming o ciclo PDCA (del inglés Plan-Do-Check-Act). Es una estrategia de mejora continua muy utilizada en los SGSI. Los resultados de la implementación del Ciclo de Deming permiten a las organizaciones una mejora integral en competitividad, calidad, productividad, etc. reduciendo los costes.

Para la parte correspondiente al análisis de riesgos, se ha utilizado la metodología MAGERIT de análisis de riesgos.

1.4. Planificación y entregables

Las fases en las que se ha dividido el trabajo son las siguientes:

- FASE 1: Situación actual: contextualización, objetivos y análisis diferencial
- FASE 2: Sistema de gestión documental
- FASE 3: Análisis de riesgos
- FASE 4: Propuesta de proyectos
- FASE 5: Auditoría de cumplimiento de la ISO/IEC 27002:2013

- FASE 6: Presentación de resultados y entrega de informes.

Como output del proyecto se han generado los siguientes entregables:

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

2. Situación actual: Contextualización, Objetivos y Análisis Diferencial

2.1. Introducción

El Plan Director de Seguridad es uno de los elementos clave con que debe trabajar el Responsable de Seguridad de una organización. Este plan constituye la hoja de ruta que debe seguir la empresa para gestionar de una forma adecuada la seguridad, permitiendo no sólo conocer el estado de esta, sino en qué líneas se debe actuar para mejorarla. Estamos hablando por tanto de un modelo de mejora continua PDCA (Plan-Do-Check-Act).

El marco legal ha reflejado la importancia de la seguridad de la información (a nivel del estado español, leyes como la 11/2007 artículo 42: "Esquema Nacional de Interoperabilidad y Esquema Nacional de Seguridad", lo demuestran) . La seguridad no es por tanto un aspecto opcional, sino que debe ser inherente a las actividades de la propia empresa, y constituye un punto de partida ineludible para toda organización en la actualidad.

El planteamiento del proyecto será, por tanto, sentar las bases de un Plan de Director de Seguridad para la empresa. Simplificando, y como iremos viendo, nuestro proceso será el siguiente:

- Analizar y detallar nuestro inventario de activos.
- Estudiar las amenazas a las que están expuestos.
- Estudiar el impacto potencial de dichas amenazas.
- Proponer un plan de acción para luchar contra dichas amenazas.
- Evaluar el impacto residual una vez aplicado el plan de acción.

Intencionadamente, la lista anterior no contempla aspectos organizativos, que aún así, tocaremos a lo largo del presente proyecto.

2.2. Conociendo la ISO/IEC 27001

La norma **ISO 27001** es un estándar para la seguridad de la información (*Information technology - Security techniques - Information security management systems - Requirements*) aprobado y publicado como estándar internacional en octubre de 2005 por International Organization for Standardization y por la comisión International Electrotechnical Commission.

Especifica los requisitos necesarios para establecer, implantar, mantener y mejorar un sistema de gestión de la seguridad de la información (SGSI) según el conocido como "Ciclo de Deming": PDCA - acrónimo de **P**lan, **D**o, **C**heck, **A**ct (Planificar, Hacer, Verificar, Actuar). Es consistente con las mejores prácticas descritas en ISO/IEC 27002, anteriormente conocida como ISO/IEC 17799, con orígenes en la norma BS 7799-2:2002, desarrollada por la entidad de normalización británica, la British Standards Institution (BSI).

Se debe señalar que la única norma a certificar de la serie es la ISO 27001. No así la ISO 27002, que, como hemos comentado, tan sólo establece una serie de recomendaciones y buenas prácticas.

Por último, es importante recordar las principales ventajas que una certificación como la ISO 27001 puede aportar a las organizaciones que decidan abordarla:

- Establece un marco de gestión de la seguridad consistente e internacionalmente reconocido.
- Se garantizan los controles internos, los controles de requisitos de gestión corporativa y de continuidad de la actividad de negocio.
- Se demuestra el cumplimiento de leyes y normativas que se apliquen a la organización.
- Ofrece interesantes ventajas competitivas al mostrar a los clientes que la seguridad de su información es primordial, promoviendo a su vez la confianza en las relaciones con terceros.
- Reduce los riesgos estableciendo un marco de gestión de la seguridad.
- Demuestra el compromiso de la cúpula directiva de la organización con la seguridad de la información.

2.3. Conociendo la ISO/IEC 27002

ISO/IEC 27002 (anteriormente denominada ISO 17799) es un estándar para la seguridad de la información publicado por la Organización Internacional de

Normalización y la Comisión Electrotécnica Internacional. Su versión más reciente fue publicada en el año 2013.

ISO 27002 consiste en una guía de buenas prácticas que permiten a las organizaciones mejorar la seguridad de su información. Con este fin, define una serie de objetivos de control y gestión que deberían ser perseguidos por las organizaciones. Estos objetivos, se hallan distribuidos en diferentes dominios que abarcan de una forma integral todos los aspectos que han de ser tenidos en cuenta por las organizaciones.

Los dominios que estructura la ISO 27002 son:

1. Políticas
2. Organización
3. Recursos Humanos
4. Activos
5. Accesos
6. Cifrado
7. Fisica y ambiental
8. Operativas
9. Telecomunicaciones
10. Adq., Des. y Mantto
11. Proveedores
12. Incidentes
13. Continuidad de negocio
14. Cumplimiento

2.4. Contextualización de la empresa

Conecta Bus S.L es una empresa de autobuses dedicada al transporte de viajeros a nivel nacional. Desde su fundación en 1984 la empresa ha ido creciendo año tras año hasta lograr convertirse en todo un referente en el sector.

En el año 2008, el hijo del fundador se hizo cargo de la empresa y desde entonces, Conecta Bus se ha visto sumergida en un proceso de digitalización completo. En este proceso de digitalización, se han incorporado nuevas tecnologías que han elevado el rendimiento y facturación de la empresa notablemente.

Actualmente la compañía, concienciada con la importancia de la seguridad de la información, se enfrenta al desafío de implementar una metodología que permita la implementación de un Sistema de Gestión de Seguridad de la Información, que

provea los niveles de seguridad requeridos, y que garantice la confianza necesaria a la misma entidad, a sus directivos y a sus clientes

La descripción de la empresa a alto nivel es:

- Dispone de una única sede, situada en Madrid.
- La plantilla de la empresa está formada actualmente por 72 profesionales.
- Dispone de un CPD en la oficina donde se encuentran todas las comunicaciones.
- Dispone de una aplicación web desde donde los clientes realizan las contrataciones.
- Dispone de un servicio de atención al usuario para resolver incidencias relativas a la aplicación web.

La actividad económica de la empresa se rige al transporte de viajeros, mediante servicios como:

- Viajes por el territorio español.
- Servicios discrecionales.
- Rutas escolares.
- Excursiones de grupo.
- Rutas profesionales.
- Bodas y bautizos.

Anteriormente todas las contrataciones se realizaban únicamente por teléfono, pero desde el cambio de gerencia se implementó una aplicación web donde los clientes habituales pueden registrarse y realizar la contratación del autobús con muchas ventajas. La contratación por telefonía móvil o email también se sigue realizando para nuevos clientes.

Con la nueva aplicación, además, se ha incorporado un sistema de atención a los usuarios para resolver las dudas o problemas que surjan a los clientes con el uso de la aplicación.

2.5. Alcance del SGSI

La propuesta de alcance para el SGSI, para el desarrollo del plan director de seguridad y como propuesta para la futura certificación ISO/IEC 27001:2013 es la siguiente:

"La gestión de la seguridad de la información en todas las actividades relacionadas con la aplicación web que los clientes usan para la contratación de los servicios de la empresa, y el soporte telefónico de atención al cliente de la empresa."

No se contempla dentro del presente alcance la obtención de la certificación de la norma.

2.6. Organigrama

Conecta Bus ha sido siempre una empresa familiar y su organigrama es bastante sencillo. Los distintos departamentos que forman la empresa están definidos tal y como se puede apreciar en la siguiente ilustración:

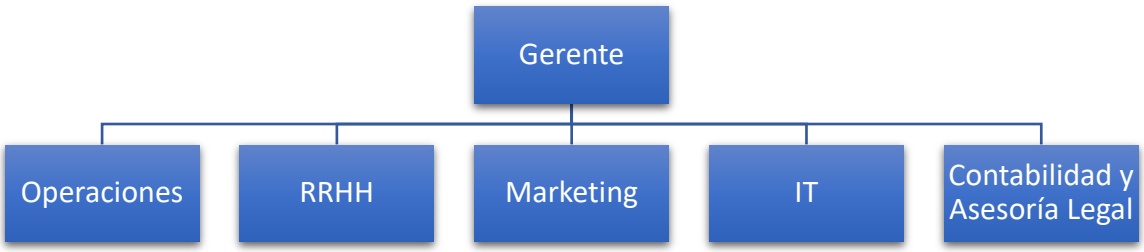

Ilustración 1: Organigrama general de Conecta Bus.

El **Gerente** es el encargado de tomar las decisiones que afectan a toda la empresa y realiza tareas de coordinación para que los distintos departamentos trabajen entre sí.

Cada departamento a su vez, esta constituido por un jefe de departamento y por personal cualificado que realizan los trabajos propios del departamento.

Para hacer referencia al alcance del proyecto nos centraremos en el departamento de IT, el cuál esta constituido como se muestra en la ilustración siguiente:

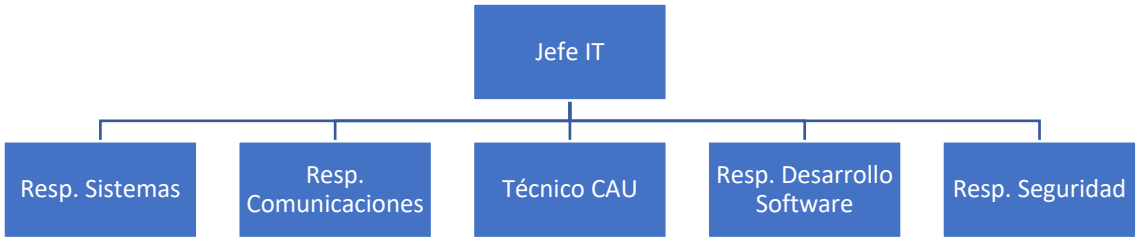

Ilustración 2: Organigrama Departamento IT.

El **Coordinador** es el responsable del departamento y el encargado de hacer funcionar las distintas áreas.

El **Resp. de Sistemas** es el encargado de los sistemas y aplicaciones de los que dispone la empresa.

El **Resp. de Comunicaciones** se encarga de las comunicaciones de la empresa.

El **Técnico CAU** se encarga de dar soporte a los usuarios a través de la telefonía. Recoge todas las incidencias que tienen los usuarios con la aplicación web de la empresa.

El **Resp. de Desarrollo** se encarga de implementar las actualizaciones de las distintas aplicaciones que usa la empresa y que son de creación propia. Entre ellas se encuentra la aplicación web de los clientes.

El **Resp. de Seguridad** es la figura encargada de la seguridad de la información, aunque debido a que no existe un responsable o área encargada de la seguridad física, la mayoría de las responsabilidades de esta área recaen también sobre él.

2.7. Infraestructura de Red

Conecta Bus dispone de un CPD situado en la oficina central. El CPD es controlado y gestionado por el departamento de IT. La arquitectura lógica de la red de la compañía muestra un esquema como el siguiente:

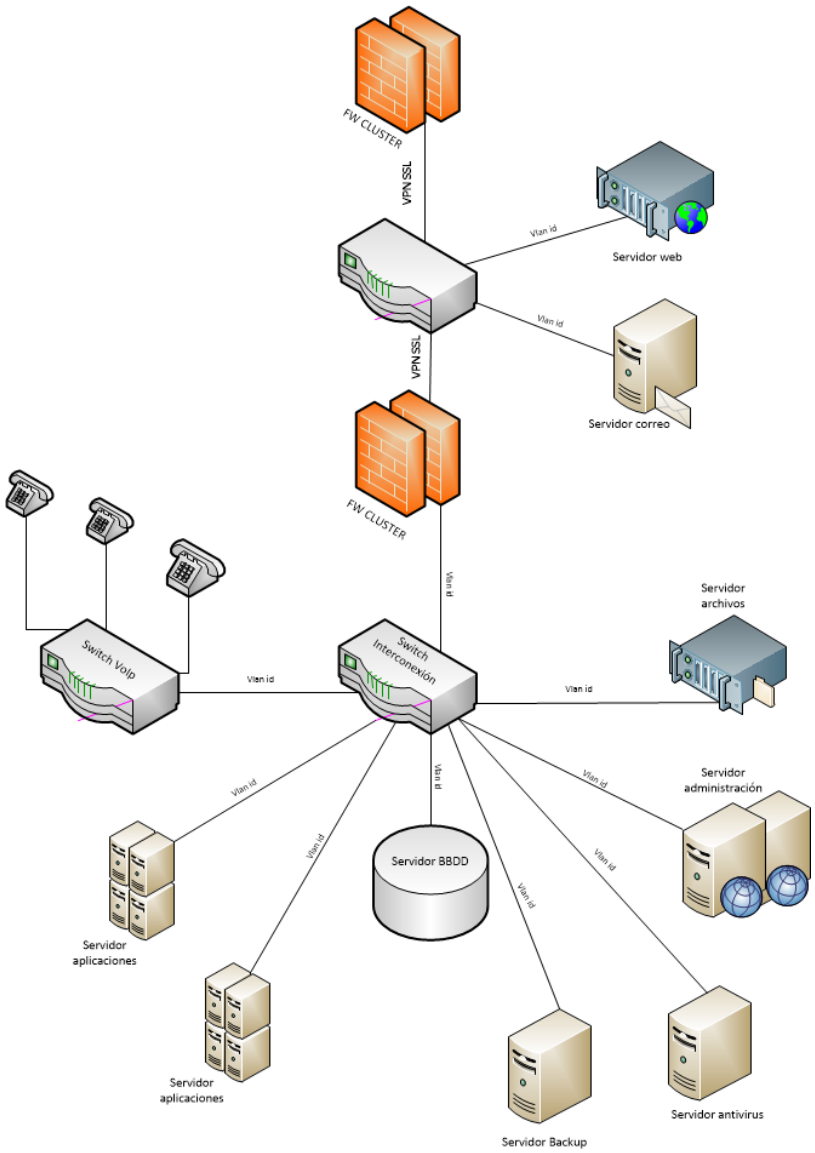

Ilustración 3: Arquitectura lógica de los sistemas y redes de Conecta Bus.

Como se puede apreciar, la red se encuentra segmentada formando una red interna y una red perimetral DMZ. Como dispositivos de seguridad dispone de 4

firewall que delimitan la red DMZ donde se encuentra el servidor web y el antiguo servidor de correo electrónico (algunas cuentas aún no se han migrado a la nube).

La red interna está dividida en VLAN´s para separar los servidores de la compañía de la red donde se conectan los teléfonos de voz IP.

2.8. Análisis Diferencial

Con el objetivo de conocer el grado de madurez actual en materia de seguridad de la empresa, se hace necesario realizar un análisis diferencial con respecto a los estándar ISO27001:2013 e ISO27002:2013. Esta actividad se realiza estudiando de forma individual cada uno de los controles de ambos documentos y calificando el grado de cumplimiento según lo establecido en la tabla 1:

Nivel	Madurez	Cumplimiento
L0	Inexistente: Carencia completa de cualquier proceso reconocible. No se ha reconocido siquiera que existe un problema a resolver	No cumple
L1	Inicial: Estado inicial donde el éxito de las actividades de los procesos se basa la mayoría de las veces en el esfuerzo personal. Los procedimientos son inexistentes o localizados en áreas concretas. No existen plantillas definidas a nivel corporativo.	Parcial
L2	Reproducible pero intuitivo: Los procesos similares se llevan en forma similar por diferentes personas con la misma tarea. Se normalizan las buenas prácticas en base a la experiencia y al método. No hay comunicación o entrenamiento formal, las responsabilidades quedan a cargo de cada individuo. Se depende del grado de conocimiento de cada individuo.	Parcial
L3	Proceso definido: La organización entera participa en el proceso. Los procesos están implantados, documentados y comunicados mediante entrenamiento.	Cumple
L4	Gestionable y medible: Se puede seguir con indicadores numéricos y estadísticos la evolución de los procesos. Se dispone de tecnología	Cumple

	para automatizar el flujo de trabajo, se tienen herramientas para mejorar la calidad y la eficiencia.	
L5	Optimizado: Los procesos están bajo constante mejora. En base a criterios cuantitativos se determinan las desviaciones más comunes y se optimizan los procesos.	Cumple

Tabla 1: Escala nivel de madurez

En el **Anexo I** y **Anexo II** se encuentra el resultado del análisis diferencial realizado a la compañía con respecto a la norma ISO 27001 y a la normal ISO 27002 respectivamente.

2.9. Resultado

Análisis diferencial – Evaluación Controles ISO27001:2013

Los resultados obtenidos en la evaluación de los controles de la ISO27001:2013 han mostrado un nivel de madurez muy bajo. Esto es debido a que actualmente en la empresa no existe implementado ningún tipo de sistema de gestión y únicamente destaca la implicación e intención de implementar un SGSI por parte de la dirección de la empresa.

Ilustración 4: Porcentaje de cumplimiento de la ISO27001:2013.

Análisis diferencial – Evaluación Controles ISO27002:2013

Tras realizar el estudio de los controles de ISO27002:2013 se han recogido de forma cuantitativa los resultados obtenido para ser mostrados en la siguiente tabla:

DOMINIO	CONTROLES	CUMPLE	% CUMPLE	CUMPLE PARCIAL	% CUMPLE PARCIAL	NO CUMPLE	% NO CUMPLE
5.POLITICAS DE SEGURIDAD DE LA INFORMACIÓN	2	0	0%	0	0,00%	2	100,00%
6.ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	7	0	0%	1	14,29%	6	85,71%
7.SEGURIDAD RELATIVA A LOS RECURSOS HUMANOS	6	1	17%	2	33,33%	3	50,00%
8.GESTIÓN DE ACTIVOS	10	0	0%	4	40,00%	6	60,00%
9.CONTROL DE ACCESO	14	1	7%	8	57,14%	5	35,71%
10.CRIPTOGRAFÍA	2	0	0%	1	50,00%	1	50,00%
11.SEGURIDAD FÍSICA Y DEL ENTORNO	15	2	13%	6	40,00%	7	46,67%
12.SEGURIDAD DE LAS OPERACIONES	14	0	0%	7	50,00%	7	50,00%
13.SEGURIDAD DE LAS COMUNICACIONES	7	1	14%	4	57,14%	2	28,57%
14.ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACION	13	0	0%	5	38,46%	8	61,54%
15.RELACION CON PROVEEDORES	5	0	0%	3	60,00%	2	40,00%
16.GESTION DE INCIDENTES DE SEGURIDAD DE LA INFORMACION	7	0	0%	2	28,57%	5	71,43%

17.ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN PARA LA GESTION DE LA CONTINUIDAD DEL NEGOCIO	4	0	0%	1	25,00%	3	75,00%
18.CUMPLIMIENTO	8	0	0%	2	25,00%	6	75,00%
TOTAL	**114**	**5**	**4,39%**	**46**	**40,35%**	**63**	**55,26%**

Tabla 2: Evaluación controles ISO27002:2013

Como se aprecia, el nivel de madurez con respecto a la norma es bastante bajo, ya que tan solo existe un nivel de cumplimiento del 4,39% del total de los controles que conforman el estándar.

