# Elaboración de un Plan de implementación de la norma ISO/IEC 27001:2013

**Nom Estudiant:** Juan González Martínez

**Programa:** Màster Universitari en Seguretat de les Tecnologies de la Informació i de les Comunicacions (MISTIC)

**Nom Consultor:** Arsenio Tortajada Gallego

**Centre:** Universitat Oberta de Catalunya

**Data Lliurament:** 10 de Junio de 2015

**C) Copyright**

**FITXA DEL TREBALL FINAL**

| | |
|---|---|
| **Títol del treball:** | Elaboración de un Plan de implementación de la norma ISO/IEC 27001:2013 |
| **Nom de l'autor:** | Juan González Martínez |
| **Nom del consultor:** | Arsenio Tortajada Gallego |
| **Data de lliurament (mm/aaaa):** | *06/2015* |
| **Àrea del Treball Final:** | Sistemas de gestión de la seguridad de la información |
| **Titulació:** | Màster Universitari en Seguretat de les Tecnologies de la Informació i de les Comunicacions (MISTIC) |

**Resum del Treball (màxim 250 paraules):**

Proyecto Fin de Máster Interuniversitario de Seguridad de las Tecnologías de la Información y Comunicaciones, donde se trata la implementación de un Sistema de Gestión de la Seguridad Informática, que cubra personal, sistemas informáticos, aulas, almacenes CPD, sala de comunicaciones, copias de seguridad, armarios de red, electrónica de red, servidores, servicios y datos de una Organización basándonos en la norma ISO/IEC 27001:2013 y su anexo a la ISO 27002.

Trabajo orientado a establecer las bases del Plan director de seguridad implementando un SGSI desde su inicio. Centrándonos es un primer estudio de la situación actual, donde se ha de identificar las amenazas que la organización tiene o a las que esté expuesta, y su impacto presente y futuro.

Se realiza un inventariar los activos de la empresa, realizando su clasificando por tipo de activo, documentando la normativa de seguridad de la información que regirá, describiendo los riesgos de los diferentes activos, proponiendo proyectos a realizar para solucionar las posibles carencias o riesgos detectados.

**Abstract (in English, 250 words or less):**

End Master Project Inter-University Security Information Technology and Communications, where the implementation of a Management System of Information Security, which covers personnel, computer systems, classrooms, warehouses CPD, communications room, copies it comes security, network cabinets, network electronics, servers, services, and data of an organization based on the ISO / IEC 27001: 2013 and ISO 27002 Annex.

Work aimed at establishing the basis of the master plan of implementing an ISMS security since its inception. Focusing is a first study of the current situation, where you have to identify threats that the organization has or that is exposed, and their present and future impact.

It takes an inventory of the assets of the company, making its sorting by type of asset, documenting the safety regulations governing information describing the risks of different assets, proposing projects to be undertaken to address possible shortcomings or risks identified.

**Paraules clau (entre 4 i 8):**

SGSI, ISO, SEGURIDAD, ANALISIS, ORGANIZACIÓN, AUDITORIA.

# Índice

1. Introducción…….. … 1
1.1 Contextualización y justificación del Trabajo…….. … 1
1.2 Objetivos del Trabajo……..... 2
1.3 Enfoque y métodos a seguir…… 2
1.4 Planificación del Trabajo…… 3
1.5 Breve descripción de los otros capítulos de la memoria…….. 3
2. Situación actual y análisis diferencial …….. 5
2.1 Selección y descripción de la empresa…….. 5
2.2 Definición de los objetivos del Plan Director de Seguridad…… 10
2.3 Análisis diferencial con las norma ISO/IEC 27001:2013 y :2013…… 11
3. Sistema de Gestión Documental…….. 17
3.1 Introducción …… 17
3.2 Política de Seguridad…….. 18
3.3 Procedimiento de Auditorías Internas…… 18
3.4 Gestión de Indicadores…….. 18
3.5 Procedimiento de revisión por Dirección…… 19
3.6 Gestión de Roles y Responsabilidades …….. 19
3.7 Metodología de análisis de riesgos…….. 22
3.8 Declaración de Aplicabilidad…….. 24
4. Análisis de Riesgos…….. 30
4.1 Inventario de activos…… 30
4.2 Valoración de los activos…… 31
4.3 Dimensiones de seguridad…….. 34
4.4 Tabla resumen de la valoración…… 35
4.5 Análisis de amenazas…….. 36
4.6 Impacto potencial…… 39
4.7 Nivel de riesgos Aceptable/Residual…… 40
4.8 Resultados…… 41
5. Propuestas de Proyectos…… 44
5.1 Introducción …….. 44
5.2 Estructura de las propuestas…….. 44
5.3 Propuestas de los proyectos…….. 44