El siguiente gráfico recoge el cumplimiento por dominio de la ISO27002:2013:

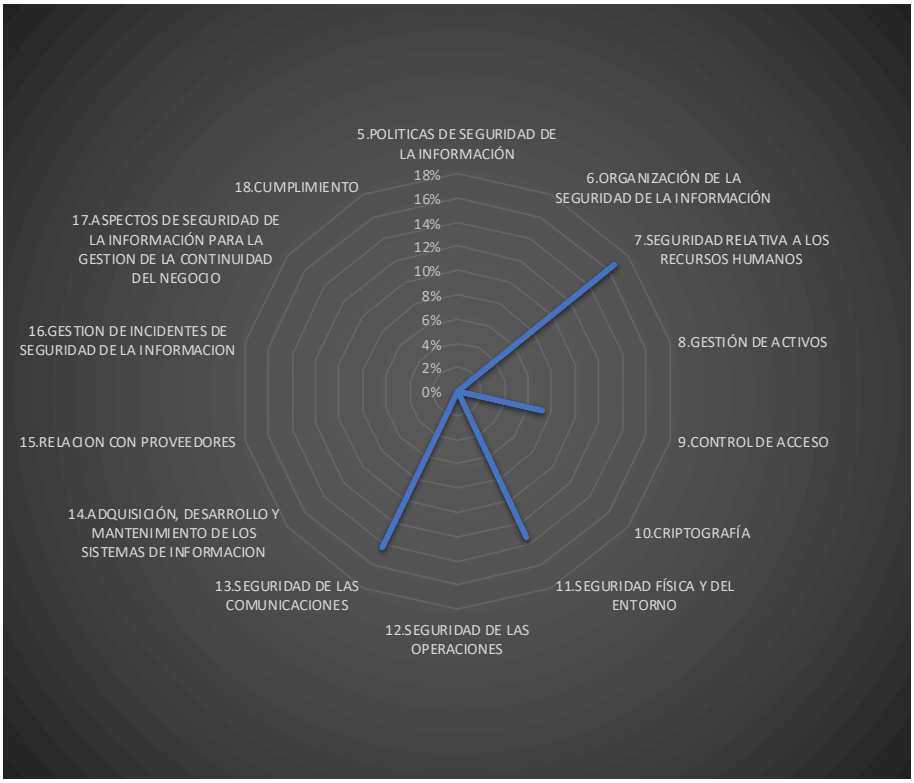

Ilustración 5: Porcentaje cumplimiento ISO27002:2013.

La empresa dispone de un nivel de cumplimiento muy bajo debido a no disponer de un SGSI implementado.

3. Sistema de Gestión Documental

3.1. Introducción

Todos los Sistemas de Gestión se apoyan en un cuerpo documental para el cumplimiento normativo. Esto significa que en nuestro Sistema de Gestión de Seguridad de la Información tendremos que tener una serie de documentos, los cuales vienen establecidos en la propia norma ISO/IEC 27001

3.2. Esquema documental

La propia ISO/IEC 27001 define cuales son los documentos necesarios para poder certificar el sistema. En este trabajo, nosotros nos centraros en los siguientes:

- **Política de Seguridad (Anexo III)**: Normativa interna que debe conocer y cumplir todo el personal afectado por el alcance del Sistema de Gestión de Seguridad de la Información. El contenido de la Política debe cubrir aspectos relativos al acceso de la información, uso de recursos de la Organización, comportamiento en caso de incidentes de seguridad, etc.
- **Procedimiento de Auditorías Internas (Anexo IV)**: Documento que debe incluir una planificación de las auditorías que se llevarán a cabo durante la vigencia de la certificación (una vez se obtenga), requisitos que se establecerán a los auditores internos y se definirá el modelo de informe de auditoría.
- **Gestión de Indicadores (Anexo V)**: Es necesario definir indicadores para medir la eficacia de los controles de seguridad implantados. Igualmente es importante definir la sistemática para medir.
- **Procedimiento Revisión por Dirección (Anexo VI)**: La Dirección de la Organización debe revisar anualmente las cuestiones más importantes que han sucedido en relación con el Sistema de Gestión de Seguridad de la Información. Para esta revisión, la ISO/IEC 27001 define tanto los puntos de entrada, como los puntos de salida que se deben obtener de estas revisiones.
- **Gestión de Roles y Responsabilidades (Anexo VII)**: El Sistema de Gestión de Seguridad de la Información tiene que estar compuesto

por un equipo que se encargue de crear, mantener, supervisar y mejorar el Sistema. Este equipo de trabajo, conocido habitualmente como Comité de Seguridad, debe estar compuesto al menos por una persona de Dirección, para que de esta manera las decisiones que se tomen puedan estar respaldadas por alguien de Dirección.

- **Metodología de Análisis de Riesgos (Anexo VIII)**: Establece la sistemática que se seguirá para calcular el riesgo, lo cual deberá incluir básicamente la identificación y valoración de los activos, amenazas y vulnerabilidades.
- **Declaración de Aplicabilidad (Anexo IX)**: Documento que incluye todos los controles de Seguridad establecidos en la Organización, con el detalle de su aplicabilidad, estado y documentación relacionada.

4. Análisis de Riesgos

4.1. Introducción

Toda empresa que disponga de un Sistema de Gestión de Seguridad de la Información necesita llevar a cabo una adecuada gestión de riesgos que le permita saber cuáles son las principales vulnerabilidades de sus activos de información y cuáles son las amenazas que podrían explotar las vulnerabilidades. Una vez que la empresa tenga clara esta identificación de riesgos podrá establecer las medidas preventivas y correctivas viables que garanticen mayores niveles de seguridad en su información.

Son muchas las metodologías utilizadas para la gestión de riesgos, pero todas parten de un punto común: la identificación de activos de información, es decir todos aquellos recursos involucrados en la gestión de la información, que va desde datos y hardware hasta documentos escritos y el recurso humano. Sobre estos activos de información es que hace la identificación de las amenazas o riesgos y las vulnerabilidades.

Para la realización del análisis de riesgos de este Plan Director nos basaremos en la metodología de MAGERIT. Como ya se ha comentado en apartados anteriores, esta metodología tiene como característica fundamental que los riesgos que se plantean para una organización se expresan en valores económicos directamente, lo que una ventaja y un inconveniente:

El aspecto positivo de esta metodología es que el resultado se expresa en valores económicos. Esto hace que las decisiones que deban tomarse y que tengan que ser validadas por la dirección estarán fundamentadas y serán fácilmente defendibles.

Por el contrario, el hecho detener que traducir de forma directa todas las valoraciones en valores económicos hace que la aplicación de esta metodología sea realmente costosa.

En los siguientes apartados procederemos con las diferentes fases que forman la metodología.

4.2. Identificación de los activos

Esta fase del estudio consiste en identificar cuales son los activos que posee la organización y que necesita para llevar a cabo sus actividades. Para MAGERIT en un sistema de información hay dos elementos esenciales: la información que se maneja y los servicios que se prestan.

Siguiendo la clasificación expuesta en el Libro II de MAGERIT, agruparemos los activos en las siguientes categorías:

- Datos [D]
- Claves Criptográficas [K]
- Servicios [S]
- Software [SW]
- Hardware [HW]
- Redes de Comunicaciones [COM]
- Equipamiento Auxiliar [AUX]
- Instalaciones [L]
- Personal[P]

CATEGORÍA	IDENTIDICADOR	ACTIVO
Datos [D]	[D_XFILE]	Datos departamentales
	[D_BKP]	Copias de seguridad
	[D_BDCL]	Bases de Datos de clientes
	[D_COD]	Código fuente de desarrollos
	[D_LOG]	Logs registros de actividad
	[D_CONF]	Archivos de configuración
Claves Criptográficas [K]	[K_SSL]	Certificado SSL
Servicios [S]	[S_WEB]	Servicio Web
	[S_CAU]	Servicio CAU
	[S_EMAIL]	Correo corporativo
Software [SW]	[SW_SQL]	SQL Server 2013
	[SW_BKP]	Backups Symantec
	[SW_OFI]	OfiBus
	[SW_VIR]	Antivirus Corporativo
	[SW_MS]	MS Office 365
	[SW_WS]	Windows Server 2016
	[SW_W10]	Windows 10
	[SW_PBX]	Astérix PBX
	[SW_GPS]	Localizate (GPS)

Hardware [HW]	[HW_PORT]	Portátiles de trabajo
	[HW_IMP]	Impresoras
	[HW_FW]	Firewalls
	[HW_SWTH]	Switches
	[HW_SERV]	Servidores
	[HW_ALM]	Cabina almacenamiento
	[HW_TELF]	Teléfonos de trabajo
Redes de Comunicaciones [COM]	[COM_TEL]	Red telefónica
	[COM_LAN]	Red LAN interna
	[COM_WIFI]	Red Wifi
	[COM_INTER]	Internet
Equipamiento Auxiliar [AUX]	[AUX_VENT]	Equipo ventilación
	[AUX_CONS]	Consumibles varios
	[AUX_CE]	Corriente eléctrica
	[AUX_ACCCON]	Sistema de alimentación continua
	[AUX_RED]	Cableado de la red
Instalaciones [L]	[L_CPD]	CPD
	[L_OFI]	Oficina
Personal [P]	[P_RRHH]	Resp. de RRHH
	[P_SIST]	Resp. de Sistemas
	[P_COM]	Resp. de Comunicaciones
	[P_CAU]	Técnico CAU
	[P_SW]	Resp. de Desarrollo
	[P_SEG]	Resp. de Seguridad
	[P_CORD]	Coordinador IT

Tabla 3: Inventario de activos.

4.3. Dependencia de los activos

La dependencia entre activos permite identificar las relaciones de dependencia entre los mismos. Los activos que se encuentran en las partes superiores dependen de los activos que se encuentran por debajo de ellos. De esta deducción se puede analizar que el riesgo asociado a un activo puede aumentar según las dependencias que este tenga con otros activos.

La dependencia entre los activos de la compañía atendiendo a la clasificación de MAGERIT es la siguiente:

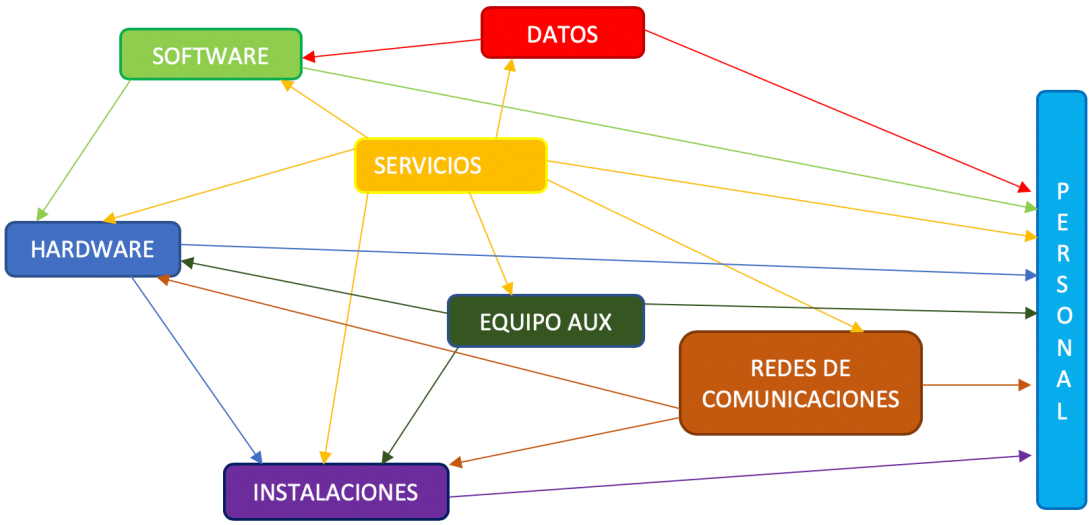

Ilustración 6: Dependencia entre los activos.

4.4. Valoración de los activos

Disponer de una valoración de activos es de suma importancia. Para realizar dicha valoración se toma en consideración tanto las dimensiones en las cuales el activo es relevante, como su estimación de la valoración de cada dimensión.

Las dimensiones para considerar según la metodología MAGERIT son:

- [D] Disponibilidad de los servicios
- [I] Integridad de los datos
- [C] Confidencialidad de los datos
- [A] Autenticidad de la información y los usuarios
- [T] Trazabilidad del uso del servicio y los datos

La anterior clasificación propuesta por MAGERIT atiende a una clasificación cualitativa. Para obtener una valoración completa de los activos, se debe clasificar el valor de los activos de forma cualitativa y cuantitativa.

La siguiente tabla vuestra los criterios de valoración que se han seguido en este proyecto:

Valoración	Valor
Muy alta	9
Alta	7
Media	4
Baja	2
Despreciable	1

Tabla 4: Valor de los activos.

El resultado obtenido se recoge en la siguiente tabla:

				CRITICIDAD				
CATEGORÍA	ACTIVO		VALOR	D	I	C	A	T
Datos [D]	[D_XFILE]	Datos departamentales	MEDIO	3	7	7	7	7
	[D_BKP]	Copias de seguridad	MEDIO	6	8	3	8	8
	[D_BDCL]	Bases de Datos de clientes	MUY ALTO	9	10	9	10	10
	[D_COD]	Código fuente de desarrollos	ALTO	6	9	8	7	6
	[D_LOG]	Logs registros de actividad	MEDIO	5	2	5	1	8
	[D_CONF]	Archivos de configuración	MUY ALTO	9	9	9	9	9
Claves Criptográficas [K]	[K_SSL]	Certificado SSL	MUY ALTO	9	9	9	9	9
Servicios [S]	[S_WEB]	Servicio Web	ALTO	9	9	7	8	7
	[S_CAU]	Servicio CAU	ALTO	7	8	7	7	5
	[S_EMAIL]	Correo corporativo	MEDIO	7	8	7	7	5
Software [SW]	[SW_SQL]	SQL Server 2013	MEDIO	7	7	3	7	7
	[SW_BKP]	Backups Symantec	MEDIO	5	3	3	3	7
	[SW_OFI]	OfiBus	MEDIO	5	5	7	5	4
	[SW_VIR]	Antivirus Corporativo	BAJO	5	3	3	3	4
	[SW_MS]	MS Office 365	BAJO	1	3	3	3	1
	[SW_WS]	Windows Server 2016	ALTO	8	7	7	4	7
	[SW_W10]	Windows 10	BAJO	2	2	2	3	2
	[SW_PBX]	Asterix PBX	ALTO	8	7	7	4	7

	[SW_GPS]	Localizate (GPS)	MEDIO	5	7	3	7	7
Hardware [HW]	[HW_PORT]	Portátiles de trabajo	MEDIO	5	5	5	4	4
	[HW_IMP]	Impresoras	BAJO	3	3	4	3	3
	[HW_FW]	Firewalls	MUY ALTO	9	9	9	9	9
	[HW_SWTH]	Switches	ALTO	7	9	7	7	5
	[HW_SERV]	Servidores	ALTO	9	9	7	8	7
	[HW_ALM]	Cabina almacenamiento	ALTO	7	9	8	7	7
	[HW_TELF]	Teléfonos de trabajo	MEDIO	6	5	4	4	4
Redes de Comunicaciones [COM]	[COM_TEL]	Red telefónica	MEDIO	6	1	3	5	2
	[COM_LAN]	Red LAN interna	ALTO	10	8	10	5	8
	[COM_WIFI]	Red Wifi	ALTO	7	9	7	7	7
	[COM_INTER]	Internet	MUY ALTO	9	9	9	9	9
Equipamiento Auxiliar [AUX]	[AUX_VENT]	Equipo ventilación	MUY ALTO	9				
	[AUX_CONS]	Consumibles varios	BAJO	3				
	[AUX_CE]	Corriente eléctrica	MUY ALTO	9				
	[AUX_ACCCON]	Sistema de alimentación continua	ALTO	7	7	7	7	
	[AUX_RED]	Cableado de la red	MUY ALTO	9				
Instalaciones [L]	[L_CPD]	CPD	ALTO	10	10	8	9	7
	[L_OFI]	Oficina	MEDIO	5	3	5	7	2
Personal [P]	[P_RRHH]	Resp. de RRHH	MEDIO	6				
	[P_SIST]	Resp. de Sistemas	MUY ALTO	9				
	[P_COM]	Resp. de Comunicaciones	MUY ALTO	9				
	[P_CAU]	Técnico CAU	ALTO	7				
	[P_SW]	Resp. de Desarrollo	MEDIO	4				
	[P_SEG]	Resp. de Seguridad	ALTO	7				
	[P_CORD]	Coordinador IT	MEDIO	4				

Tabla 5: Resultado valoración de activos.

4.5. Identificación de las Amenazas

Con los activos ya identificados y valorados, se procederá a determinar las amenazas que pueden afectar a cada activo. Para ello, MAGERIT clasifica las amenazas que pueden afectar a los activos en las siguientes categorías:

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

Para la identificación de las amenazas se ha usado el capítulo 5 del libro II de la metodología (MAGERIT - versión 3.0. Metodología de análisis y gestión de riesgos de los sistemas de información. Libro II. Catálogo de elementos., 2012, págs. 25- 47), de las cuales se obtiene la tabla de identificación de amenazas:

En el **Anexo X** se encuentra el listado de estas amenazas.

4.6. Valoración de las amenazas

Una vez identificadas las amenazas que afectan al sistema, se valora su influencia en el valor del activo teniendo en cuenta dos parámetros:

- La **impacto** del activo, es decir, el daño que sufrir el valor del activo en el caso de materializarse la amenaza.
- La **probabilidad de ocurrencia** que se materialice la amenaza.

En este análisis en concreto, se ha tomado la siguiente tabla de probabilidad de ocurrencia, de carácter cuantitativo:

Vulnerabilidad	Rango	Valor
Frecuencia extrema	1 ves al día	1
Frecuencia alta	1 vez cada 2 semanas	0,07
Frecuencia media	1 vez cada 2 meses	0,016

Frecuencia baja	1 vez cada 6 meses	0,005
Frecuencia muy baja	1 vez al año	0,002

Tabla 6: Valor estimado probabilidad de ocurrencia.

El impacto se mide en base al porcentaje del valor del activo dañado en el caso de que materialice la amenaza. Se ha seguido la siguiente tabla para tener una relación cualitativa-cuantitativa:

IMPACTO	VALOR
MUY ALTO	100%
ALTO	75%
MEDIO	50%
BAJO	20%
MUY BAJO	5%

Tabla 7: Valor de impacto.

Uniendo ambas tablas se puede generar un mapa de riesgo que nos será útil para ver el efecto que tiene el impacto y la frecuencia sobre el riesgo.

RIESGO		PROBABILIDAD				
		MUY BAJA	BAJA	MEDIA	ALTA	EXTREMA
IMPACTO	MUY ALTO	ALTO	MUY ALTO	MUY ALTO	MUY ALTO	MUY ALTO
	ALTO	MEDIO	ALTO	ALTO	MUY ALTO	MUY ALTO
	MEDIO	BAJO	MEDIO	MEDIO	ALTO	ALTO
	BAJO	MUY BAJO	BAJO	BAJO	MEDIO	MEDIO

	MUY BAJO	MUY BAJO	MUY BAJO	MUY BAJO	BAJO	BAJO

Tabla 8: Mapa de riesgo.

ACTIVO	AMENAZA	FRECUENCIA	%D	%I	%C	%A	%T
DATOS [D]	[E.1] Errores de los usuarios	0,016	75	75	50		
	[E.2] Errores del administrador	0,005	75	75	75		
	[E.3] Errores de monitorización (log)	0,07					20
	[E.4] Errores de configuración	0,016		50			
	[E.15] Alteración accidental de la información	0,005		75			
	[E.18] Destrucción de información	0,005	100				
	[E.19] Fugas de información	0,005			100		
	[A.3] Manipulación de los registros de actividad (log)	0,002	75		50	75	
	[A.4] Manipulación de la configuración	0,005					100
	[A.5] Suplantación de la identidad del usuario	0,005	50		75	100	
	[A.6] Abuso de privilegios de acceso	0,002	50	50	100		
	[A.11] Acceso no autorizado	0,005		50	100		
	[A.13] Repudio	0,002					75
	[A.15] Modificación deliberada de la información	0,002		100			
	[A.18] Destrucción de información	0,002	100				
	[A.19] Revelación de información	0,005			100		
CLAVES [K]	[E.2] Errores del administrador	0,002	5	5	5		
	[E.15] Alteración accidental de la información	0,002		5			
	[E.18] Destrucción de información	0,005	5				
	[E.19] Fugas de información	0,005			50		
	[A.5] Suplantación de la identidad del usuario	0,002		20	50	50	

	[A.6] Abuso de privilegios de acceso	0,005	5	20	50		
	[A.11] Acceso no autorizado	0,005		5	50		
	[A.15] Modificación deliberada de la información	0,002		5			
	[A.18] Destrucción de información	0,005	5				
	[A.19] Revelación de información	0,005			5		
	[E.1] Errores de los usuarios	0,016	50	20	20		
	[E.2] Errores del administrador	0,005	100	75	75		
	[E.9] Errores de [re-]encaminamiento	0,005	50				
	[E.10] Errores de secuencia	0,005		50			
	[E.15] Alteración accidental de la información	0,005		100			
	[E.18] Destrucción de información	0,005	100				
	[E.19] Fugas de información	0,005			50		
	[E.24] Caída del sistema por agotamiento de recursos	0,005	100				
	[A.5] Suplantación de la identidad del usuario	0,005		50	75	100	
SERVICIOS [S]	[A.6] Abuso de privilegios de acceso	0,005	75	100	100		
	[A.7] Uso no previsto	0,002	50	50	50		
	[A.9] [Re-]encaminamiento de mensajes	0,005			50		
	[A.10] Alteración de secuencia	0,005		50			
	[A.11] Acceso no autorizado	0,005		75	75		
	[A.12] Análisis de tráfico	0,002			50		
	[A.15] Modificación deliberada de la información	0,002		100			
	[A.18] Destrucción de información	0,005	100				
	[A.19] Revelación de información	0,005			50		
	[A.24] Denegación de servicio	0,005	100				
SOFTWARE [SW]	[I.5] Avería de origen físico o lógico	0,005	75				
	[E.1] Errores de los usuarios	0,016	75	75	50		
	[E.2] Errores del administrador	0,005	75	75	75		
	[E.8] Difusión de software dañino	0,002	75	75	75		
	[E.10] Errores de secuencia	0,002			50		

	[E.15] Alteración accidental de la información	0,016		100			
	[E.18] Destrucción de información	0,016	100				
	[E.19] Fugas de información	0,016			100		
	[E.20] Vulnerabilidades de los programas (software)	0,005	20	75	75		
	[E.21] Errores de mantenimiento / actualización de programas (software)	0,005	75	75			
	[A.5] Suplantación de la identidad del usuario	0,005	75		50	100	
	[A.6] Abuso de privilegios de acceso	0,005	20	20	100		
	[A.7] Uso no previsto	0,002	20	20	20		
	[A.8] Difusión de software dañino	0,002	100	100	100		
	[A.9] [Re-]encaminamiento de mensajes	0,002			50		
	[A.10] Alteración de secuencia	0,002		50			
	[A.11] Acceso no autorizado	0,005		50	100		
	[A.15] Modificación deliberada de la información	0,005		100			
	[A.18] Destrucción de información	0,005	100				
	[A.19] Revelación de información	0,005			75		
	[A.22] Manipulación de programas	0,005	50	75	50		
HARDWARE [HW]	[N.1] Fuego	0,002	100				
	[N.2] Daños por agua	0,002	100				
	[I.1] Fuego	0,002	100				
	[I.2] Daños por agua	0,002	100				
	[I.3] Contaminación mecánica	0,002	100				
	[I.4] Contaminación electromagnética	0,002	100				
	[I.5] Avería de origen físico o lógico	0,005	100				
	[I.6] Corte del suministro eléctrico	0,002	100				

	[I.7] Condiciones inadecuadas de temperatura y/o humedad	0,005	100				
	[I.11] Emanaciones electromagnéticas	0,002	100				
	[E.2] Errores del administrador	0,002	50	50	50		
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	0,002	50				
	[E.24] Caída del sistema por agotamiento de recursos	0,005	100				
	[E.25] Robo	0,005	100		75		
	[A.6] Abuso de privilegios de acceso	0,005	20	50	50		
	[A.7] Uso no previsto	0,005	20	20	20		
	[A.11] Acceso no autorizado	0,005		50	50		
	[A.23] Manipulación de los equipos	0,005	75		75		
	[A.24] Denegación de servicio	0,002	100				
	[A.25] Robo	0,005	100		100		
	[A.26] Ataque destructivo	0,002	100				
REDES [COM]	[I.8] Fallo de servicios de comunicaciones	0,016	100				
	[E.2] Errores del administrador	0,005	50	20	20		
	[E.9] Errores de [re-]encaminamiento	0,002			20		
	[E.10] Errores de secuencia	0,002		20			
	[E.15] Alteración accidental de la información	0,002		20			
	[E.18] Destrucción de información	0,002	75				
	[E.19] Fugas de información	0,002			20		
	[E.24] Caída del sistema por agotamiento de recursos	0,005	100				
	[A.5] Suplantación de la identidad del usuario	0,005	20	50	100		
	[A.6] Abuso de privilegios de acceso	0,016	20	20	20		
	[A.7] Uso no previsto	0,002	50	20	20		

	[A.9] [Re-]encaminamiento de mensajes	0,002			50		
	[A.10] Alteración de secuencia	0,002		50			
	[A.11] Acceso no autorizado	0,002		50			
	[A.12] Análisis de tráfico	0,016			20		
	[A.14] Interceptación de información (escucha)	0,002			75		
	[A.15] Modificación deliberada de la información	0,002		100			
	[A.24] Denegación de servicio	0,002	100				
	[N.1] Fuego	0,002	100				
	[N.2] Daños por agua	0,002	100				
	[I.1] Fuego	0,002	100				
	[I.2] Daños por agua	0,002	100				
	[I.3] Contaminación mecánica	0,002	100				
	[I.4] Contaminación electromagnética	0,002	100				
EQUIPO AUX [AUX]	[I.5] Avería de origen físico o lógico	0,002	100				
	[I.7] Condiciones inadecuadas de temperatura o humedad	0,002	100				
	[I.9] Interrupción de otros servicios y suministros esenciales	0,002	100				
	[E.23] Errores de mantenimiento/actualización de equipos	0,002	100				
	[E.25] Pérdida de equipos	0,002	100		5		
	[A.7] Uso no previsto	0,005	5	5	5		
	[A.11] Acceso no autorizado	0,002		5	5		
	[A.23] Manipulación de los equipos	0,005	100		5		

	[A.25] Robo	0,002	100		5		
	[A.26] Ataque destructivo	0,002	100				
INSTALACIONES [L]	[N.1] Fuego	0,002	100				
	[N.2] Daños por agua	0,002	100				
	[I.1] Fuego	0,002	100				
	[I.2] Daños por agua	0,005	100				
	[I.11] Emanaciones electromagnéticas	0,002			5		
	[E.15] Alteración accidental de la información	0,005		20			
	[E.18] Destrucción de información	0,005	50	100			
	[E.19] Fugas de información	0,005			50		
	[A.7] Uso no previsto	0,005	20	50	20		
	[A.11] Acceso no autorizado	0,005		50	50		
	[A.15] Modificación deliberada de la información	0,002		75			
	[A.18] Destrucción de información	0,002	75				
	[A.19] Revelación de información	0,002			75		
	[A.26] Ataque destructivo	0,002	100				
	[A.27] Ocupación enemiga	0,002	100		50		
PERSONAL [P]	[E.7] Deficiencias en la organización	0,002	20	20	20		
	[E.19] Fugas de información	0,005			100		
	[E.28] Indisponibilidad del personal	0,005	50				
	[A.28] Indisponibilidad del personal	0,005	50				
	[A.29] Extorsión	0,002	20	20	50		
	[A.30] Ingeniería social (picaresca)	0,002	20	20	20		

Tabla 9: Dimensiones de seguridad.

4.7. Análisis del impacto

A partir de la tabla de activos y dimensiones de seguridad, y conociendo previamente los valores de los diferentes activos, es posible determinar el impacto potencial que pueden suponer para la organización la materialización de las amenazas. Se trata de un dato relevante, ya que permitirá priorizar el plan de acción y a la vez evaluar como se ve modificado el denominado valor una vez se apliquen las contramedidas.

El impacto potencial para cada dimensión de cada activo lo obtenemos mediante la siguiente formula:

Impacto Potencial = Valor Activo * Impacto

Para el impacto de cada activo se toma el valor de la amenaza que sufre mayor impacto obtenido en el estudio de impacto realizado previamente.

CATEGORÍA	ACTIVO	VALOR					IMPACTO					IMPACTO POTENCIAL				
		D	I	C	A	T	D	I	C	A	T	D	I	C	A	T
Datos [D]	[D_XFILE]	3	7	7	7	7	1	1	1	1	1	3	7	7	7	7
	[D_BKP]	6	8	3	8	8						6	8	3	8	8
	[D_BDCL]	9	10	9	10	10						9	10	9	10	10
	[D_COD]	6	9	8	7	6						6	9	8	7	6
	[D_LOG]	5	2	5	1	8						5	2	5	1	8
	[D_CONF]	9	9	9	9	9						9	9	9	9	9
Claves [K]	[K_SSL]	9	9	9	9	9	0,05	0,2	0,5	0,5		0,45	1,8	4,5	4,5	
Servicios [S]	[S_WEB]	9	9	7	8	7	1	1	1	1		9	9	7	8	
	[S_CAU]	7	8	7	7	5						7	8	7	7	
	[S_EMAIL]	7	8	7	7	5						7	8	7	7	
Software [SW]	[SW_SQL]	7	7	3	7	7	1	1	1	1		7	7	3	7	
	[SW_BKP]	5	3	3	3	7						5	3	3	3	
	[SW_OFI]	5	5	7	5	4						5	5	7	5	

	[SW_VIR]	5	3	3	3	4						5	3	3	3	
	[SW_MS]	1	3	3	3	1						1	3	3	3	
	[SW_WS]	8	7	7	4	7						8	7	7	4	
	[SW_W10]	2	2	2	3	2						2	2	2	3	
	[SW_PBX]	8	7	7	4	7						8	7	7	4	
	[SW_GPS]	5	7	3	7	7						5	7	3	7	
Hardware [HW]	[HW_PORT]	5	5	5	4	4	1	0,5	1			5	2,5	5		
	[HW_IMP]	3	3	4	3	3						3	1,5	4		
	[HW_FW]	9	9	9	9	9						9	4,5	9		
	[HW_SWTH]	7	9	7	7	5						7	4,5	7		
	[HW_SERV]	9	9	7	8	7						9	4,5	7		
	[HW_ALM]	7	9	8	7	7						7	4,5	8		
	[HW_TELF]	6	5	4	4	4						6	2,5	4		
Redes de Comunicaciones [COM]	[COM_TEL]	6	1	3	5	2	1	1	1			6	1	3		
	[COM_LAN]	10	8	10	5	8						10	8	10		
	[COM_WIFI]	7	9	7	7	7						7	9	7		
	[COM_INTER]	9	9	9	9	9						9	9	9		
Equipamiento Auxiliar [AUX]	[AUX_VENT]	9					1	0,05	0,05			9				
	[AUX_CONS]	3										3				
	[AUX_CE]	9										9				
	[AUX_ACCCON]	7	7	7	7							7	0,4	0,4		
	[AUX_RED]	9										9				
Instalaciones [L]	[L_CPD]	10	10	8	9	7	1	1	0,75			10	10	6		
	[L_OFI]	5	3	5	7	2						5	3	3,8		
Personal [P]	[P_RRHH]	6					0,5	0,2	1			3				
	[P_SIST]	9										4,5				
	[P_COM]	9										4,5				
	[P_CAU]	7										3,5				

	[P_SW]	4										2				
	[P_SEG]	7										3,5				
	[P_CORD]	4										2				

Tabla 10: Cálculo Impacto Potencial.

4.8. Nivel de riesgo aceptable y riesgo residual

La última fase en este análisis de riesgo es determinar en base a la probabilidad de ocurrencia y el impacto potencial, el riesgo que está dispuesta a asumir la compañía.

Estos niveles tienen que ser aceptados por la Dirección de la compañía y en este caso particular se ha llegado al siguiente acuerdo:

RANGO	RIESGO
> 0,5	RIESGO INTOLERANTE
0,1 < X < 0,5	RIESGO MODERADO
< 0,1	RIESGO ACEPTABLE

Tabla 11: Nivel de riesgo.

Para calcular el riesgo se ha empleado la siguiente fórmula:

Riesgo = Impacto Potencial x Frecuencia

El resultado obtenido se recoge en la tabla:

CATEGORÍA	ACTIVO	VALOR	IMPACTO					IMPACTO POTENCIAL					FREC	RIESGO				
			D	I	C	A	T	D	I	C	A	T		D	I	C	A	T
Datos [D]	[D_XFILE]	MEDIO	1	1	1	1	1	3	7	7	7	7	0,07	0,21	0,5	0,5	0,5	0,5

	[D_BKP]	MEDIO						6	8	3	8	8		0,42	0,6	0,2	0,6	0,6
	[D_BDCL]	MUY ALTO						9	10	9	10	10		0,63	0,7	0,6	0,7	0,7
	[D_COD]	ALTO						6	9	8	7	6		0,42	0,6	0,6	0,5	0,4
	[D_LOG]	MEDIO						5	2	5	1	8		0,35	0,1	0,4	0,1	0,6
	[D_CONF]	MUY ALTO						9	9	9	9	9		0,63	0,6	0,6	0,6	0,6
Claves [K]	[K_SSL]	MUY ALTO	0,1	0,2	0,5	0,5		0,5	1,8	5	5		0,005	0	0	0	0,1	
Servicios [S]	[S_WEB]	ALTO	1	1	1	1		9	9	7	8		0,016	0,14	0,1	0,1	0,1	
	[S_CAU]	ALTO						7	8	7	7			0,11	0,1	0,1	0,1	
	[S_EMAIL]	MEDIO						7	8	7	7			0,11	0,1	0,1	0,1	
Software [SW]	[SW_SQL]	MEDIO	1	1	1	1		7	7	3	7		0,016	0,11	0,1	0	0,1	
	[SW_BKP]	MEDIO						5	3	3	3			0,08	0	0	0	
	[SW_OFI]	MEDIO						5	5	7	5			0,08	0,1	0,1	0,1	
	[SW_VIR]	BAJO						5	3	3	3			0,08	0	0	0	
	[SW_MS]	BAJO						1	3	3	3			0,02	0	0	0	
	[SW_WS]	ALTO						8	7	7	4			0,13	0,1	0,1	0,1	
	[SW_W10]	BAJO						2	2	2	3			0,03	0	0	0	
	[SW_PBX]	ALTO						8	7	7	4			0,13	0,1	0,1	0,1	
	[SW_GPS]	MEDIO						5	7	3	7			0,08	0,1	0	0,1	
Hardware [HW]	[HW_PORT]	MEDIO	1	0,5	1			5	2,5	5			0,005	0,03	0	0		
	[HW_IMP]	BAJO						3	1,5	4				0,02	0	0		

	[HW_FW]	MUY ALTO						9	4,5	9				0,05	0	0		
	[HW_SWTH]	ALTO						7	4,5	7				0,04	0	0		
	[HW_SERV]	ALTO						9	4,5	7				0,05	0	0		
	[HW_ALM]	ALTO						7	4,5	8				0,04	0	0		
	[HW_TELF]	MEDIO						6	2,5	4				0,03	0	0		
Redes de Comunicaciones [COM]	[COM_TEL]	MEDIO	1	1	1			6	1	3			0,016	0,1	0	0		
	[COM_LAN]	ALTO						10	8	10				0,16	0,1	0,2		
	[COM_WIFI]	ALTO						7	9	7				0,11	0,1	0,1		
	[COM_INTER]	MUY ALTO						9	9	9				0,14	0,1	0,1		
Equipamiento Auxiliar [AUX]	[AUX_VENT]	MUY ALTO	1	0,1	0,05			9					0,005	0,05				
	[AUX_CONS]	BAJO						3						0,02				
	[AUX_CE]	MUY ALTO						9						0,05				
	[AUX_ACCCON]	ALTO						7	0,4	0				0,04	0	0		
	[AUX_RED]	MUY ALTO						9						0,05				
Instalaciones [L]	[L_CPD]	ALTO	1	1	0,75			10	10	6			0,005	0,05	0,1	0		
	[L_OFI]	MEDIO						5	3	4				0,03	0	0		
Personal [P]	[P_RRHH]	MEDIO	0,5	0,2	1			3					0,005	0,02				
	[P_SIST]	MUY ALTO						4,5						0,02				

	[P_COM]	MUY ALTO					4,5						0,02				
	[P_CAU]	ALTO					3,5						0,02				
	[P_SW]	MEDIO					2						0,01				
	[P_SEG]	ALTO					3,5						0,02				
	[P_CORD]	MEDIO					2						0,01				

Tabla 12: Resultado del análisis de riesgos.

Según los resultados hallados, el Comité de Seguridad de la Información de la compañía acuerda categorizar el riesgo igual o inferior a 0,50 como riesgo moderado, focalizándose en analizar el riesgo cuyo valor supera el 0,5 para realizar acciones de mitigación de riesgo que reduzcan dichos valores a valores inferiores en un corto plazo de tiempo.

La compañía, por tanto, dirigirá su esfuerzo y presupuesto en realizar proyectos que aumenten el grado de madurez en ciberseguridad de la dimensión de Datos[D].

A medio plazo intentará también reducir el riesgo que actualmente se encuentra entre 0,1 y 0,5.

El riesgo por debajo de 0,1 se considera riesgo aceptable y no se realizará ninguna acción sobre el mismo.

5. PROPUESTAS DE PROYECTOS

Con el objetivo de mejorar el grado de madurez en seguridad de la información, en esta fase se procederá a la presentación de proyectos que se espera reduzcan el riesgo asociado a los distintos elementos que se analizaron en la fase anterior.

5.1. Proyectos propuestos

En la siguiente tabla se recoge la lista de los proyectos propuestos, asociándoles el control que soportan e indicando el riesgo que se pretende mitigar.

Hay que destacar que se ha puesto el foco en la categoría de activos de MAGERIT, Datos [D], ya que se obtuvo en el análisis anterior que eran los activos con mayor riesgo.

	PROYECTO	CONTROL	RIESGO
PJ1	Implementación de un software para la gestión de activos	A8.1, A8.3, A11.2.5, A11.2.7 A11.2.8	E.25, A.18, A.19
PJ2	Diseño Plan de Continuidad de Negocio	A12.3, A.17.1, A17.2	N.1, N.2, N.*, I.2, I.*, I.8, I.10
PJ3	Implementación de un software DLP (Data Loss Prevention)	A18.1.2, A18.1.3, A18.1.4	E.19, A.18, A.19, A.30
PJ4	Diseño de Política de clasificación de la información	A8.2, A18.1.4	E.19, A.11, A.14, A.19
PJ5	Elaboración de guías de bastionado para los servidores	A9.4.1, A9.4.2, A9.4.3, A9.4.4, A12.6.2	A.3, A.4, A.6, A.11, A.22, A.23, A.24

PJ6	Plan de contingencia de datos - Backups y Restores	A12.3.1, A17.2.1	E.15, E.18, A.4, A.15, A.18
PJ7	Implementación de un sistema gestor de eventos y seguridad de la información (SIEM)	A16.1	E.2, E.3, E.4, E.20, A.3, A.5, A.6, A.7, A.8, A.11, A.12, A.14, A.24
PJ8	Implementación de un sistema de prevención y detección de intrusos (IDS e IPS)	A16.1	A.3, A.5, A.6, A.7, A.8, A.11, A.12, A.14, A.24
PJ9	Implementación de un sistema de detección de vulnerabilidades	A16.1	E.20

Tabla 13: Proyectos propuestos.

- **PJ1: Implementación de un software para la gestión de activos**

Responsable:	Jefe TICs
Prioridad:	Alta
Objetivo:	Soportar las actividades de gestión de activos físicos
Tiempo:	6 meses
Presupuesto:	15.000 €
Actividades:	
– Estudio del mercado y selección de proveedores. – Realización de una PoC con cada uno de los proveedores escogidos. – Selección de las métricas para la toma de decisión de la mejor solución. – Selección de la solución final y adquisición de la misma. – Implementación de la solución. – Pruebas de la solución. – Puesta en producción.	

Tabla 14: Proyecto 1.

- **PJ2: Diseño Plan de Continuidad de Negocio**

Responsable:	Resp. de Seguridad
Prioridad:	Alta
Objetivo:	Evitar la interrupción de los servicios de misión crítica y restablecer el pleno funcionamiento en el menor tiempo posible
Tiempo:	1 año
Presupuesto:	40.000 €
Actividades	
– Identificación y priorización de las amenazas. – Análisis de impacto en la compañía. – Creación del plan de respuesta y recuperación. – Adecuación de la solución. – Pruebas. – Refinamiento del plan de continuidad.	

Tabla 15: Proyecto 2.

- **PJ3: Implementación de un software DLP (Data Loss Prevention)**

Responsable:	Jefe TICs
Prioridad:	Alta
Objetivo:	Disminuir los riesgos asociados con fuga de información sensible y confidencial.
Tiempo:	6 meses
Presupuesto:	15.000 €
Actividades:	
– Estudio del mercado y selección de proveedores. – Realización de una PoC con cada uno de los proveedores escogidos. – Selección de las métricas para la toma de decisión de la mejor solución. – Selección de la solución final y adquisición de la misma. – Implementación de la solución . – Pruebas de la solución.	

– Puesta en producción.

Tabla 16: Proyecto 3.