5.4 Resumen de resultados…… 48
6. Auditoria del cumplimiento…… 53
6.1 Introducción…….. 53
6.2 Metodología …… 53
6.3 Evaluación de la madurez…….. 53
6.4 Resultados…… 62
7. Conclusiones…… 63
8. Glosario…….. 64
9. Bibliografía…… 66
10. Anexos…… 67
10.1 Anexo I Documento de Políticas de Seguridad
10.2 Anexo II Procedimiento de Auditorías Internas
10.3 Anexo III Gestión de Indicadores
10.4 Anexo IV Revisión por la Dirección
10.5 Anexo V Hoja Excel análisis_de_amenazas.xlsx
10.6 Anexo VI Auditoria del Cumplimiento

## Índice de figuras


Figura 1. Controles ISO/IEC 27001:2013……. 1
Figura 2. Fases planificación Proyecto Fin de Máster……. 3
Figura 3. Organigrama de la Organización……. 6
Figura 4. Estructura de red de la Organización……. 10
Figura 5. Estado de la ISO 27001……. 12
Figura 6. Diagrama de barras implementación controles ISO 21001 12
Figura 7. Diagrama radar implementación controles ISO 27001…… 12
Figura 8. Diagrama de barras implementación controles ISO 21002 15
Figura 9. Diagrama radar implementación controles ISO 27002…… 15
Figura 10. Estado de la ISO 27002……. 16
Figura 11. Estructura piramidal ISO 9000 de calidad documental….. 17
Figura 12. Calculo del riesgo según metodología NIST……. 22
Figura 13. Características valoración seguridad de la información…. 23
Figura 14. Grafico de barras análisis de amenazas..... 40
Figura 15. Grafico de barras niveles de riesgo……. 41
Figura 16. Grafico valores de riesgo de los activos……. 43
Figura 17. Planificación temporal de los proyectos de mejora…….. 48
Figura 18. Diagrama radar análisis diferencial pre y post proyectos… 49
Figura 19. Modelo de madurez (CMM) cumplimiento ISO 27001…….. 54
Figura 20. Grafico de complimiento controles ISO/IEC 27001:2013…. 61
Figura 21. Diagrama radar cumplimiento ISO/IEC 27001:2013…….. 61


## Índice de tablas

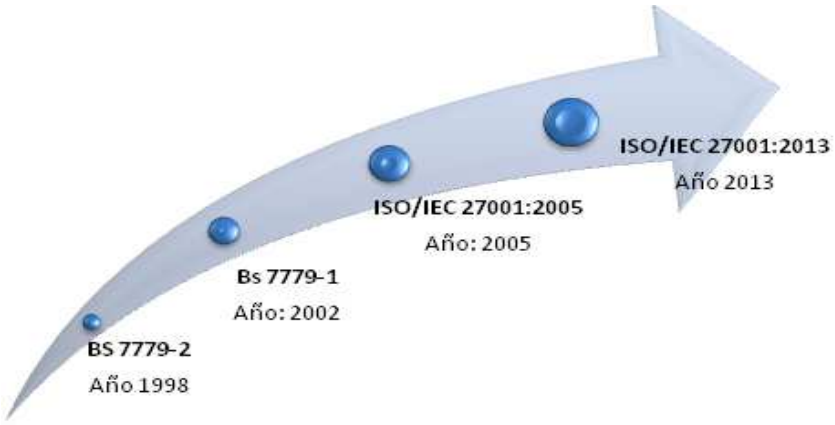

Tabla 1. Análisis diferencial respecto a la norma ISO 27001……. 11
Tabla 2. Análisis diferencial respecto a la norma ISO 27002……. 12
Tabla 3. Declaración aplicabilidad en dominios ISO 27002……. 24
Tabla 4. Inventario de Activos según metodología MAGERIT……. 30
Tabla 5. Árbol de dependencia entre activos……. 32
Tabla 6. Valoración de Activos según grupo de dependencia…….. 32
Tabla 7. Valoración de Activos según impacto (ACIDT)……. 34
Tabla 8. Escala de valoración según gravedad……. 34
Tabla 9. Tabla resumen de valoraciones…….. 35
Tabla 10. Tabla resumen de amenazas……. 36
Tabla 11. Tabla valoración del riesgo de amenazas…….. 40
Tabla 12. Tabla niveles de riesgo de los activos……. 42
Tabla 13. Tablas de los diferentes proyectos aportados…….. 45
Tabla 14. Análisis diferencial ISO 27001 tras aplicación de proyecto 50
Tabla 15. Tabla cumplimiento ISO/IEC 27002:2013……. 57
Tabla 16. Tabla resumen de cumplimiento ISO/IEC 27002:2013……. 61