- **PJ4: Diseño de Política de clasificación de la información**

Responsable:	Jefe TICs
Prioridad:	Alta
Objetivo:	Mejorar el tratamiento de los datos almacenados en los servidores y el acceso a los mismos. Cumplimiento de normativas de seguridad y auditoria de acceso a los datos.
Tiempo:	1 mes y medio
Presupuesto:	4.500 €
Actividades:	
– Elaboración de la Política de clasificación de documentos. – Aprobación y publicación de la política.	

Tabla 17: Proyecto 4.

- **PJ5: Elaboración de guías de bastionado para los servidores**

Responsable:	Resp. Sistemas
Prioridad:	Alta
Objetivo:	Mitigar el riesgo relacionado por errores en las configuraciones, instalaciones por defecto, puertos abierto innecesarios, mal uso de mecanismos de autenticación y vulnerables de los sistemas operativos, servicios y protocolos.
Tiempo:	6 meses
Presupuesto:	16.000 €
Actividades:	

– Elaboración de las guías. – Aplicación de las guías elaboradas. – Banco de pruebas de los sistemas.

Tabla 18: Proyecto 5.

- **PJ6: Plan de contingencia de datos - Backups y Restores**

Responsable:	Jefe TICs
Prioridad:	Alta
Objetivo:	Mejora de contingencia de datos de los servidores y reducir en los tiempos de restauración de datos en caso de necesidad
Tiempo:	3 meses
Presupuesto:	5.000 €
Actividades:	
– Revisión de la Política de Backups y Restores. – Adquisición de librería de cinta con dos drive – Configuración de la librería de cintas y software de gestión para su uso – Distribución de clientes en los servidores objetivo de las copias y configuración de los recursos que requieran Backups. – Pruebas y puesta en marcha.	

Tabla 19: Proyecto 6.

- **PJ7: Implementación de un sistema gestor de eventos y seguridad de la información (SIEM)**

Responsable:	Jefe TICs
Prioridad:	Media
Objetivo:	Soportar el proceso de gestión de incidentes de seguridad.
Tiempo:	6 meses

Presupuesto:	18.000€
Actividades:	
– Estudio del mercado y selección de proveedores. – Realización de una PoC con cada uno de los proveedores escogidos. – Selección de las métricas para la toma de decisión de la mejor solución. – Selección de la solución final y adquisición de la misma. – Implementación de la solución . – Pruebas de la solución. – Puesta en producción.	

Tabla 20: Proyecto 7.

- **PJ8: Implementación de un sistema de detección de vulnerabilidades**

Responsable:	Jefe TICs
Prioridad:	Media
Objetivo:	Detectar las vulnerabilidades de sistemas, software, redes y servicios y realizar actividades de pentesting al momento de implementar soluciones nuevas para el manejo de información.
Tiempo:	6 meses
Presupuesto:	12.000 €
Actividades:	
– Estudio del mercado y selección de proveedores. – Realización de una PoC con cada uno de los proveedores escogidos. – Selección de las métricas para la toma de decisión de la mejor solución. – Selección de la solución final y adquisición de la misma. – Implementación de la solución . – Pruebas de la solución. – Puesta en producción.	

Tabla 21: Proyecto 8.

- **PJ9: Implementación de un sistema de prevención y detección de intrusos (IDS e IPS)**

Responsable:	Jefe TICs

Prioridad:	Media
Objetivo:	Detectar las actividades anormales, que puedan evidenciar la explotación de alguna vulnerabilidad de la infraestructura de red o la materialización de un riesgo de un activo.
Tiempo:	6 meses
Presupuesto:	20.000 €
Actividades:	
– Estudio del mercado y selección de proveedores. – Realización de una PoC con cada uno de los proveedores escogidos. – Selección de las métricas para la toma de decisión de la mejor solución. – Selección de la solución final y adquisición de la misma. – Implementación de la solución . – Pruebas de la solución. – Puesta en producción.	

Tabla 22: Proyecto 9.

5.2. Evolución y desarrollo de los proyectos

Para la ejecución de la totalidad de los proyectos se ha estimado una duración de 2 años y medio, ejecutando en el primer año todos los proyectos con prioridad alta y dejando los proyectos con prioridad media para el comiendo del segundo año.

	PROYECTO	TIEMPO ESTIMADO	PRESUPUESTO
PJ1	Implementación de un software para la gestión de activos	6 meses	15.000 €
PJ2	Diseño Plan de Continuidad de Negocio	1 año	40.000 €
PJ3	Implementación de un software DLP (Data Loss Prevention)	6 meses	15.000 €

PJ4	Diseño de Política de clasificación de la información	1 mes y medio	4.500 €
PJ5	Elaboración de guías de bastionado para los servidores	6 meses	16.000 €
PJ6	Plan de contingencia de datos - Backups y Restores	3 meses	5.000 €
Presupuesto 1º año			95.500 €
PJ7	Implementación de un sistema gestor de eventos y seguridad de la información (SIEM)	6 meses	18.000 €
PJ8	Implementación de un sistema de detección de vulnerabilidades	6 meses	12.000 €
Presupuesto 2º año			30.000 €
PJ9	Implementación de un sistema de prevención y detección de intrusos (IDS e IPS)	6 meses	20.000 €
Presupuesto 3º año			20.000 €

Tabla 23: Presupuesto previsto para los proyectos.

5.3. Diagrama de GANTT

La evolución prevista para los proyectos, sin contar las posibles desviaciones que pudiera producirse, es la siguiente:

			2019						2020												2021											
Proyecto	F. Inicio	F. Final	7	8	9	10	11	12	1	2	3	4	5	6	7	8	9	10	11	12	1	2	3	4	5	6	1	2	3	4	5	6
PJ1	Julio '19	Diciembre '19																														
PJ2	Julio '19	Junio '20																														
PJ3	Enero '20	Junio '20																														
PJ4	Agosto '19	Septiembre '19																														
PJ5	Enero '20	Junio '20																														
PJ6	Octubre '19	Diciembre '19																														
PJ7	Julio '20	Diciembre '20																														
PJ8	Enero '21	Junio '21																														
PJ9	Enero '21	Junio '21																														

Tabla 24: Plazo estimado de ejecución de los proyectos.

5.4. Resultados

El siguiente gráfico muestra la mejora que se espera obtener con la ejecución de los proyectos. Como puede observe, se obtendrá una mejora considerable, consiguiendo niveles cercanos a los deseados en los dominios de **7. Gestión de activos y 8. Control de accesos.**

Sin duda, el dominio que obtiene una mayor mejora es **17. Aspectos de seguridad de la información para la gestión de la continuidad del negocio** debido a la fuerte inversión del proyecto PJ2.

Tabla 25.: Mejora esperada tras la ejecución de los proyectos.

6. Auditoría de Cumplimiento

6.1. Introducción

Llegados a esta fase, conocemos los activos de la empresa y hemos evaluado las amenazas. Es el momento de hacer un alto en el camino y evaluar hasta que punto la empresa cumple con las buenas prácticas en materia de seguridad. La ISO/IEC 27002:2013 nos servirá como marco de control del estado de la seguridad.

6.2. Evaluación de la madurez

Para calcular el grado de madurez de la compañía se ha procedido a la revisión de los controles de la norma ISO27000.

Para medir el grado de madurez se ha tomado como referencia la escala presentada en la Tabla 1. El resultado obtenido en esta auditoría se presenta a continuación.

El resultado de la revisión de los controles de la ISO27001:2013 ha sido:

4. CONTEXTO DE LA ORGANIZACIÓN	
4.1 CONOCIMIENTO DE LA ORGANIZACIÓN Y SU CONTEXTO	L3
4.2 COMPRENSIÓN DE LAS NECESIDADES Y EXPECTATIVAS DE LAS PARTES INTERESADAS	L3
4.3 DETERMINACIÓN DEL ALCANCE DEL SGSI	L4
4.4 SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN	L4
5. LIDERAZGO	
5.1 LIDERAZGO Y COMPROMISO	L4
5.2 POLÍTICA	L4
5.3 ROLES, RESPONSABILIDADES Y AUTORIDADES EN LA ORGANIZACIÓN	L4
6. PLANIFICACIÓN	
6.1 ACCIONES PARA TRATAR RIESGOS Y OPORTUNIDADES	L3
6.2 OBJETIVOS DE LA SEGURIDAD DE LA INFORMACIÓN	L3
7. SOPORTE	
7.1 RECURSOS	L5

7.2 COMPETENCIA	L4
7.3 TOMA DE CONCIENCIA	L3
7.4 COMUNICACIÓN	L4
7.5 INFORMACIÓN DOCUMENTADA	L4
8. OPERACIÓN	
8.1 PLANIFICACIÓN Y CONTROL OPERACIONAL	L3
8.2 EVALUACIÓN DE RIESGO DE LA SEGURIDAD DE LA INFORMACIÓN	L4
8.3 TRATAMIENTO DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN	L4
9. EVALUACIÓN DEL DESEMPEÑO	
9.1 SEGUIMIENTO, MEDICIÓN, ANÁLISIS Y EVALUACIÓN	L3
9.2 AUDITORÍA INTERNA	L4
9.3 REVISIÓN POR LA DIRECCIÓN	L4
10. MEJORA	
10.1 NO CONFORMIDADES Y ACCIONES CORRECTIVAS	L3
10.2 MEJORA CONTINUA	L4

Tabla 26: Revisión ISO27001:2013

En cuanto a los controles de la norma ISO27002:2013, el resultado de la revisión de sus 114 controles ha sido el siguiente.

OBJETIVO DE CONTROL/CONTROL	
A.5 POLITICAS DE SEGURIDAD DE LA INFORMACIÓN	
A.5.1.DIRECTRICES DE GESTIÓN DE SEGURIDAD DE LA INFORMACION	
A.5.1.1 POLÍTICAS PARA LA SEGURIDAD DE LA INFORMACIÓN	L3
A.5.1.2 REVISIÓN DE LAS POLÍTICAS PARA LA SEGURIDAD DE LA INFORMACIÓN	L4
A.6 ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	
A.6.1 ORGANIZACION INTERNA	
A.6.1.1 ROLES Y RESPONSABILIDADES EN SEGURIDAD DE LA INFORMACIÓN	L3
A.6.1.2 SEGREGACIÓN DE TAREAS	L4
A.6.1.3 CONTACTO CON LAS AUTORIDADES	L4
A.6.1.4 CONTACTO CON GRUPOS DE INTERÉS ESPECIAL	L3
A.6.1.5 SEGURIDAD DE LA INFORMACIÓN EN LA GESTIÓN DE PROYECTOS	L4
A.6.2 LOS DISPOSITIVOS MÓVILES Y EL TELETRABAJO	

A.6.2.1 POLÍTICA DE DISPOSITIVOS MÓVILES	L4
A.6.2.2 TELETRABAJO	L4
A.7 SEGURIDAD RELATIVA A LOS RECURSOS HUMANOS	
A.7.1. ANTES DEL EMPLEO	
A.7.1.1 INVESTIGACIÓN DE ANTECEDENTES	L2
A.7.1.2 TÉRMINOS Y CONDICIONES DEL EMPLEO	L5
A.7.2 DURANTE EL EMPLEO	
A.7.2.1 RESPONSABILIDADES DE GESTIÓN	L4
A.7.2.2 CONCIENCIACIÓN, EDUCACIÓN Y CAPACITACIÓN EN SEGURIDAD DE LA INFORMACIÓN	L4
A.7.2.3 PROCESO DISCIPLINARIO	L1
A.7.3 FINALIZACIÓN DEL EMPLEO O CAMBIO EN EL PUESTO DE TRABAJO	
A.7.3.1 RESPONSABILIDADES ANTE LA FINALIZACIÓN O CAMBIO	L3
A.8 GESTIÓN DE ACTIVOS	
A.8.1 RESPONSABILIDAD SOBRE LOS ACTIVOS	
A.8.1.1 INVENTARIO DE ACTIVOS	L5
A.8.1.2 PROPIEDAD DE LOS ACTIVOS	L5
A.8.1.3 USO ACEPTABLE DE LOS ACTIVOS	L4
A.8.1.4 DEVOLUCIÓN DE ACTIVOS	L4
A.8.2 CLASIFICACIÓN DE LA INFORMACIÓN	
A.8.2.1 CLASIFICACIÓN DE LA INFORMACIÓN	L4
A.8.2.2 ETIQUETADO DE LA INFORMACIÓN	L4
A.8.2.3 MANIPULADO DE LA INFORMACIÓN	L4
A.8.3 MANIPULACIÓN DE LOS SOPORTES	
A.8.3.1 GESTIÓN DE SOPORTES EXTRAIBLES	L3
A.8.3.2 ELIMINACIÓN DE SOPORTES	L3
A.8.3.3 SOPORTES FÍSICOS EN TRÁNSITO	L3
A.9 CONTROL DE ACCESO	
A.9.1. REQUISITOS DE NEGOCIO PARA EL CONTROL DE ACCESO	
A.9.1.1 POLÍTICA DE CONTROL DE ACCESO	L4
A.9.1.2 ACCESO A LAS REDES Y A LOS SERVICIOS DE RED	L4
A.9.2 GESTIÓN DE ACCESO DE USUARIO	
A.9.2.1 REGISTRO Y BAJA DE USUARIO	L4
A.9.2.2 PROVISIÓN DE ACCESO DE USUARIO	L4
A.9.2.3 GESTIÓN DE PRIVILEGIOS DE ACCESO	L4
A.9.2.4 GESTIÓN DE LA INFORMACIÓN SECRETA DE AUTENTICACIÓN DE LOS USUARIOS	L3
A.9.2.5 REVISIÓN DE LOS DERECHOS DE ACCESO DE USUARIO	L4

A.9.2.6 RETIRADA O REASIGNACIÓN DE LOS DERECHOS DE ACCESO	L4
A.9.3 RESPONSABILIDADES DEL USUARIO	
A.9.3.1 USO DE LA INFORMACIÓN SECRETA DE LA AUTENTICACIÓN	L3
A.9.4 CONTROL DE ACCESO A SISTEMAS Y APLICACIONES	
A.9.4.1 RESTRICCIÓN DEL ACCESO A LA INFORMACIÓN	L4
A.9.4.2 PROCEDIMIENTOS SEGUROS DE INICIO DE SESIÓN	L4
A.9.4.3 SISTEMA DE GESTIÓN DE CONTRASEÑAS	L5
A.9.4.4 USO DE UTILIDADES CON PRIVILEGIOS DEL SISTEMA	L2
A.9.4.5 CONTROL DE ACCESO AL CÓDIGO FUENTE DE PROGRAMAS	L3
A.10 CRIPTOGRAFÍA	
A.10.1 CONTROLES CRIPTOGRÁFICOS	
A.10.1.1 POLÍTICA DE USO DE LOS CONTROLES CRIPTOGRÁFICOS	L3
A.10.1.2 GESTION DE CLAVES	L4
A.11 SEGURIDAD FÍSICA Y DEL ENTORNO	
A.11.1 ÁREAS SEGURAS	
A.11.1.1 PERÍMETRO DE SEGURIDAD FÍSICA	L5
A.11.1.2 CONTROLES FÍSICOS DE ENTRADA	L4
A.11.1.3 SEGURIDAD DE OFICINAS, DESPACHOS Y RECURSOS	L4
A.11.1.4 PROTECCIÓN CONTRA LAS AMENAZAS EXTERNAS Y AMBIENTALES	L4
A.11.1.5 EL TRABAJO EN ÁREAS SEGURAS	L3
A.11.1.6 ÁREAS DE CARGA Y DESCARGA	L3
A.11.2 SEGURIDAD DE LOS EQUIPOS	
A.11.2.1 EMPLAZAMIENTO Y PROTECCIÓN DE EQUIPOS	L2
A.11.2.2 INSTALACIONES DE SUMINISTRO	L3
A.11.2.3 SEGURIDAD DEL CABLEADO	L3
A.11.2.4 MANTENIMIENTO DE LOS EQUIPOS	L2
A.11.2.5 RETIRADA DE MATERIALES PROPIEDAD DE LA EMPRESA	L2
A.11.2.6 SEGURIDAD DE LOS EQUIPOS FUERA DE LAS INSTALACIONES	L2
A.11.2.7 REUTILIZACIÓN O ELIMINACIÓN SEGURA DE EQUIPOS	L2
A.11.2.8 EQUIPO DE USUARIO DESATENDIDO	L3
A.11.2.9 POLÍTICA DE PUESTO DE TRABAJO DESPEJADO Y PANTALLA LIMPIA	L4
A.12 SEGURIDAD DE LAS OPERACIONES	
A.12.1 PROCEDIMIENTOS Y RESPONSABILIDADES OPERACIONALES	

A.12.1.1 PROCEDIMIENTOS OPERACIONALES DOCUMENTADOS	L1
A.12.1.2 GESTION DE CAMBIOS	L1
A.12.1.3 GESTION DE LA CAPACIDAD	L2
A.12.1.4 SEPARACION DE LOS ENTORNOS DE DESARROLLO, TEST Y OPERACIONES	L3
A.12.2 PROTECCION CONTRA SOFTWARE MALICIOSO	
A.12.2.1 CONTROLES CONTRA EL CÓDIGO MALICIOSO	L4
A.12.3 COPIAS DE SEGURIDAD	
A.12.3.1 COPIAS DE SEGURIDAD DE LA INFORMACION	L4
A.12.4 REGISTROS Y SUPERVISIÓN	
A.12.4.1 REGISTRO DE EVENTOS	L4
A.12.4.2 PROTECCION DE LA INFORMACION DE LOS REGISTROS	L2
A.12.4.3 REGISTROS DE ADMINISTRADOR Y OPERADOR	L2
A.12.4.4 SINCRONIZACION DE RELOJES	L3
A.12.5 CONTROL DEL SOFTWARE EN EXPLOTACIÓN	
A.12.5.1 INSTALACIÓN DE SOFTWARE EN SISTEMAS DE PRODUCCIÓN	L3
A.12.6 GESTION DE LA VULNERABILIDAD TECNICA	
A.12.6.1 CONTROL DE VULNERABILIDADES TECNICAS	L2
A.12.6.2 RESTRICCIONES DE LA INSTALACIÓN DE SOFTWARE	L3
A.12.7 CONSIDERACIONES EN LA AUDITORIA DE SISTEMAS DE INFORMACION	
A.12.7.1 CONTROLES DE LA AUDITORIA DE LOS SISTEMAS DE INFORMACION	L3
A.13 SEGURIDAD DE LAS COMUNICACIONES	
A.13.1 GESTION DE LA SEGURIDAD DE REDES	
A.13.1.1 CONTROLES DE RED	L4
A.13.1.2 SEGURIDAD DE LOS SERVICIOS DE RED	L4
A.13.1.3 SEGREGACION EN REDES	L4
A.13.2 INTERCAMBIO DE INFORMACION	
A.13.2.1 POLITICAS Y PROCEDIMIENTOS DE INTERCAMBIO DE INFORMACION	L3
A.13.2.2 ACUERDOS DE INTERCAMBIO DE INFORMACIÓN	L4
A.13.2.3 MENSAJERIA ELECTRONICA	L3
A.13.2.4 ACUERDOS DE CONFIDENCIALIDAD O NO DIVULGACIÓN	L3
A.14 ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACION	
A.14.1 REQUISITOS DE SEGURIDAD EN SISTEMAS DE INFORMACION	
A.14.1.1 ANALISIS Y ESPECIFICACION DE REQUISITOS DE SEGURIDAD DE LA INFORMACIÓN	L2

A.14.1.2 SEGURIDAD DE SERVICIOS DE APLICACIÓN EN REDES PÚBLICAS	L3
A.14.1.3 PROTECCIÓN DE TRANSCCIONES DE SERVICIOS DE APLICACIONES	L3
A.14.2 SEGURIDAD EN LOS PROCESOS DE DESARROLLO Y SOPORTE	
A.14.2.1 POLITICA DE DESARROLLO SEGURO	L2
A.14.2.2 PROCEDIMIENTOS DE CONTROL DE CAMBIOS DEL SISTEMA	L3
A.14.2.3 REVISION TECNICA DE LAS APLICACIONES TRAS CAMBIOS EN EL SISTEMA OPERATIVO	L4
A.14.2.4 RESTRICCIONES A LOS CAMBIOS EN LOS PAQUETES DE SOFTWARE	L2
A.14.2.5 PRINCIPIOS DE INGENIERÍA DE SISTEMAS SEGUROS	L2
A.14.2.6 ENTORNO DE DESARROLLO SEGURO	L2
A.14.2.7 EXTERNALIZACIÓN DEL DESARROLLO SOFTWARE	L3
A.14.2.8 PRUEBAS DE SEGURIDAD DEL SISTEMA	L2
A.14.2.9 PRUEBAS DE ACEPTACION DEL SISTEMA	L2
A.14.3 DATOS DE PRUEBA	
A.14.3.1 PROTECCION DE LOS DATOS DE PRUEBA	L1
A.15 RELACION CON PROVEEDORES	
A.15.1 SEGURIDAD EN LAS RELACIONES CON PROVEEDORES	
A.15.1.1 POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN PARA LAS RELACIONES CON PROVEEDORES	L3
A.15.1.2 ABORDAR LA SEGURIDAD DENTRO DE LOS ACUERDOS CON PROVEEDORES	L4
A.15.1.3 CADENA DE SUMINISTRO TIC	L4
A.15.2 GESTION DE LA PROVISIÓN DE SERVICIOS DEL PROVEEDOR	
A.15.2.1 MONITORIZACION Y REVISION DE SERVICIOS DEL PROVEEDOR	L3
A.15.2.2 GESTION DE CAMBIOS A SERVICIOS DEL PROVEEDOR	L3
A.16 GESTION DE INCIDENTES DE SEGURIDAD DE LA INFORMACION	
A.16.1 GESTION DE INCIDENTES DE SEGURIDAD DE LA INFORMACION Y MEJORAS	
A.16.1.1 RESPONSABILIDADES Y PROCEDIMIENTOS	L3
A.16.1.2 NOTIFICACIÓN DE LOS EVENTOS DE SEGURIDAD DE LA INFORMACION	L3
A.16.1.3 NOTIFICACIÓN DE LOS PUNTOS DÉBILES DE LA SEGURIDAD	L3
A.16.1.4 EVALUACIÓN Y DECISIÓN SOBRE LOS EVENTOS DE SEGURIDAD DE LA INFORMACIÓN	L3
A.16.1.5 RESPUESTA A INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	L3

A.16.1.6 APRENDIZAJE DE LOS INCIDENTES DE SEGURIDAD DE LA INFORMACION	L3
A.16.1.7 RECOPILACIÓN DE EVIDENCIAS	L3
A.17 ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN PARA LA GESTION DE LA CONTINUIDAD DEL NEGOCIO	
A.17.1 CONTINUIDAD DE LA SEGURIDAD DE LA INFORMACION	
A.17.1.1 PLANIFICACIÓN LA CONTINUIDAD DE LA SEGURIDAD DE LA INFORMACIÓN	L4
A.17.1.2 IMPLEMENTAR LA CONTINUIDAD DE LA SEGURIDAD DE LA INFORMACION	L4
A.17.1.3 VERIFICACIÓN, REVISIÓN Y EVALUACIÓN DE LA CONTINUIDAD DE LA SEGURIDAD DE LA INFORMACIÓN	L4
A.17.2 REDUNDANCIAS	
A.17.2.1 DISPONIBILIDAD DE LOS RECURSOS DE TRATAMIENTO DE LA INFORMACIÓN	L3
A.18 CUMPLIMIENTO	
A.18.1 CUMPLIMIENTO DE LOS REQUISITOS LEGALES Y CONTRACTUALES	
A.18.1.1 IDENTIFICACION DE LA LEGISLACION APLICABLE Y REQUISITOS CONTRACTUALES	L3
A.18.1.2 DERECHOS DE PROPIEDAD INTELECTUAL	L3
A.18.1.3 PROTECCION DE LOS REGISTROS DE LA ORGANIZACIÓN	L3
A.18.1.4 PROTECCION Y PRIVACIDAD DE LA INFORMACIÓN DE CARÁCTER PERSONAL	L3
A.18.1.5 REGULACION DE LOS CONTROLES CRIPTOGRAFICOS	L3
A.18.2 REVISIONES DE SEGURIDAD DE LA INFORMACIÓN	
A.18.2.1 REVISION INDEPENDIENTE DE LA SEGURIDAD DE LA INFORMACION	L3
A.18.2.2 CUMPLIMIENTO DE LAS POLITICAS Y NORMAS DE SEGURIDAD	L3
A.18.2.3 COMPROBACIÓN DEL CUMPLIMIENTO TÉCNICO	L3

Tabla 27: Resultado Análisis Madurez de los controles ISO27002:2013.

En la auditoría realizada se han encontrado ***4 No conformidades de grado Menor (L1)***.

Dominio: 7 SEGURIDAD RELATIVA A LOS RECURSOS HUMANOS
Control: 7.2.3 PROCESO DISCIPLINARIO
Grado de No conformidad: Menor
Comentario: El proceso disciplinario no cuenta con la suficiente aprobación y su existencia no ha sido debidamente comunicada a los empleados.

Dominio: 12. SEGURIDAD DE LAS OPERACIONES
Control: 12.1.1 PROCEDIMIENTOS OPERACIONALES DOCUMENTADOS
Grado de No conformidad: Menor
Comentario: La documentación no se está llevando a cabo regularmente. Los procedimientos son insuficientes.
Dominio: 12. SEGURIDAD DE LAS OPERACIONES
Control: 12.1.2 GESTION DE CAMBIOS
Grado de No conformidad: Menor
Comentario: La gestión de cambios no está automatizada. No existen indicadores que midan la eficiencia del control.
Dominio: 14. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN
Control: 14.3.1 PROTECCION DE LOS DATOS DE PRUEBA
Grado de No conformidad: Menor
Comentario: No existen medidas que garanticen la seguridad de los datos de prueba.

Tabla 28: No conformidades detectadas.

6.3. Resultados

Como resultado, se muestra de manera general el nivel de madurez de la compañía tras la realización de la auditoria interna donde se han revisado todos los controles de la norma ISO27000 siguiendo los valores de la Tabla 1.

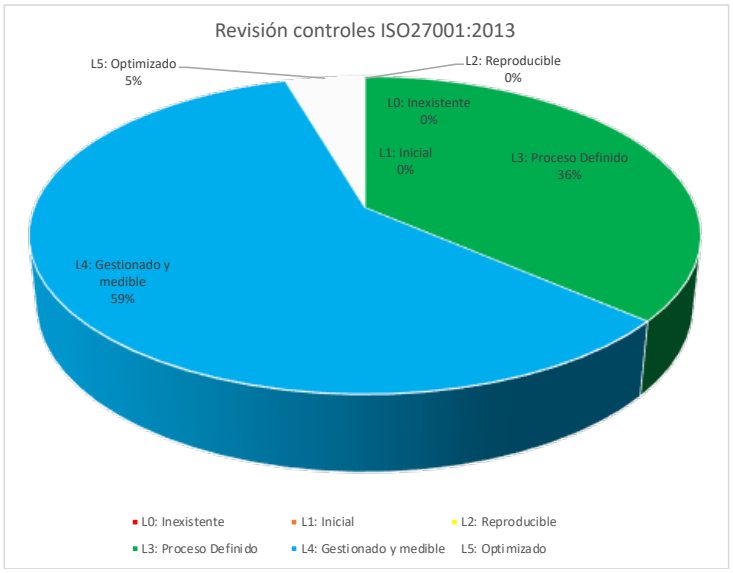

Ilustración 7: Resultado madurez conforme ISO27001:2013.

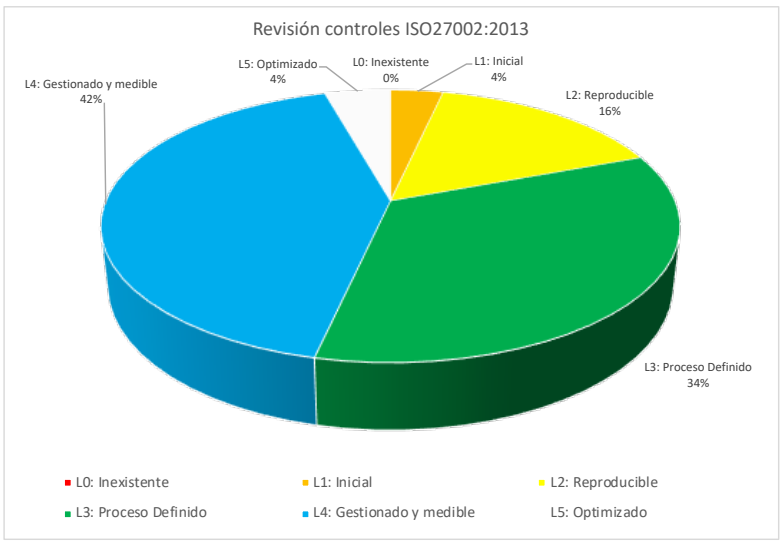

Ilustración 8: Resultado madurez conforme ISO27002:2013.

6.4. Evolución de la seguridad de la información en la organización

Echando la vista atrás, se pueden comparar estos resultados con los obtenidos en la fase inicial del proyecto donde se realizó el análisis diferencial. La mejora en el grado de madurez de la compañía es más que notoria, tal y como se puede apreciar en los gráficos siguientes.

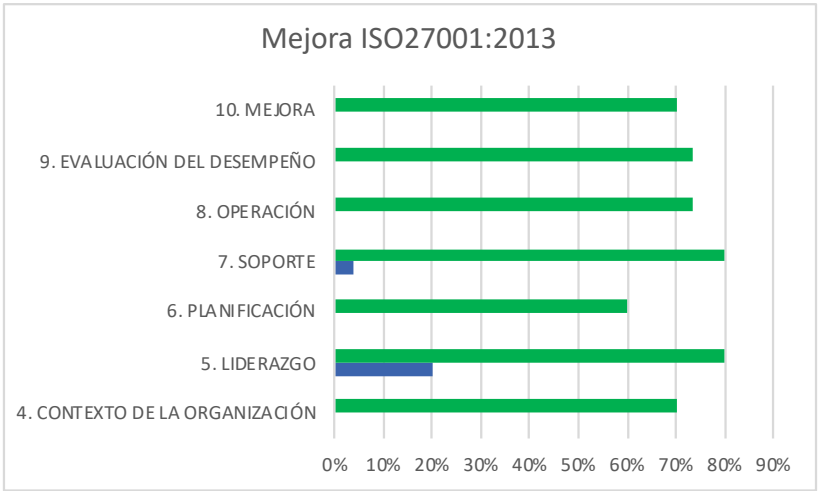

Ilustración 10:Comparativa ISO27001 antes y después del proyecto.

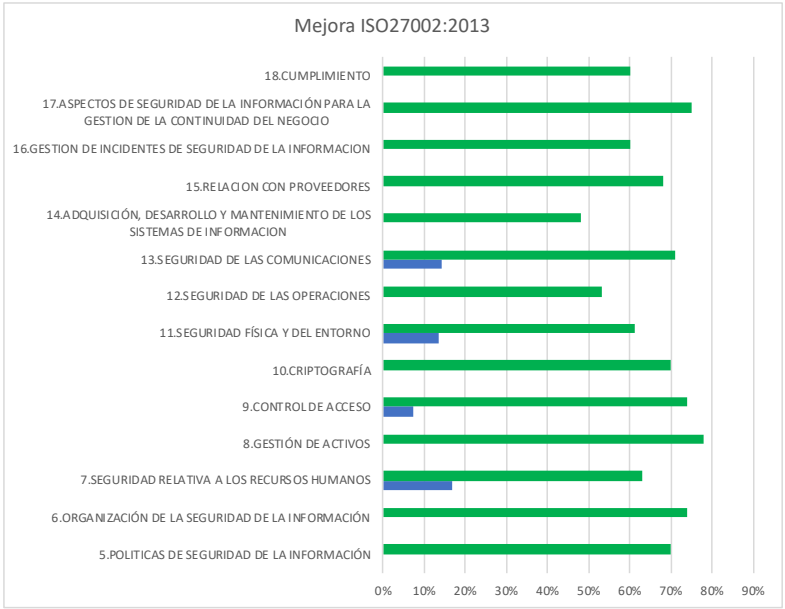

Ilustración 9: Comparativa ISO27002 antes y después del proyecto.

Mirando a futuro, podemos ver que cada vez la compañía se encuentra más cerca del valor de cumplimiento deseado.

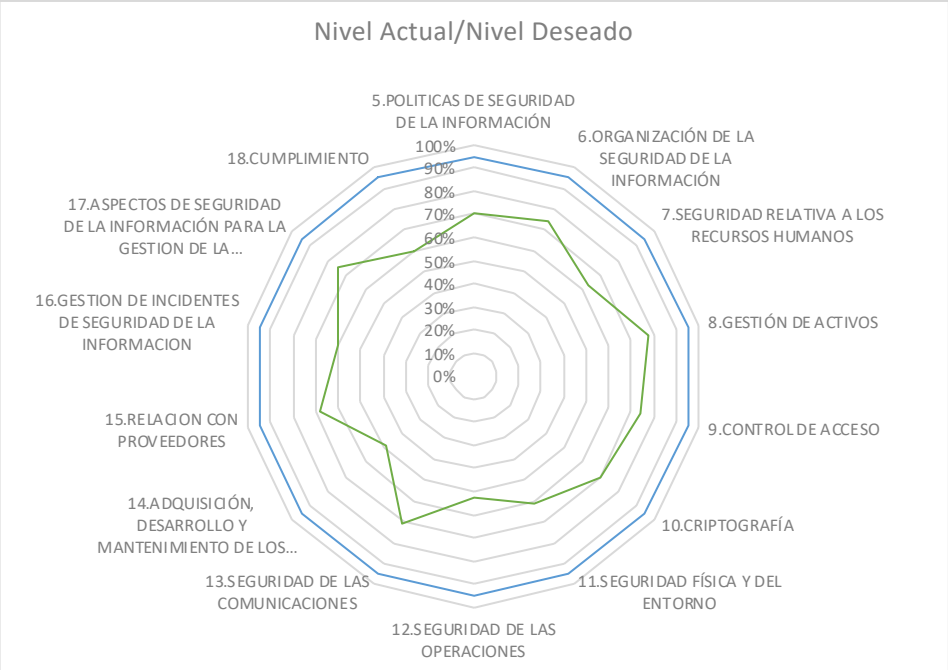

Ilustración 11: Comparativa nivel actual con nivel deseado.

7. Conclusión

La ejecución del presente proyecto ha supuesto una mejora en el nivel de madurez de seguridad de la información de la compañía Conecta Bus S.L.

Al inicio del proyecto la empresa carecía de SGSI y gracias a la ejecución del proyecto, Conecta Bus S.L ya cuenta con un SGSI funcionando de forma transversal para casi la totalidad de los departamentos de la compañía.

Los empleados han adquirido muchos conocimientos y el grado de concienciación con la importancia de la seguridad de la información ha aumentado como se ha podido conocer tras la realización de exámenes tipo test que han pasado los empleados al finalizar el proyecto.

Por parte de la gerencia también se ha conseguido una mayor tranquilidad al comprobar que el gasto en materia de seguridad ha sido correctamente invertido.

Como posibles líneas futuras se plantea la ejecución a posteriori de otro Plan Director de seguridad que proporcione los siguientes proyectos en materia de seguridad a ejecutar por la compañía en su búsqueda por aumentar el grado de madurez y reducir más aún el nivel de riesgo de la compañía.

8. Bibliografía

- Portal Web ISO27000 en Español

http://www.iso27000.es/

- Controles de la norma ISO 27002:2013

http://www.iso27000.es/download/ControlesISO27002-2013.pdf

- Proceso de Auditoria

http://www.iso27000.es/certificacion.html

- INCIBE

https://www.incibe.es/extfrontinteco/img/File/intecocert/sgsi/index.html

- Wikipedia ISO 27000

https://es.wikipedia.org/wiki/ISO/IEC_27000-series

- Magerit Libro II

https://www.ccn-cert.cni.es/documentos-publicos/1791-magerit-libro-ii-catalogo.html

- Documentación de la asignatura Sistemas de Gestión de la Seguridad de la Información de la UOC

ANEXO I

Análisis diferencial ISO 27001:2013

CONECTA BUS S.L

4. CONTEXTO DE LA ORGANIZACIÓN	
4.1 CONOCIMIENTO DE LA ORGANIZACIÓN Y SU CONTEXTO	0%
4.2 COMPRENSIÓN DE LAS NECESIDADES Y EXPECTATIVAS DE LAS PARTES INTERESADAS	0%
4.3 DETERMINACIÓN DEL ALCANCE DEL SGSI	0%
4.4 SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN	0%
5. LIDERAZGO	
5.1 LIDERAZGO Y COMPROMISO	60%
5.2 POLÍTICA	0%
5.3 ROLES, RESPONSABILIDADES Y AUTORIDADES EN LA ORGANIZACIÓN	0%
6. PLANIFICACIÓN	
6.1 ACCIONES PARA TRATAR RIESGOS Y OPORTUNIDADES	0%
6.2 OBJETIVOS DE LA SEGURIDAD DE LA INFORMACIÓN	0%
7. SOPORTE	
7.1 RECURSOS	0%
7.2 COMPETENCIA	0%
7.3 TOMA DE CONCIENCIA	0%
7.4 COMUNICACIÓN	0%
7.5 INFORMACIÓN DOCUMENTADA	20%
8. OPERACIÓN	
8.1 PLANIFICACIÓN Y CONTROL OPERACIONAL	0%
8.2 EVALUACIÓN DE RIESGO DE LA SEGURIDAD DE LA INFORMACIÓN	0%
8.3 TRATAMIENTO DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN	0%
9. EVALUACIÓN DEL DESEMPEÑO	
9.1 SEGUIMIENTO, MEDICIÓN, ANÁLISIS Y EVALUACIÓN	0%
9.2 AUDITORÍA INTERNA	0%
9.3 REVISIÓN POR LA DIRECCIÓN	0%
10. MEJORA	
10.1 NO CONFORMIDADES Y ACCIONES CORRECTIVAS	0%
10.2 MEJORA CONTINUA	0%

Ilustración 1: Resultado análisis diferencial ISO 27001:2013.