# 1. Introducción.

## 1.1 Contextualización y justificación.

La norma ISO/IEC 27001 describe los requisitos que debe tener todo SGSI que aspire a obtener dicha certificación. Este estándar fue publicado como tal por la ISO (International Organization of Standarization) en 2005, y en la actualidad es el único aceptado para la gestión de la seguridad de la información, sin embargo es producto de toda una evolución. Por ello, la norma aceptada actualmente para este menester es la norma UNE-ISO/IEC 27001:2013 que son un conjunto de normas y estándares que proporcionan un marco de gestión de la seguridad de la información aplicable a cualquier organización.

Ahora bien, estas normas no son de obligado cumplimientos pero si unas normas de buenas prácticas que acreditan a las empresas que la información que manejan se hace de manera correcta y siguiendo unos controles exhaustivos.




El origen de la norma ISO/IEC 27001 se encuentra en la norma BS 7799-1:1995 que fue desarrollado como un manual de buenas prácticas para la seguridad de la información de las empresas británicas, esta guía no ofrecía una certificación; en 1999 esta norma es revisada y recién se convierte en una norma certificable como BS 7799-2:1999. En el año 2000 la ISO la toma como base y publica la norma ISO/IEC 17799:2000, sin embargo no implementan cambios significativos; posteriormente en 2005 la norma ISO/IEC 17799 es revisada, y aparece la norma certificable ISO/IEC 27001:2005. En 2007 la norma ISO/IEC 17799 es renombrada como ISO/IEC 27002. Esta norma es una guía de buenas prácticas que describe los controles (114 controles) que pueden ser implementados para la gestión de la seguridad de la información. No es una norma certificable. En 2009 se público un documento de modificaciones adicionales a la norma ISO 27001 llamado ISO/IEC 27001:2005/1M:2009.

Es en 2013 la última vez que se vuelve a revisar la norma ISO 27001 en la que se incluyen cambios significativos y se publica la norma ISO/IEC 27001:2013. Y fue en 2007 cuando se publicó una versión de la norma ISO 27001 traducida al castellano.

Las organizaciones que actualmente se encuentren certificadas en ISO/IEC 27001:2005 disponen de un periodo de transición estimado para adaptarse al nuevo estándar de 2 a 3 años.

## 1.2 Objetivos.


El objetivo de este trabajo fin de Máster, es el de realizar un plan de implementación de la ISO 27001:2013 en un Centro Especial de Empleo, dedico a la integración laboral y social de personas discapacitadas a través de formación específica en conocimientos técnicos informáticos y dar la oportunidad de empleabilidad de estas personas en labores de soporte técnico, montaje y reparación de equipos informáticos, así como el reciclaje de estos, consiguiendo la certificación en ISO 27001:2013.

Este proyecto se va a establecer en primer lugar realizando una auditoria con los controles contemplados en la norma ISO/IEC 27002:2013 para obtener una situación de partida y poder realizar el SGSI en base al resultado de la misma.

Esta certificación como se indica en el punto anterior, no es de obligado cumplimiento, pero sirve para que los potenciales clientes puedan tener la certeza del compromiso real de la empresa para con este tipo de información y así confiar en ella para poder contar con sus servicios.

## 1.3 Enfoque y método a seguir.

La empresa que describo, no posee todavía ningún sistema de gestión de la seguridad de la información implantado. Los procedimientos de seguridad existentes son los que coherentemente y siguiendo las normas básicas de actuación se han ido configurando en el entorno empresarial; por tanto, con esta situación el método a seguir será la de desarrollar el Plan Director de Seguridad que permita comenzar la implantación de un SGSI a fin de de mejorar la seguridad de la información en toda la organización y adaptarla al estándar ISO27000 integrando en todos sus procesos de negocio los procedimientos adecuados para consolidar la seguridad de la información en la empresa.

Como método de trabajo, se sigue el guion que se nos ha propuesto, desarrollando este SGSI basándonos en las normas ISO / IEC27001: 2103 e ISO / IEC27002: 2013, que actualmente tienen una mayor difusión y aceptación a nivel internacional.