ANEXO II

Análisis diferencial ISO 27002:2013

CONECTA BUS S.L

A.5 POLITICAS DE SEGURIDAD DE LA INFORMACIÓN	
A.5.1.DIRECTRICES DE GESTIÓN DE SEGURIDAD DE LA INFORMACION	
A.5.1.1 POLÍTICAS PARA LA SEGURIDAD DE LA INFORMACIÓN	0%
A.5.1.2 REVISIÓN DE LAS POLÍTICAS PARA LA SEGURIDAD DE LA INFORMACIÓN	0%
A.6 ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	
A.6.1 ORGANIZACION INTERNA	
A.6.1.1 ROLES Y RESPONSABILIDADES EN SEGURIDAD DE LA INFORMACIÓN	0%
A.6.1.2 SEGREGACIÓN DE TAREAS	0%
A.6.1.3 CONTACTO CON LAS AUTORIDADES	20%
A.6.1.4 CONTACTO CON GRUPOS DE INTERÉS ESPECIAL	0%
A.6.1.5 SEGURIDAD DE LA INFORMACIÓN EN LA GESTIÓN DE PROYECTOS	0%
A.6.2 LOS DISPOSITIVOS MÓVILES Y EL TELETRABAJO	
A.6.2.1 POLÍTICA DE DISPOSITIVOS MÓVILES	0%
A.6.2.2 TELETRABAJO	0%
A.7 SEGURIDAD RELATIVA A LOS RECURSOS HUMANOS	
A.7.1. ANTES DEL EMPLEO	
A.7.1.1 INVESTIGACIÓN DE ANTECEDENTES	0%
A.7.1.2 TÉRMINOS Y CONDICIONES DEL EMPLEO	80%
A.7.2 DURANTE EL EMPLEO	
A.7.2.1 RESPONSABILIDADES DE GESTIÓN	20%
A.7.2.2 CONCIENCIACIÓN, EDUCACIÓN Y CAPACITACIÓN EN SEGURIDAD DE LA INFORMACIÓN	0%
A.7.2.3 PROCESO DISCIPLINARIO	0%
A.7.3 FINALIZACIÓN DEL EMPLEO O CAMBIO EN EL PUESTO DE TRABAJO	
A.7.3.1 RESPONSABILIDADES ANTE LA FINALIZACIÓN O CAMBIO	20%
A.8 GESTIÓN DE ACTIVOS	
A.8.1 RESPONSABILIDAD SOBRE LOS ACTIVOS	
A.8.1.1 INVENTARIO DE ACTIVOS	20%
A.8.1.2 PROPIEDAD DE LOS ACTIVOS	20%
A.8.1.3 USO ACEPTABLE DE LOS ACTIVOS	0%
A.8.1.4 DEVOLUCIÓN DE ACTIVOS	20%
A.8.2 CLASIFICACIÓN DE LA INFORMACIÓN	
A.8.2.1 CLASIFICACIÓN DE LA INFORMACIÓN	0%
A.8.2.2 ETIQUETADO DE LA INFORMACIÓN	0%
A.8.2.3 MANIPULADO DE LA INFORMACIÓN	0%
A.8.3 MANIPULACIÓN DE LOS SOPORTES	
A.8.3.1 GESTIÓN DE SOPORTES EXTRAIBLES	0%
A.8.3.2 ELIMINACIÓN DE SOPORTES	40%
A.8.3.3 SOPORTES FÍSICOS EN TRÁNSITO	0%
A.9 CONTROL DE ACCESO	
A.9.1. REQUISITOS DE NEGOCIO PARA EL CONTROL DE ACCESO	

A.9.1.1 POLÍTICA DE CONTROL DE ACCESO	0%
A.9.1.2 ACCESO A LAS REDES Y A LOS SERVICIOS DE RED	40%
A.9.2 GESTIÓN DE ACCESO DE USUARIO	
A.9.2.1 REGISTRO Y BAJA DE USUARIO	40%
A.9.2.2 PROVISIÓN DE ACCESO DE USUARIO	40%
A.9.2.3 GESTIÓN DE PRIVILEGIOS DE ACCESO	40%
A.9.2.4 GESTIÓN DE LA INFORMACIÓN SECRETA DE AUTENTICACIÓN DE LOS USUARIOS	0%
A.9.2.5 REVISIÓN DE LOS DERECHOS DE ACCESO DE USUARIO	0%
A.9.2.6 RETIRADA O REASIGNACIÓN DE LOS DERECHOS DE ACCESO	40%
A.9.3 RESPONSABILIDADES DEL USUARIO	
A.9.3.1 USO DE LA INFORMACIÓN SECRETA DE LA AUTENTICACIÓN	0%
A.9.4 CONTROL DE ACCESO A SISTEMAS Y APLICACIONES	
A.9.4.1 RESTRICCIÓN DEL ACCESO A LA INFORMACIÓN	40%
A.9.4.2 PROCEDIMIENTOS SEGUROS DE INICIO DE SESIÓN	40%
A.9.4.3 SISTEMA DE GESTIÓN DE CONTRASEÑAS	60%
A.9.4.4 USO DE UTILIDADES CON PRIVILEGIOS DEL SISTEMA	0%
A.9.4.5 CONTROL DE ACCESO AL CÓDIGO FUENTE DE PROGRAMAS	40%
A.10 CRIPTOGRAFÍA	
A.10.1 CONTROLES CRIPTOGRÁFICOS	
A.10.1.1 POLÍTICA DE USO DE LOS CONTROLES CRIPTOGRÁFICOS	0%
A.10.1.2 GESTION DE CLAVES	20%
A.11 SEGURIDAD FÍSICA Y DEL ENTORNO	
A.11.1 ÁREAS SEGURAS	
A.11.1.1 PERÍMETRO DE SEGURIDAD FÍSICA	40%
A.11.1.2 CONTROLES FÍSICOS DE ENTRADA	60%
A.11.1.3 SEGURIDAD DE OFICINAS, DESPACHOS Y RECURSOS	60%
A.11.1.4 PROTECCIÓN CONTRA LAS AMENAZAS EXTERNAS Y AMBIENTALES	0%
A.11.1.5 EL TRABAJO EN ÁREAS SEGURAS	0%
A.11.1.6 ÁREAS DE CARGA Y DESCARGA	0%
A.11.2 SEGURIDAD DE LOS EQUIPOS	
A.11.2.1 EMPLAZAMIENTO Y PROTECCIÓN DE EQUIPOS	20%
A.11.2.2 INSTALACIONES DE SUMINISTRO	40%
A.11.2.3 SEGURIDAD DEL CABLEADO	40%
A.11.2.4 MANTENIMIENTO DE LOS EQUIPOS	0%
A.11.2.5 RETIRADA DE MATERIALES PROPIEDAD DE LA EMPRESA	0%
A.11.2.6 SEGURIDAD DE LOS EQUIPOS FUERA DE LAS INSTALACIONES	0%
A.11.2.7 REUTILIZACIÓN O ELIMINACIÓN SEGURA DE EQUIPOS	0%
A.11.2.8 EQUIPO DE USUARIO DESATENDIDO	40%
A.11.2.9 POLÍTICA DE PUESTO DE TRABAJO DESPEJADO Y PANTALLA LIMPIA	40%
A.12 SEGURIDAD DE LAS OPERACIONES	
A.12.1 PROCEDIMIENTOS Y RESPONSABILIDADES OPERACIONALES	

A.12.1.1 PROCEDIMIENTOS OPERACIONALES DOCUMENTADOS	0%
A.12.1.2 GESTION DE CAMBIOS	0%
A.12.1.3 GESTION DE LA CAPACIDAD	0%
A.12.1.4 SEPARACION DE LOS ENTORNOS DE DESARROLLO, TEST Y OPERACIONES	40%
A.12.2 PROTECCION CONTRA SOFTWARE MALICIOSO	
A.12.2.1 CONTROLES CONTRA EL CÓDIGO MALICIOSO	40%
A.12.3 COPIAS DE SEGURIDAD	
A.12.3.1 COPIAS DE SEGURIDAD DE LA INFORMACION	40%
A.12.4 REGISTROS Y SUPERVISIÓN	
A.12.4.1 REGISTRO DE EVENTOS	0%
A.12.4.2 PROTECCION DE LA INFORMACION DE LOS REGISTROS	40%
A.12.4.3 REGISTROS DE ADMINISTRADOR Y OPERADOR	0%
A.12.4.4 SINCRONIZACION DE RELOJES	40%
A.12.5 CONTROL DEL SOFTWARE EN EXPLOTACIÓN	
A.12.5.1 INSTALACIÓN DE SOFTWARE EN SISTEMAS DE PRODUCCIÓN	40%
A.12.6 GESTION DE LA VULNERABILIDAD TECNICA	
A.12.6.1 CONTROL DE VULNERABILIDADES TECNICAS	0%
A.12.6.2 RESTRICCIONES DE LA INSTALACIÓN DE SOFTWARE	20%
A.12.7 CONSIDERACIONES EN LA AUDITORIA DE SISTEMAS DE INFORMACION	
A.12.7.1 CONTROLES DE LA AUDITORIA DE LOS SISTEMAS DE INFORMACION	0%
A.13 SEGURIDAD DE LAS COMUNICACIONES	
A.13.1 GESTION DE LA SEGURIDAD DE REDES	
A.13.1.1 CONTROLES DE RED	40%
A.13.1.2 SEGURIDAD DE LOS SERVICIOS DE RED	40%
A.13.1.3 SEGREGACION EN REDES	60%
A.13.2 INTERCAMBIO DE INFORMACION	
A.13.2.1 POLITICAS Y PROCEDIMIENTOS DE INTERCAMBIO DE INFORMACION	0%
A.13.2.2 ACUERDOS DE INTERCAMBIO DE INFORMACIÓN	40%
A.13.2.3 MENSAJERIA ELECTRONICA	0%
A.13.2.4 ACUERDOS DE CONFIDENCIALIDAD O NO DIVULGACIÓN	40%
A.14 ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACION	
A.14.1 REQUISITOS DE SEGURIDAD EN SISTEMAS DE INFORMACION	
A.14.1.1 ANALISIS Y ESPECIFICACION DE REQUISITOS DE SEGURIDAD DE LA INFORMACIÓN	0%
A.14.1.2 SEGURIDAD DE SERVICIOS DE APLICACIÓN EN REDES PÚBLICAS	0%
A.14.1.3 PROTECCIÓN DE TRANSCCIONES DE SERVICIOS DE APLICACIONES	0%
A.14.2 SEGURIDAD EN LOS PROCESOS DE DESARROLLO Y SOPORTE	
A.14.2.1 POLITICA DE DESARROLLO SEGURO	0%
A.14.2.2 PROCEDIMIENTOS DE CONTROL DE CAMBIOS DEL SISTEMA	20%
A.14.2.3 REVISION TECNICA DE LAS APLICACIONES TRAS CAMBIOS EN EL SISTEMA OPERATIVO	40%
A.14.2.4 RESTRICCIONES A LOS CAMBIOS EN LOS PAQUETES DE SOFTWARE	0%

A.14.2.5 PRINCIPIOS DE INGENIERÍA DE SISTEMAS SEGUROS	20%
A.14.2.6 ENTORNO DE DESARROLLO SEGURO	20%
A.14.2.7 EXTERNALIZACIÓN DEL DESARROLLO SOFTWARE	20%
A.14.2.8 PRUEBAS DE SEGURIDAD DEL SISTEMA	0%
A.14.2.9 PRUEBAS DE ACEPTACION DEL SISTEMA	0%
A.14.3 DATOS DE PRUEBA	
A.14.3.1 PROTECCION DE LOS DATOS DE PRUEBA	0%
A.15 RELACION CON PROVEEDORES	
A.15.1 SEGURIDAD EN LAS RELACIONES CON PROVEEDORES	
A.15.1.1 POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN PARA LAS RELACIONES CON PROVEEDORES	0%
A.15.1.2 ABORDAR LA SEGURIDAD DENTRO DE LOS ACUERDOS CON PROVEEDORES	40%
A.15.1.3 CADENA DE SUMINISTRO TIC	40%
A.15.2 GESTION DE LA PROVISIÓN DE SERVICIOS DEL PROVEEDOR	
A.15.2.1 MONITORIZACION Y REVISION DE SERVICIOS DEL PROVEEDOR	20%
A.15.2.2 GESTION DE CAMBIOS A SERVICIOS DEL PROVEEDOR	0%
A.16 GESTION DE INCIDENTES DE SEGURIDAD DE LA INFORMACION	
A.16.1 GESTION DE INCIDENTES DE SEGURIDAD DE LA INFORMACION Y MEJORAS	
A.16.1.1 RESPONSABILIDADES Y PROCEDIMIENTOS	0%
A.16.1.2 NOTIFICACIÓN DE LOS EVENTOS DE SEGURIDAD DE LA INFORMACION	20%
A.16.1.3 NOTIFICACIÓN DE LOS PUNTOS DÉBILES DE LA SEGURIDAD	0%
A.16.1.4 EVALUACIÓN Y DECISIÓN SOBRE LOS EVENTOS DE SEGURIDAD DE LA INFORMACIÓN	0%
A.16.1.5 RESPUESTA A INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	0%
A.16.1.6 APRENDIZAJE DE LOS INCIDENTES DE SEGURIDAD DE LA INFORMACION	0%
A.16.1.7 RECOPILACIÓN DE EVIDENCIAS	20%
A.17 ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN PARA LA GESTION DE LA CONTINUIDAD DEL NEGOCIO	
A.17.1 CONTINUIDAD DE LA SEGURIDAD DE LA INFORMACION	
A.17.1.1 PLANIFICACIÓN LA CONTINUIDAD DE LA SEGURIDAD DE LA INFORMACIÓN	0%
A.17.1.2 IMPLEMENTAR LA CONTINUIDAD DE LA SEGURIDAD DE LA INFORMACION	0%
A.17.1.3 VERIFICACIÓN, REVISIÓN Y EVALUACIÓN DE LA CONTINUIDAD DE LA SEGURIDAD DE LA INFORMACIÓN	0%
A.17.2 REDUNDANCIAS	
A.17.2.1 DISPONIBILIDAD DE LOS RECURSOS DE TRATAMIENTO DE LA INFORMACIÓN	40%
A.18 CUMPLIMIENTO	
A.18.1 CUMPLIMIENTO DE LOS REQUISITOS LEGALES Y CONTRACTUALES	
A.18.1.1 IDENTIFICACION DE LA LEGISLACION APLICABLE Y REQUISITOS CONTRACTUALES	0%
A.18.1.2 DERECHOS DE PROPIEDAD INTELECTUAL	0%
A.18.1.3 PROTECCION DE LOS REGISTROS DE LA ORGANIZACIÓN	0%
A.18.1.4 PROTECCION Y PRIVACIDAD DE LA INFORMACIÓN DE CARÁCTER PERSONAL	20%
A.18.1.5 REGULACION DE LOS CONTROLES CRIPTOGRAFICOS	0%

A.18.2 REVISIONES DE SEGURIDAD DE LA INFORMACIÓN	
A.18.2.1 REVISION INDEPENDIENTE DE LA SEGURIDAD DE LA INFORMACION	0%
A.18.2.2 CUMPLIMIENTO DE LAS POLITICAS Y NORMAS DE SEGURIDAD	0%
A.18.2.3 COMPROBACIÓN DEL CUMPLIMIENTO TÉCNICO	20%

Ilustración 1: Resultado análisis diferencial ISO 27002:2013.

ANEXO III - DOCSEC001

Política de Seguridad

CONECTA BUS S.L

Tabla de contenido

1. Objeto

El objeto del presente documento es el de responder a la necesidad de Conecta Bus S.L de redactar un documento que recoja y defina las Políticas de Seguridad de la Información para el SGSI.

En este documento se redacta la política de seguridad de la compañía enmarcada en la norma internacional ISO/IEC 27001.

2. Alcance

La política de seguridad es de aplicación a todo el personal y activos de Conecta Bus S.L, la dirección es responsable de ponerla en su conocimiento y de comunicarla a todas las partes interesadas.

3. Políticas de Seguridad

3.1. Acuerdo de confidencialidad

La compañía exigirá la firma de un acuerdo de confidencialidad a sus empleados, empresas proveedoras y otros usuarios que deban tener acceso a información sensible o interna, en el momento que se inicie su relación contractual u operativa.

3.2. Uso de los activos de la compañía

No se podrá hacer uso de los activos de la compañía para fines ajenos a la compañía, salvo que exista autorización explícita del responsable del activo.

3.3. Baja de usuarios

Cuando se produzca una baja en la compañía, se deberá notificar al departamento de RRHH e IT para que sigan el procedimiento de seguridad establecido, retirando todos los accesos al usuario.

3.4. Uso de credenciales

Los accesos a los sistemas de información de la compañía se conceden de forma nominal. Cada usuario es responsable de proteger su contraseña e impedir que otra persona pueda hacer uso de ella.

No está permitido hacer uso de credenciales ajenas o difundir las credenciales propias a otros miembros de la compañía.

3.5. Mesas vacías

Todo el personal deberá cumplir con la política de mesas vacías donde cada empleado es responsable de mantener su puesto de trabajo limpio y sin ninguna información de ningún tipo a simple vista.

3.6. Acceso remoto

Todo acceso remoto deberá ser aprobado por el responsable de IT.

Únicamente se permite acceso remoto a la red de Conecta Bus S.L mediante soluciones de seguridad certificadas y aprobadas por el departamento de TI.

3.7. Acceso a recursos telemáticos

Los accesos a la información de la compañía deberán ser solicitados al departamento de IT y dicha solicitud deberá ir acompañada una autorización del responsable del departamento propiedad del recurso.

El responsable del departamento de IT se guarda la última palabra para permitir o denegar dicho acceso.

3.8. Formación

Empleados y proveedores serán formados e informados en relación con la política de seguridad y procedimientos internos de la compañía.

El personal de la compañía dispondrá en todo momento de información publicada en la intranet relativa a las políticas de seguridad definidas en la compañía.

3.9. Gestión de incidentes de seguridad

Los incidentes de seguridad relevantes serán tratados por el director de TI y el responsable de seguridad de la información.

Se tratarán como incidentes de seguridad todo incumplimiento de la política de seguridad, mal uso de sistemas de información y comportamientos que pongan en riesgo la seguridad. Los empleados deben reportar los incidentes de seguridad.

ANEXO IV - DOCSEC002

Procedimiento de Auditorías Internas

CONECTA BUS S.L

Tabla de contenido

1. Objeto

El objeto del presente documento es el de responder a la necesidad de Conecta Bus S.L para establecer un procedimiento de auditoria interna a llevar a cabo en la compañía.

Este documento incluye planificación de las auditorias, requisitos que establecerán los auditores internos y el modelo de informe final de la auditoría.

2. Alcance

El procedimiento aplica a las auditorías internas que se realicen en el marco del Sistema de Gestión de la Seguridad de la Información de la Compañía.

3. Plan de auditoría

Para poder realizar una auditoría interna se requiere de un plan de auditoría. Este plan de auditoría es definido por el responsable de seguridad de la información de la compañía y en el se definen los elementos o departamentos que van a ser auditados.

Para las auditorías internas **se establece una periodicidad anual**, quedando abierta la posibilidad de realizar auditorias excepcionales donde se indicaría al departamento o grupo afectado el motivo y alcance de la auditoría.

El plan de auditoría detallará el equipo que llevará a cabo la auditoría interna. El personal puede ser propio o externo a la compañía, pero en ambos casos deberá mostrar independencia con los procesos a auditar.

3.1 Realización de la auditoría

La realización de las auditorías internas tiene como objetivo conocer el grado de cumplimiento del SGSI con respecto a la norma ISO/IEC 27001. Para ello, **se realizará anualmente la revisión de -todos- los controles de la norma ISO2700**.

Para cumplir con los objetivos fijados para las auditorias, será necesario que exista cooperación total por parte del personal implicado facilitando la documentación que se requiera y atendiendo los requisitos que solicite el equipo auditor.

En el caso de necesitar acceso a entornos de producción por parte del equipo auditor se acompañará siempre a los miembros del grupo por un responsable de IT para que no afecte a la continuidad del negocio.

Durante la auditoría, el equipo auditor realizará reuniones con las diferentes áreas convocadas para entrevistar al personal implicado con el objetivo de obtener la información o documentación que considere necesarios para la realización de la auditoría. Las fechas de dichas entrevistas serán previamente acordadas con el auditado.

El equipo auditor mantendrá una reunión final con el auditado para comentar las no conformidades encontradas.

3.2 Resultado de auditoría

A la finalización de la auditoría, el equipo auditor entregará un informe final dejando de forma clara y explícita las no conformidades detectadas respecto a la norma, así como los puntos de mejora detectados u observaciones.

El informe final de la auditoría deberá contener al menos los siguientes ítems:

Los informes de auditoría deberán recoger diversa información como:

- Fecha de auditoría
- Compañía auditada
- Equipo auditor
- Áreas y personal auditados
- Objetivos de la auditoría
- El alcance y la norma de referencia
- Conformidad del SGSI con la norma
- No conformidades detectadas en el proceso
- Resumen final y Conclusiones de la auditoría

Una vez entregado el informe de la auditoría este será analizado por el comité de seguridad a fin de establecer un plan de acción a llevar a cabo para solucionar las no conformidades, si las ha habido, los puntos identificados como mejora y las observaciones realizadas.

3.3 Equipo auditor

El equipo auditor que se encargue de la ejecución de la auditoría deberá cumplir con los siguientes requisitos:

- Deben de existir independencia, con lo que no podrían haber formado parte del trabajo que se está auditando.

- Deben de estar cualificados en la materia, es decir, deben de estar formados en el sistema de auditoría además de tener experiencia en el campo de la seguridad de información.

ANEXO V - DOCSEC003

Gestión de Indicadores

CONECTA BUS S.L

Tabla de contenido

1. Objeto

El objeto del presente documento es el de responder a la necesidad de Conecta Bus S.L para definir los indicadores para medir la eficacia de los controles de seguridad implantados.

2. Alcance

Los indicadores recogidos en este documento aplican a los controles del SGSI, correspondientes a la norma ISO/IEC 27002:2013.

3. Definición de indicadores

Se definen indicadores para medir la eficacia de los controles de seguridad implantados.

CONTROL	OBJETIVO	FRECUENCIA	TOLERANCIA
5.1.2 Revisión de las políticas para la seguridad de la información	Verificar que las políticas de seguridad son revisadas anualmente.	Anual	1 revisión anual
6.2.2 Teletrabajo	Verificar que los empleados firman y cumplen con la política de teletrabajo	Anual	80% de empleados
7.1.2 Términos y condiciones del empleo	Existencia de contratos de confidencialidad firmados para todos los empleados y proveedores de la compañía.	Anual	100% acuerdos firmados
8.1.1 Inventario de activos	Existe un inventario de activo que se actualiza de forma anual.	Anual	90% actualizado
8.1.4 Devolución de activos	Verificar que todos los responsables de activos están dados de alta como empleados.	Anual	100% se cumple.
9.2 Gestión de acceso de usuario	Se verifica que se cumple el proceso formal de altas y bajas en la compañía	Trimestral	Actualizado máx 6 meses
11.1.3 Seguridad de oficinas, despachos y recursos	Los accesos a la oficina, a los despachos y a los recursos se encuentra documentado.	Mensual	Actualizado máx 2 meses
11.2.9 Política de puesto de trabajo despejado y pantalla limpia	No se encuentran documentos confidenciales en las mesas a simple vista	Trimestral	3 puestos incumplidos
12.3.1 Copias de seguridad de la información	Se ejecutan los trabajos de backup declarados en el documento de backup de la compañía.	Mensual	95% de los trabajos se ejecutan.

14.2.3 Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo	Cada actualización documentada lleva consigo un test de pruebas definido	Trimestral	3 actualizaciones sin test de pruebas
18.1.4 Protección y privacidad de la información de carácter personal	En los contratos de los empleados y proveedores existen clausulas y condiciones relativas a la protección de datos de carácter personal.	Anual	100% de los contratos dispone de las clausulas.

Ilustración 1: Indicadores definidos en la compañía.

ANEXO VI - DOCSEC004

Procedimiento Revisión por Dirección

CONECTA BUS S.L

Tabla de contenido

1. Objeto

El objeto del presente documento es el de responder a la necesidad de Conecta Bus S.L para describir la revisión anual que debe ser realizada por la Dirección.

2. Alcance

El alcance del presente documento contempla el SGSI de la compañía.

3. Revisión

Para el correcto funcionamiento del SGSI, la Dirección de la compañía debe formar parte de las revisiones y decisiones que se tomen con relación al mismo.

La revisión debe servir para comprobar que se han obtenido los objetivos fijados y analizar las oportunidades de mejora identificadas y las necesidades de cambio en el SGSI, incluyendo la política y los objetivos de seguridad de la información.

Los puntos de entrada que serán tratados en las reuniones son:

- Resultados de auditorías y revisiones de SGSI.
- Comentarios recogidos de forma interna sobre el SGSI.
- Vulnerabilidades o amenazas no abordadas en la evaluación de riegos anterior.
- Cumplimiento de los objetivos de seguridad de la información.
- Estado de las acciones realizadas desde la última revisión de la Dirección.
- Actualización de la política de seguridad.
- Cambios que pudiesen afectar el SGSI;
- Oportunidades y mejoras detectadas

Las entradas presentadas en la reunión deben ser revisadas por la Dirección que emitirá un informe donde se recogerá cualquier decisión o acción tomada, acompañado con el acta de la reunión.

Los puntos de salida de dicho informen recogerán:

- Mejoras para el funcionamiento del SGSI.
- Actualización de la evaluación de riesgos y nuevo plan de tratamiento de riesgos.
- Modificación de los procedimientos o políticas de seguridad.
- Mejora en las métricas de los controles.

ANEXO VII - DOCSEC005

Gestión de Roles y Responsabilidades

CONECTA BUS S.L

Tabla de contenido

1. Objeto

El objeto del presente documento es el de responder a la necesidad de Conecta Bus S.L para definir los roles y responsabilidades del personal relacionado con el Sistema de Gestión de Seguridad de la Información.

2. Alcance

Los roles y responsabilidades que se definan en el presente documento serán de aplicación para todo el personal de la compañía que tenga relación con el SGSI.

3. Modelo organizativo

A continuación, se define de forma detallada los distintos roles y responsabilidades encargados de gestionar el SGSI de la compañía. Es de vital importancia conocer las distintas funciones que están asociadas al SGSI y saber en todo momento de forma unívoca quien es el responsable de que estas funciones se lleven a cabo.

3.1 Comité de Dirección

El comité de dirección de la compañía está formado por:

- Director General.
- Jefe de operaciones.
- Responsable de recursos humanos.
- Responsable de marketing.
- Jefe del departamento IT.
- Responsable de contabilidad y asesoría legal.

Las funciones del Comité de Dirección son:

- Hacer de la seguridad de la información un punto de la agenda del Comité de Dirección de la compañía.
- Nombrar a los miembros de un Comité de Seguridad de la Información y darles soporte, dotarlo de los recursos necesarios y establecer sus directrices de trabajo.
- Aprobar la política, normas y responsabilidades generales en materia de seguridad de la información.
- Determinar el umbral de riesgo aceptable en materia de seguridad.

- Analizar posibles riesgos introducidos por cambios en las funciones o funcionamiento de la compañía para adoptar las medidas de seguridad más adecuadas.
- Aprobar el Plan de seguridad de la información, que recoge los principales proyectos e iniciativas en la materia.
- Realizar el seguimiento del cuadro de mando de la seguridad de la información.

3.2 Comité de Seguridad

El comité de seguridad de la compañía está formado por:

- Director General.
- Jefe de operaciones.
- Responsable de recursos humanos.
- Responsable de marketing.
- Jefe del departamento IT.
- Responsable de contabilidad y asesoría legal.

Las funciones del Comité de Dirección son:

- Implantar las directrices del Comité de Dirección.
- Asignar roles y funciones en materia de seguridad.
- Presentar a aprobación al Comité de Dirección las políticas, normas y responsabilidades en materia de seguridad de la información.
- Validar el mapa de riesgos y las acciones de mitigación propuestas por el responsable de seguridad de la información (RSI).
- Validar el Plan de seguridad de la información o Plan director de seguridad de la información y presentarlo a aprobación al Comité de Dirección. Supervisar y hacer el seguimiento de su implantación.
- Supervisar y aprobar el desarrollo y mantenimiento del Plan de continuidad de negocio.
- Velar por el cumplimiento de la legislación que en materia de seguridad sea de
- aplicación.
- Promover la concienciación y formación de usuarios y liderar la comunicación necesaria.
- Revisar las incidencias más destacadas.
- Aprobar y revisar periódicamente el cuadro de mando de la seguridad de la información y de la evolución del SGSI.

3.3 Responsable de seguridad de la información (RSI)

La designación de un responsable de seguridad de la información (RSI) es la única vía para avanzar de forma organizada y paulatina en seguridad de la información, ya que garantiza que hay alguien para quien la seguridad de la información es una prioridad.

La compañía cuenta con un responsable de seguridad IT en el departamento de IT cuyas funciones son:

- Implantar las directrices del Comité de Seguridad de la Información de la compañía.
- Elaborar, promover y mantener una política de seguridad de la información, y proponer anualmente objetivos en materia de seguridad de la información.
- Desarrollar y mantener el documento de Organización de la seguridad de la información en colaboración con el área de Organización/RR. HH., en el cual se recogerá quien asume cada una de las responsabilidades en seguridad, así como una descripción detallada de funciones y dependencias.
- Desarrollar, con el soporte de las unidades correspondientes, el marco normativo de seguridad y controlar su cumplimiento.
- Actuar como punto focal en materia de seguridad de la información dentro de la compañía, lo cual incluye la coordinación con otras unidades y funciones (seguridad física, prevención, emergencias, relaciones con la prensa...), a fin de gestionar la seguridad de la información de forma global.
- Promover y coordinar entre las áreas de negocio el análisis de riesgos de los procesos más críticos e información más sensible, y proponer acciones de mejora y mitigación del riesgo, de acuerdo con el umbral aceptable definido por el Comité de Dirección. Elevar el mapa de riesgos y el Plan de seguridad de la información al CSI.
- Controlar la gestión de riesgos de nuevos proyectos y velar por el desarrollo seguro de aplicaciones.
- Revisar periódicamente el estado de la seguridad en cuestiones organizativas, técnicas o metodológicas. Esta revisión ha de permitir proponer o actualizar el Plan de seguridad de la información, incorporando todas las acciones preventivas, correctivas y de mejora que se hayan ido detectando. Una vez aprobado dicho plan y el presupuesto por el CSI, el RSI deberá gestionar el presupuesto asignado y la contratación de recursos cuando sea necesario.
- Coordinar acciones con las áreas de negocio para elaborar y gestionar un Plan de continuidad de negocio de la compañía, basado en el análisis de riesgo y la criticidad de los procesos de negocio, y la determinación del impacto en caso de materialización del riesgo.

- Velar por el cumplimiento legal (LOPD, RD 3/2010 Esquema Nacional de Seguridad, Basilea, SOX...), coordinando las actuaciones necesarias con las unidades responsables.
- Definir la arquitectura de seguridad de los sistemas de información, monitorizar la seguridad a nivel tecnológico (gestión de trazas, vulnerabilidades, cambios...), hacer el seguimiento de los incidentes de seguridad y escalarlos al CSI si corresponde.
- Elaborar y mantener un plan de concienciación y formación en seguridad de la información del personal, en colaboración con la unidad responsable de la formación en la compañía.
- Hacer seguimiento y revisar los incidentes de seguridad, escalándolos al CSI si corresponde.
- Coordinar la implantación de herramientas y controles de seguridad de la información y definir el cuadro de mando de la seguridad. El RSI debe analizar y mantener actualizado dicho cuadro de mando, presentándolo al CSI con la periodicidad que se establezca.

3.4 Personal en General

En este grupo se engloba toda aquella persona profesional que no esté incluida en las categorías de responsables o dirección de la empresa.

Sus funciones y responsabilidades son:

- Mantener la confidencialidad de la información.
- Hacer un buen uso de los equipos y de la información a la cual tienen acceso y protegerla de accesos no autorizados.
- Respetar las normas y procedimientos vigentes en materia de seguridad de la
- información, y velar por que terceras partes en prestación de servicios también la respeten.
- Utilizar adecuadamente las credenciales de acceso a los sistemas de información.
- Respetar la legislación vigente en materia de protección de datos de carácter personal y cualquier otra que sea de aplicación.
- Notificar, por la vía establecida, insuficiencias, anomalías o incidentes de seguridad y situaciones sospechosas que pudieran poner en peligro la seguridad de la información.

3.5 Área de Tecnologías de la Información y Comunicaciones (TIC)

El Jefe del departamento de TI de la compañía es una de las personas más implicadas en el desarrollo del SGSI. Además de ser reportado por el RSI, tiene las siguientes funciones y responsabilidades:

- Cumplir con las políticas, normas y procedimientos en materia de seguridad de la información. Colaborar con el RSI en su definición.
- Implantar en los sistemas de información los controles de seguridad prescritos, las acciones correctoras establecidas y gestionar las vulnerabilidades detectadas.
- Requerir la participación del RSI en nuevos proyectos de desarrollo o adaptación/implantación de productos de mercado, especialmente cuan- do puedan ser críticos en términos de confidencialidad, privacidad, integridad, continuidad, autenticidad, no repudio y trazabilidad, o puedan tener un impacto mediático importante.
- Requerir la participación del RSI en la implantación o gestión de los cambios de hardware y software.
- Garantizar la inclusión de la seguridad en todo el ciclo de vida de los datos: creación, mantenimiento, conservación y destrucción, y en los procesos de gestión de hardware y software.
- Adoptar medidas para proteger la información según su clasificación por parte del responsable de la información.
- Colaborar con el RSI en la identificación de riesgos y la propuesta de soluciones, y colaborar en las revisiones o auditorías de seguridad que se lleven a cabo.

3.6 Área de RR. HH.

Existe la figura de un responsable de Recursos Humanos cuyas funciones son:

- Informar a las unidades gestoras de recursos de información sobre cambios / movimientos de personal para poder realizar una buena gestión de recursos: altas, bajas definitivas y temporales, cambios de categoría y/o funciones, cambios organizativos, etc.
- Trabajar juntamente con el RSI en el desarrollo de la política de seguridad de la información en los temas referentes al personal.
- Aplicar procedimientos disciplinarios en caso de vulneración del marco normativo.

3.7 Área de Asesoría Jurídica y Contabilidad

Existe la figura de un responsable de contabilidad y asesoría legal cuyas funciones son:

- Colaborar con el RSI en la emisión de nuevas políticas y normas de seguridad y en la investigación y resolución de incidentes de seguridad cuan do se puedan derivar acciones legales (reclamaciones de terceras partes, acciones contra un trabajador...).

- Colaborar con el RSI en la definición de cláusulas específicas de seguridad de la información, e incluirlas en los contratos con terceras partes y contratos de personal externo.
- Informar al RSI de nueva legislación o cambios en la legislación aplicable, que pudieran tener impacto sobre la seguridad de la información, dando soporte en su interpretación.

ANEXO VIII - DOCSEC006

Metodología de Análisis de Riesgos

CONECTA BUS S.L

Tabla de contenido

1. Objeto

El objeto del presente documento es el de responder a la necesidad de Conecta Bus S.L para definir la metodología empleada en los análisis de riesgos.

2. Alcance

La metodología definida en el presente documento será aplicada en los análisis de riesgos que se realicen con relación al SGSI de la compañía.

3. Análisis de riesgos

La primera y principal tarea que se realiza cuando se quiere mejorar cualquier aspecto de la seguridad de la información es la realización de un análisis de riesgos.

Las metodologías empleadas para realizar los análisis de riesgos trabajan sobre los siguientes elementos:

- Activos: elementos que deben protegerse.
- Amenazas: situaciones de las que deben protegerse los activos.
- Vulnerabilidades: aspectos que facilitan la materialización de las amenazas.
- Impactos: consecuencias que se producen cuando una amenaza aprovecha una vulnerabilidad para dañar un activo.

A partir de estos elementos, las organizaciones estiman los riesgos a los que se encuentra expuesta la organización. Estos riesgos son tratados en el proceso de gestión de los riesgos.

4. Metodología: MAGERIT

Magerit es una metodología de análisis de riesgos elaborada por el Ministerio de Administraciones Públicas con el fin de ayudar a las administraciones públicas españolas a mejorar diversos aspectos. Su característica fundamental es que los riesgos que se plantean para una organización se expresan en valores económicos directamente.

Esta metodología presenta una guía completa, paso a paso de como llevar a cabo el análisis de riesgos.

4.1 Fases de la metodología Magerit

La metodología Magerit esta compuesta por las siguientes fases:

1) **Toma de datos. Proceso de información**

En esta primera fase tiene como objetivos:

- Definir el alcance que se ha de estudiar o analizar.
- Analizar los procesos de la organización.
- Establecer el nivel de granularidad en el análisis.

2) **Establecimiento de parámetros**

Consiste en el establecimiento de los parámetros que se utilizan durante todo el proceso de análisis de riesgos.

Los parámetros que deben ser identificados son:

- Valor de los activos.
- Vulnerabilidad.
- Impacto.
- Efectividad del control de seguridad.

El **valor de los activos** tiene como objetivo asignar una valoración económica a todos los activos de una organización que se pretenden analizar. Los valores que se han de tener en cuenta para cada activo son:

- Valor de reposición.
- Valor de configuración.
- Valor de uso del activo.
- Valor de perdida de oportunidad.

La **vulnerabilidad** se entiende como una frecuencia de ocurrencia de una amenaza. Esta frecuencia se define en una escala de valores que puede ser calculada con la siguiente fórmula:

Vulnerabilidad = Frecuencia estimada / Días del año

Se entiende por **impacto** el tanto por ciento del valor del activo que se pierde en el caso de que suceda un incidente sobre él.

El parámetro **Efectividad del control de seguridad** consiste en ver la influencia que tendrán las medidas de protección antes los riesgos que vamos a detectar.

3) **Análisis de activos**

El objetivo de esta fase del estudio es identificar cuáles son los activos que posee la organización y que necesita para llevar a cabo sus actividades. Los activos analizables son:

- Activos físicos.
- Activos lógicos.
- Activos de personal.

- Activos de entorno infraestructura.
- Activos intangibles.

4) Análisis de amenazas

Una amenaza son aquellas situaciones que podrían llegar a darse en una organización y que desembocarían en un problema de seguridad.

MAGERIT clasifica las amenazas que pueden afectar a una organización en cuatro grandes grupos:

- Accidentes: Son aquellas situaciones no provocadas.
- Errores: Son aquellas situaciones que son cometidas de forma involuntaria.
- Amenazas intencionales presenciales: Son las provocadas por el propio personal de la organización de forma voluntaria.
- Amenazas intencionales remotas: Amenazas provocadas por terceras personas, es decir, por personas ajenas a nuestra organización y que consiguen dañarla.

5) Establecimiento de las vulnerabilidades

Esta fase definida en la metodología Magerit tiene como objetivo analizar las vulnerabilidades que existen.

6) Establecimiento de impactos

Esta fase definida en la metodología Magerit tiene como objetivo identificar los posibles impactos que pueden producirse en la organización.

7) Análisis de riesgos

En esta fase se realiza el estudio de los riesgos actuales a los que está sometida la organización. Para calcular los riesgos se usa la siguiente fórmula:

Riesgos = Valor del activo x Vulnerabilidad x Impacto

En este punto habiendo obtenido el valor del riesgo, la compañía deberá decidir el rango de riesgo aceptable para la misma.

NOTA: En el año 2019, la Dirección de la compañía fija tras analizar la situación, el *apetito de riesgo en 0,1*. Cualquier riesgo por debajo de este valor, se considerará aceptable.

8) Influencia de las salvaguardas

Una vez que tenemos identificados los riesgos actuales a los que se encuentra expuesta la organización, se entra en la fase de gestión de riesgos, que consiste en tratar de escoger la mejor solución de seguridad que me permita reducirlos.

Para ello existen dos tipos fundamentales de controles de seguridad o salvaguardas:

- Preventivas: Aquellas que reducen las vulnerabilidades
- Correctivas: Aquellas que reducen el impacto de las amenazas

9) Análisis de riesgos efectivos

Será el resultado de estudiar como se reducirían los riesgos con cada una de las medidas de protección (controles o salvaguardas) que hemos identificado; es decir, se debería calcular el riesgo definitivo, dándose como resultado el riesgo efectivo que tendría la organización para cada una de las amenazas identificadas.

Ambos riesgos se pueden calcular de la siguiente forma:

- Riesgo residual:

$$\text{Valor activo} \times \text{Vulnerabilidad} \times \text{Impacto}$$

- Riesgo efectivo:

Valor efectivo × Nueva vulnerabilidad × Nuevo Impacto = Valor activo × (Vulnerabilidad × Porcentaje de disminución de vulnerabilidad) × (Impacto × Porcentaje de disminución de impacto) = Riesgo intrínseco × Porcentaje de disminución de vulnerabilidad × Porcentaje de disminución de impacto

10) Gestión de riesgos

En esta fase final la organización deberá tomar decisiones sobre las medidas de seguridad que debe escoger entre el listado de salvaguardas que permiten reducir los riesgos.

La organización intentará siempre disminuir todos los riesgos detectados hasta situarlos por debajo del denominado "umbral de riesgos", que en esta compañía la Dirección de Seguridad de la Información a fijado en 0,1.

Para gestionar los riesgos en una empresa pueden tomarse tres decisiones:

- Reducirlos
- Transferirlos
- Aceptarlos
- Evitarlos/Eliminarlos

Para ello debe de gestionarse un plan de acción que debería de contener la siguiente información:

- Establecer prioridades
- Planteamiento del análisis de coste / beneficio
- Selección de controles definitivos
- Asignación de responsabilidades
- Implantación de controles

ANEXO IX - DOCSEC007

Declaración de Aplicabilidad

CONECTA BUS S.L

Tabla de contenido

1. Objeto

El objeto del presente documento es el de responder a la necesidad de Conecta Bus S.L, en adelante la Compañía, para definir la declaración de aplicabilidad con los controles de seguridad establecidos.

2. Alcance

El alcance de este documento aplica en el contexto del SGSI.

3. Declaración de aplicabilidad

CN : Continuidad de negocio.

RC : Requisito Contractual.

AR: Análisis de Riesgos.

L: Legal.