Para la realización del Análisis de Riesgos hay distintas metodologías, pero para este proyecto me declino por la metodología MAGERIT

http://administracionelectronica.gob.es/?_nfpb=true&_pageLabel=PAE_PG_C TT_General&langPae=es& niciativa=magerit

## 1.4 Planificación del Trabajo.

Las fases del presente TRABAJO FIN DE MASTER, se han establecido en 6 entregas, dividiendo así el plan director y planificando en cada una de las fases una de las partes de las que está compuesto el plan director de seguridad de la información.

Por la monitorización de las diferentes entregas, el desarrollo de cada fase es secuencial, es decir, no puede comenzar una fase sin que se haya entregado la anterior.

| | | |
|---|---|---|
| Fase 1 | 06/03/2005 | Contextualización y documentación |
| Fase 2 | 27/03/2015 | Objetivos del Plan director |
| Fase 3 | 24/04/2015 | Estado del Riesgo: Identificación y valoración |
| Fase 4 | 15/05/2015 | Auditoria del cumplimiento |
| Fase 5 | 29/05/2015 | Propuesta del proyecto |
| Fase 5 | 10/06/2015 | Presentación de resultados |

## 1.5 Breve descripción de los otros capítulos de la memoria.

Situación actual y análisis diferencial.
Introducción al Proyecto. Enfoque y selección de la empresa que será objeto de estudio. Definición de los objetivos del Plan Director de Seguridad y Análisis diferencial de la empresa con respecto a la ISO / IEC 27001 + ISO / IEC 27002

Sistema de Gestión Documental.
Elaboración de la Política de Seguridad. Declaración de la aplicabilidad y documentación del SGSI, que incluye la documentación referente a la misma política de seguridad de la información, con los roles y responsabilidades en seguridad, el proceso de revisión por parte de la dirección, el proceso de gestión de indicadores, la metodología de análisis de riesgos, la declaración de aplicabilidad y el procedimiento de auditorías internas previstas.

Análisis de riesgos.
Elaboración de una metodología de análisis de riesgos: Identificación y valoración de los activos, amenazas, vulnerabilidades, cálculo del riesgo, nivel de riesgo aceptable y riesgo residual.

Propuesta de Proyectos.
Evaluación de proyectos que debe llevar a cabo la Organización para alinearse con los objetivos planteados en el Plan Director. Cuantificación económica y temporal de los mismos.
Auditoría de Cumplimiento.

Evaluación de controles, madurez y nivel de cumplimiento de la ISO / IEC 27002: 2013, que será un ajuste o segunda evaluación con respecto al realizado al inicio del proyecto en la fase de diagnóstico para ver las mejoras obtenidas en el desarrollo del proyecto.

Presentación de Conclusiones y entrega de Informes.
Consolidación de los resultados obtenidos durante el proceso de análisis. Realización de los informes y presentación ejecutiva a Dirección. Entrega del proyecto final y sus anexos…

# 2. Situación actual y análisis diferencial.

## 2.1 Selección y descripción de la empresa.

La empresa objeto de este proyecto de se trata de un Centro especial de Empleo, dedicado a ofrecer formación en informáticas y comunicaciones a personas con cierta discapacidad reconocida, además de ofrecer servicio técnico informático a otras empresas de la comunidad autónoma donde está ubicada, tales como instalación y montaje de equipos de telecomunicación, soporte técnico, formación avanzada y mantenimiento y montaje de redes de datos y telefónicas.

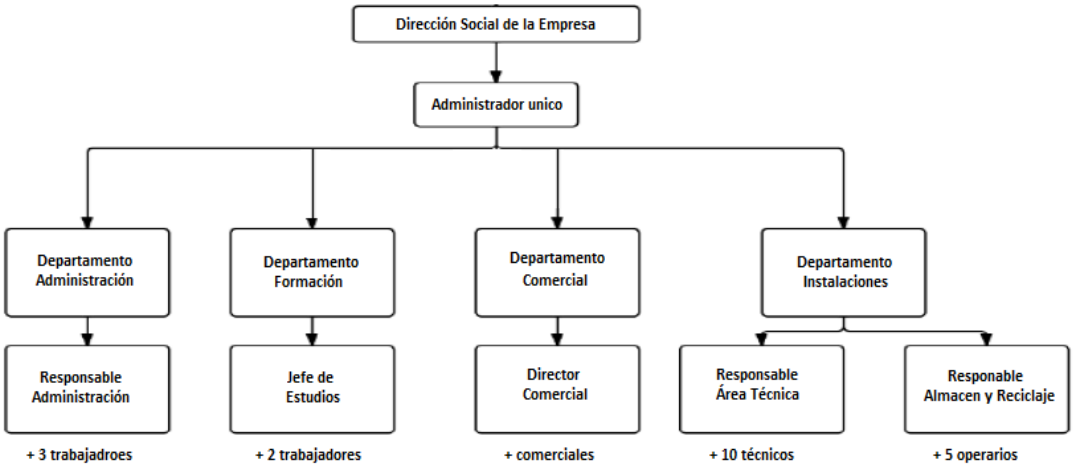
Su oferta se dirige principalmente a otras empresas dedicadas a la atención de discapacidades, centros especiales de empleo, asociaciones de discapacitados y administración pública; centrándose en proyectos acordes a su actividad y personal formado.