CONTROL	APLICA	JUSTIFICACIÓN	ORIGEN
A.5 POLITICAS DE SEGURIDAD DE LA INFORMACIÓN			
A.5.1.DIRECTRICES DE GESTIÓN DE SEGURIDAD DE LA INFORMACION			
A.5.1.1 POLÍTICAS PARA LA SEGURIDAD DE LA INFORMACIÓN	SÍ	Requerido para los procedimientos de Auditorías Internas	CN AR
A.5.1.2 REVISIÓN DE LAS POLÍTICAS PARA LA SEGURIDAD DE LA INFORMACIÓN	SÍ	Requerido para los procedimientos de Auditorías Internas	CN
A.6 ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN			
A.6.1 ORGANIZACION INTERNA			
A.6.1.1 ROLES Y RESPONSABILIDADES EN SEGURIDAD DE LA INFORMACIÓN	SÍ	Necesario para la definición de roles y responsabilidades.	CN
A.6.1.2 SEGREGACIÓN DE TAREAS	SÍ	Necesario para la definición de roles y responsabilidades.	CN
A.6.1.3 CONTACTO CON LAS AUTORIDADES	SÍ	Requerido para la norma y auditoría interna	CN L
A.6.1.4 CONTACTO CON GRUPOS DE INTERÉS ESPECIAL	SÍ	Requerido para la norma y auditoría interna	CN

A.6.1.5 SEGURIDAD DE LA INFORMACIÓN EN LA GESTIÓN DE PROYECTOS	SÍ	Requerido para la norma y auditoría interna	RC CN AR
A.6.2 LOS DISPOSITIVOS MÓVILES Y EL TELETRABAJO			
A.6.2.1 POLÍTICA DE DISPOSITIVOS MÓVILES	SÍ	Gestionar accesos de información	CN
A.6.2.2 TELETRABAJO	SÍ	Gestionar accesos de información	CN
A.7 SEGURIDAD RELATIVA A LOS RECURSOS HUMANOS			
A.7.1. ANTES DEL EMPLEO			
A.7.1.1 INVESTIGACIÓN DE ANTECEDENTES	SÍ	Mejorar los procesos de selección internos	CN RC AR L
A.7.1.2 TÉRMINOS Y CONDICIONES DEL EMPLEO	SÍ	Mejorar los procesos de selección internos	CN RC AR L
A.7.2 DURANTE EL EMPLEO			
A.7.2.1 RESPONSABILIDADES DE GESTIÓN	SÍ	Requerido por la norma	CN RC AR L
A.7.2.2 CONCIENCIACIÓN, EDUCACIÓN Y CAPACITACIÓN EN SEGURIDAD DE LA INFORMACIÓN	SÍ	Mejorar la formación del personal en seguridad	RC CN AR
A.7.2.3 PROCESO DISCIPLINARIO	SÍ	Requerido por la norma	L CN
A.7.3 FINALIZACIÓN DEL EMPLEO O CAMBIO EN EL PUESTO DE TRABAJO			
A.7.3.1 RESPONSABILIDADES ANTE LA FINALIZACIÓN O CAMBIO	SÍ	Proceso de altas / bajas / cambio de roles	RC CN
A.8 GESTIÓN DE ACTIVOS			
A.8.1 RESPONSABILIDAD SOBRE LOS ACTIVOS			
A.8.1.1 INVENTARIO DE ACTIVOS	SÍ	Mantener una correcta gestión de los activos	CN RC AR
A.8.1.2 PROPIEDAD DE LOS ACTIVOS	SÍ	Establecer responsabilidades	CN
A.8.1.3 USO ACEPTABLE DE LOS ACTIVOS	SÍ	Procedimiento uso de activos de la empresa	L RC CN AR
A.8.1.4 DEVOLUCIÓN DE ACTIVOS	SÍ	Procedimiento uso de activos de la empresa	CN AR
A.8.2 CLASIFICACIÓN DE LA INFORMACIÓN			
A.8.2.1 CLASIFICACIÓN DE LA INFORMACIÓN	SÍ	Requerido por la norma. Documento de clasificación de información	L RC CN

A.8.2.2 ETIQUETADO DE LA INFORMACIÓN	SÍ	Requerido por la norma. Documento de clasificación de información	CN AR
A.8.2.3 MANIPULADO DE LA INFORMACIÓN	SÍ	Requerido por la norma. Documento de clasificación de información	CN AR
A.8.3 MANIPULACIÓN DE LOS SOPORTES			
A.8.3.1 GESTIÓN DE SOPORTES EXTRAIBLES	SÍ	Requerido por la norma	L RC CN
A.8.3.2 ELIMINACIÓN DE SOPORTES	SÍ	Requerido por la norma	L RC CN
A.8.3.3 SOPORTES FÍSICOS EN TRÁNSITO	SÍ	Requerido por la norma	L RC CN
A.9 CONTROL DE ACCESO			
A.9.1. REQUISITOS DE NEGOCIO PARA EL CONTROL DE ACCESO			
A.9.1.1 POLÍTICA DE CONTROL DE ACCESO	SÍ	Requerido por la norma.	CN AR
A.9.1.2 ACCESO A LAS REDES Y A LOS SERVICIOS DE RED	SÍ	Requerido por la norma.	CN AR
A.9.2 GESTIÓN DE ACCESO DE USUARIO			
A.9.2.1 REGISTRO Y BAJA DE USUARIO	SÍ	Requerido por la norma .	RC CN AR
A.9.2.2 PROVISIÓN DE ACCESO DE USUARIO	SÍ	Requerido por la norma .	CN AR
A.9.2.3 GESTIÓN DE PRIVILEGIOS DE ACCESO	SÍ	Requerido por la norma .	CN AR
A.9.2.4 GESTIÓN DE LA INFORMACIÓN SECRETA DE AUTENTICACIÓN DE LOS USUARIOS	SÍ	Requerido por la norma .	CN
A.9.2.5 REVISIÓN DE LOS DERECHOS DE ACCESO DE USUARIO	SÍ	Requerido por la norma.	CN
A.9.2.6 RETIRADA O REASIGNACIÓN DE LOS DERECHOS DE ACCESO	SÍ	Requerido por la norma.	RC CN
A.9.3 RESPONSABILIDADES DEL USUARIO			
A.9.3.1 USO DE LA INFORMACIÓN SECRETA DE LA AUTENTICACIÓN	SÍ	Requerido por la norma. Asignación de roles y procedimientos de gestión de usuarios.	CN
A.9.4 CONTROL DE ACCESO A SISTEMAS Y APLICACIONES			
A.9.4.1 RESTRICCIÓN DEL ACCESO A LA INFORMACIÓN	SÍ	Mejorar la clasificación de la información	RC CN
A.9.4.2 PROCEDIMIENTOS SEGUROS DE INICIO DE SESIÓN	SÍ	Requerido por la norma.	CN

A.9.4.3 SISTEMA DE GESTIÓN DE CONTRASEÑAS	SÍ	Requerido por la norma.	RC CN AR
A.9.4.4 USO DE UTILIDADES CON PRIVILEGIOS DEL SISTEMA	SÍ	Requerido por la norma.	CN
A.9.4.5 CONTROL DE ACCESO AL CÓDIGO FUENTE DE PROGRAMAS	SÍ	Requerido por la norma.	RC CN
A.10 CRIPTOGRAFÍA			
A.10.1 CONTROLES CRIPTOGRÁFICOS			
A.10.1.1 POLÍTICA DE USO DE LOS CONTROLES CRIPTOGRÁFICOS	SÍ	Requerido por la norma. Gestión de la información	L RC CN AR
A.10.1.2 GESTION DE CLAVES	SÍ	Requerido por la norma. Gestión de la información	L RC CN AR
A.11 SEGURIDAD FÍSICA Y DEL ENTORNO			
A.11.1 ÁREAS SEGURAS			
A.11.1.1 PERÍMETRO DE SEGURIDAD FÍSICA	SÍ	Requerido por la norma.	RC CN AR
A.11.1.2 CONTROLES FÍSICOS DE ENTRADA	SÍ	Requerido por la norma.	RC CN AR
A.11.1.3 SEGURIDAD DE OFICINAS, DESPACHOS Y RECURSOS	SÍ	Requerido por la norma.	RC CN AR
A.11.1.4 PROTECCIÓN CONTRA LAS AMENAZAS EXTERNAS Y AMBIENTALES	SÍ	Requerido por la norma.	RC CN AR
A.11.1.5 EL TRABAJO EN ÁREAS SEGURAS	SÍ	Requerido por la norma.	RC CN AR
A.11.1.6 ÁREAS DE CARGA Y DESCARGA	SÍ	Requerido por la norma.	RC CN AR
A.11.2 SEGURIDAD DE LOS EQUIPOS			
A.11.2.1 EMPLAZAMIENTO Y PROTECCIÓN DE EQUIPOS	SÍ	Requerido por la norma. Protección de activos	RC CN AR
A.11.2.2 INSTALACIONES DE SUMINISTRO	SÍ	Requerido por la norma. Protección de activos	RC CN AR
A.11.2.3 SEGURIDAD DEL CABLEADO	SÍ	Requerido por la norma. Protección de activos	RC CN
A.11.2.4 MANTENIMIENTO DE LOS EQUIPOS	SÍ	Requerido por la norma. Proceso de mantenimiento de equipos	CN AR
A.11.2.5 RETIRADA DE MATERIALES PROPIEDAD DE LA EMPRESA	SÍ	Requerido por la norma. Protección de activos	CN RC L

A.11.2.6 SEGURIDAD DE LOS EQUIPOS FUERA DE LAS INSTALACIONES	SÍ	Requerido por la norma. Gestión de activos	RC CN
A.11.2.7 REUTILIZACIÓN O ELIMINACIÓN SEGURA DE EQUIPOS	SÍ	Requerido por la norma. Gestión de activos	RC CN AR
A.11.2.8 EQUIPO DE USUARIO DESATENDIDO	SÍ	Requerido por la norma. Gestión de activos	L RC CN AR
A.11.2.9 POLÍTICA DE PUESTO DE TRABAJO DESPEJADO Y PANTALLA LIMPIA	SÍ	Requerido por la norma. Gestión de activos	RC CN AR
A.12 SEGURIDAD DE LAS OPERACIONES			
A.12.1 PROCEDIMIENTOS Y RESPONSABILIDADES OPERACIONALES			
A.12.1.1 PROCEDIMIENTOS OPERACIONALES DOCUMENTADOS	SÍ	Requerido por la norma. Manual Uso de los bienes e instalaciones	CN
A.12.1.2 GESTION DE CAMBIOS	SÍ	Requerido por la norma. Gestión del material	RC CN AR
A.12.1.3 GESTION DE LA CAPACIDAD	SÍ	Requerido por la norma. Gestión del material	CN
A.12.1.4 SEPARACION DE LOS ENTORNOS DE DESARROLLO, TEST Y OPERACIONES	SÍ	Requerido por la norma. Mejorar seguridad en los sistemas de operación	CN
A.12.2 PROTECCION CONTRA SOFTWARE MALICIOSO			
A.12.2.1 CONTROLES CONTRA EL CÓDIGO MALICIOSO	SÍ	Requerido por la norma	CN AR
A.12.3 COPIAS DE SEGURIDAD			
A.12.3.1 COPIAS DE SEGURIDAD DE LA INFORMACION	SÍ	Mejorar en continuidad de negocio. Requerido por la norma	RC CN
A.12.4 REGISTROS Y SUPERVISIÓN			
A.12.4.1 REGISTRO DE EVENTOS	SÍ	Requerido por la norma. Gestión de acceso a la información	RC CN
A.12.4.2 PROTECCION DE LA INFORMACION DE LOS REGISTROS	SÍ	Requerido por la norma. Gestión de acceso a la información	CN
A.12.4.3 REGISTROS DE ADMINISTRADOR Y OPERADOR	SÍ	Requerido por la norma. Gestión de acceso a la información	RC CN
A.12.4.4 SINCRONIZACION DE RELOJES	SÍ	Requerido por la norma. Gestión de acceso a la información	CN
A.12.5 CONTROL DEL SOFTWARE EN EXPLOTACIÓN			
A.12.5.1 INSTALACIÓN DE SOFTWARE EN SISTEMAS DE PRODUCCIÓN	SÍ	Política de instalación y actualizacion de software	L RC CN AR
A.12.6 GESTION DE LA VULNERABILIDAD TECNICA			

A.12.6.1 CONTROL DE VULNERABILIDADES TECNICAS	SÍ	Requerido por la norma	CN
A.12.6.2 RESTRICCIONES DE LA INSTALACIÓN DE SOFTWARE	SÍ	Requerido por la norma	CN
A.12.7 CONSIDERACIONES EN LA AUDITORIA DE SISTEMAS DE INFORMACION			
A.12.7.1 CONTROLES DE LA AUDITORIA DE LOS SISTEMAS DE INFORMACION	SÍ	Requerido por la norma. Evolucionar el SGSI	CN AR
A.13 SEGURIDAD DE LAS COMUNICACIONES			
A.13.1 GESTION DE LA SEGURIDAD DE REDES			
A.13.1.1 CONTROLES DE RED	SÍ	Requerido por la norma. Mejora en la seguridad lógica	RC CN
A.13.1.2 SEGURIDAD DE LOS SERVICIOS DE RED	SÍ	Requerido por la norma. Mejora en la seguridad lógica	CN
A.13.1.3 SEGREGACION EN REDES	SÍ	Requerido por la norma. Mejora en la seguridad lógica	RC CN
A.13.2 INTERCAMBIO DE INFORMACION			
A.13.2.1 POLITICAS Y PROCEDIMIENTOS DE INTERCAMBIO DE INFORMACION	SÍ	Cumplimiento de GDPR	CN AR
A.13.2.2 ACUERDOS DE INTERCAMBIO DE INFORMACIÓN	SÍ	Cumplimiento de GDPR	RC CN
A.13.2.3 MENSAJERIA ELECTRONICA	SÍ	Cumplimiento de GDPR	RC CN
A.13.2.4 ACUERDOS DE CONFIDENCIALIDAD O NO DIVULGACIÓN	SÍ	Cumplimiento de GDPR	L RC CN AR
A.14 ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACION			
A.14.1 REQUISITOS DE SEGURIDAD EN SISTEMAS DE INFORMACION			
A.14.1.1 ANALISIS Y ESPECIFICACION DE REQUISITOS DE SEGURIDAD DE LA INFORMACIÓN	SÍ	Requerido por la norma. Procedimiento de seguridad de sistemas de información	C CN
A.14.1.2 SEGURIDAD DE SERVICIOS DE APLICACIÓN EN REDES PÚBLICAS	SÍ	Requerido por la norma. Procedimiento de seguridad de sistemas de información	L CN RC
A.14.1.3 PROTECCIÓN DE TRANSCCIONES DE SERVICIOS DE APLICACIONES	SÍ	Requerido por la norma. Procedimiento de seguridad de sistemas de información	CN
A.14.2 SEGURIDAD EN LOS PROCESOS DE DESARROLLO Y SOPORTE			
A.14.2.1 POLITICA DE DESARROLLO SEGURO	SÍ	Requerido por la norma	RC CN
A.14.2.2 PROCEDIMIENTOS DE CONTROL DE CAMBIOS DEL SISTEMA	SÍ	Requerido por la norma	RC CN AR
A.14.2.3 REVISION TECNICA DE LAS APLICACIONES TRAS CAMBIOS EN EL SISTEMA OPERATIVO	SÍ	Requerido por la norma .	CN

A.14.2.4 RESTRICCIONES A LOS CAMBIOS EN LOS PAQUETES DE SOFTWARE	SÍ	Requerido por la norma. Mejora de la seguridad lógica	RC CN
A.14.2.5 PRINCIPIOS DE INGENIERÍA DE SISTEMAS SEGUROS	SÍ	Requerido por la norma. Mejora de la seguridad lógica	CN
A.14.2.6 ENTORNO DE DESARROLLO SEGURO	SÍ	Requerido por la norma. Mejora de la seguridad lógica	CN
A.14.2.7 EXTERNALIZACIÓN DEL DESARROLLO SOFTWARE	SÍ	Requerido por la norma. Mejora de la seguridad lógica	CN
A.14.2.8 PRUEBAS DE SEGURIDAD DEL SISTEMA	SÍ	Requerido por la norma. Mejora de la seguridad lógica	RC CN
A.14.2.9 PRUEBAS DE ACEPTACION DEL SISTEMA	SÍ	Requerido por la norma. Mejora de la seguridad lógica	CN
A.14.3 DATOS DE PRUEBA			
A.14.3.1 PROTECCION DE LOS DATOS DE PRUEBA	SÍ	Cumplimiento de GDPR	CN
A.15 RELACION CON PROVEEDORES			
A.15.1 SEGURIDAD EN LAS RELACIONES CON PROVEEDORES			
A.15.1.1 POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN PARA LAS RELACIONES CON PROVEEDORES	SÍ	Requerido por la norma. Política Acuerdo con proveedores	RC CN AR
A.15.1.2 ABORDAR LA SEGURIDAD DENTRO DE LOS ACUERDOS CON PROVEEDORES	SÍ	Requerido por la norma. Política Acuerdo con proveedores	RC
A.15.1.3 CADENA DE SUMINISTRO TIC	SÍ	Requerido por la norma. Política Acuerdo con proveedores	RC
A.15.2 GESTION DE LA PROVISIÓN DE SERVICIOS DEL PROVEEDOR			
A.15.2.1 MONITORIZACION Y REVISION DE SERVICIOS DEL PROVEEDOR	SÍ	Requerido por la norma. Política Acuerdo con proveedores	RC
A.15.2.2 GESTION DE CAMBIOS A SERVICIOS DEL PROVEEDOR	SÍ	Requerido por la norma. Política Acuerdo con proveedores	RC CN
A.16 GESTION DE INCIDENTES DE SEGURIDAD DE LA INFORMACION			
A.16.1 GESTION DE INCIDENTES DE SEGURIDAD DE LA INFORMACION Y MEJORAS			
A.16.1.1 RESPONSABILIDADES Y PROCEDIMIENTOS	Sí	Requerido por la norma.	RC AR CN
A.16.1.2 NOTIFICACIÓN DE LOS EVENTOS DE SEGURIDAD DE LA INFORMACION	Sí	Requerido por la norma.	RC AR CN
A.16.1.3 NOTIFICACIÓN DE LOS PUNTOS DÉBILES DE LA SEGURIDAD	Sí	Requerido por la norma.	CN
A.16.1.4 EVALUACIÓN Y DECISIÓN SOBRE LOS EVENTOS DE SEGURIDAD DE LA INFORMACIÓN	Sí	Requerido por la norma.	CN
A.16.1.5 RESPUESTA A INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	Sí	Requerido por la norma.	RC CN
A.16.1.6 APRENDIZAJE DE LOS INCIDENTES DE SEGURIDAD DE LA INFORMACION	Sí	Requerido por la norma.	CN

A.16.1.7 RECOPILACIÓN DE EVIDENCIAS	Sí	Requerido por la norma.	RC CN
A.17 ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN PARA LA GESTION DE LA CONTINUIDAD DEL NEGOCIO			
A.17.1 CONTINUIDAD DE LA SEGURIDAD DE LA INFORMACION			
A.17.1.1 PLANIFICACIÓN LA CONTINUIDAD DE LA SEGURIDAD DE LA INFORMACIÓN	Sí	Requerido por la norma.	AR CN
A.17.1.2 IMPLEMENTAR LA CONTINUIDAD DE LA SEGURIDAD DE LA INFORMACION	Sí	Requerido por la norma.	CN
A.17.1.3 VERIFICACIÓN, REVISIÓN Y EVALUACIÓN DE LA CONTINUIDAD DE LA SEGURIDAD DE LA INFORMACIÓN	Sí	Requerido por la norma.	CN
A.17.2 REDUNDANCIAS			
A.17.2.1 DISPONIBILIDAD DE LOS RECURSOS DE TRATAMIENTO DE LA INFORMACIÓN	Sí	Requerido por la norma. Política de seguridad.	RC CN
A.18 CUMPLIMIENTO			
A.18.1 CUMPLIMIENTO DE LOS REQUISITOS LEGALES Y CONTRACTUALES			
A.18.1.1 IDENTIFICACION DE LA LEGISLACION APLICABLE Y REQUISITOS CONTRACTUALES	SÍ	Requerido por la norma.	RC CN
A.18.1.2 DERECHOS DE PROPIEDAD INTELECTUAL	SÍ	Requerido por la norma.	RC CN
A.18.1.3 PROTECCION DE LOS REGISTROS DE LA ORGANIZACIÓN	SÍ	Requerido por la norma.	CN
A.18.1.4 PROTECCION Y PRIVACIDAD DE LA INFORMACIÓN DE CARÁCTER PERSONAL	SÍ	Requerido por la norma.	L RC CN
A.18.1.5 REGULACION DE LOS CONTROLES CRIPTOGRAFICOS	SÍ	Requerido por la norma.	L RC CN AR
A.18.2 REVISIONES DE SEGURIDAD DE LA INFORMACIÓN			
A.18.2.1 REVISION INDEPENDIENTE DE LA SEGURIDAD DE LA INFORMACION	SÍ	Requerido por la norma.	CN
A.18.2.2 CUMPLIMIENTO DE LAS POLITICAS Y NORMAS DE SEGURIDAD	SÍ	Requerido por la norma.	CN
A.18.2.3 COMPROBACIÓN DEL CUMPLIMIENTO TÉCNICO	SÍ	Requerido por la norma.	CN AR