Su objetivo principal es la integración laboral y por tanto social de personas con discapacidad. Que como queda definido en la ley se trata de realizar un trabajo productivo, participando regularmente en las operaciones de mercado, y teniendo como finalidad el asegurar un empleo remunerado y la prestación de servicios de ajuste personal y social que requieran sus trabajadores minusválidos; a la vez que sea un medio de integración del mayor número de minusválidos al régimen de trabajo normal.

Para ello, desde la dirección se trata de generar valor empresarial consiguiendo la máxima calidad de servicio para sus clientes y de esta forma crear confianza y satisfacción en clientes, colaboradores y proveedores; a la vez de mantener un compromiso con el entorno social.

La empresa mantiene unos sistemas de planificación de recursos empresariales, para gestionar los diferentes enfoques de información gerenciales que integran y manejan las diferentes herramientas necesarias.

Sus instalaciones se encuentran repartidas en tres ubicaciones diferentes en localidad de Toledo. La dirección de la empresa, oficinas de administración y aulas, se encuentran en los bajos de un edificio situado en la zona comercial de la localidad, dispone de un local que hace las funciones de taller de reparación, zona de pruebas y formación práctica, también en el núcleo urbano de la localidad, pero a una distancia de unos tres quilómetros de las oficinas; por último se dispone de una nave en la zona del polígono, dedicada a almacenaje, centro de distribución (en caso necesario) y taller de reciclaje de equipos electrónicos e informáticos obsoletos.
La estructura de la empresa se define de la siguiente manera:




**Dirección Social de la Empresa:** Tiene estructura de Sociedad Limitada, estando formada en la actualidad por 3 miembros que toman las decisiones estratégicas y finales a nivel corporativo, dotando de los poderes necesarios al Administrador único de la empresa.

**Administrador Único**: Persona con poderes suficientes, para administrar la empresa en nombre de la dirección de la misma, que da cuentas ante esta del funcionamiento de la misma, con las prebendas legales que tiene el puesto de Administración ante las autoridades correspondientes.

**Departamento Administración:** Formado por el Responsable de Administración, dependiente directamente del Administrador Único y 3 trabajadores que desarrollan los trabajos oportunos de gestión administrativa y de personal de la empresa. Gestiona toda actuación relacionada con Recursos Humanos, Presupuestos- Facturación, Nóminas, Compra de Material y Mantenimiento de las instalaciones.

**Departamento Formación:** Formado por El jefe de Estudios, responsable del departamento y dos trabajadores que realizan funciones administrativas del mismo, como son la gestión de documentación de los cursos con los organismos oficiales y empresas solicitantes, búsqueda y gestión de subvenciones, gestión de alumnos, planificación de las acciones y administración de los textos y materiales necesarios.

**Departamento Comercial**: Formado por el Director Comercial y un número variable de comerciales, trabajadores o autónomos que se encargan de la captación y gestión tanto de Clientes y Proveedores, como de entidades oficiales y centros sociales a fin de dar salida a los cursos de formación planificados, a la vez de realizar estudios de viabilidad de futuras Ofertas, Concursos y Pedidos.

**Departamento Instalaciones**: Separado a su vez en dos bloques empresariales, uno dedicado al Área Técnica y otro al Almacenaje y Reciclaje electrónico.

El primer grupo está formado por el Responsable de Área Técnica y un equipo de 10 técnicos especialistas, encargados de las instalaciones, reparaciones y mantenimiento proactivo, tanto en las instalaciones propias como en instalaciones de clientes. Igualmente se encargan del desarrollo, gestión y mantenimiento del ERP propio.

El segundo grupo está formado por el Responsable de Almacén y Reciclaje que coordina un equipo de 5 técnicos medios, que desarrollan las labores de mantenimiento y gestión del almacén, así como el reciclaje y gestión del material electrónico, de acuerdo a las normas legales al respecto. Realizan las labores de retirada del material a reciclar en las empresas o entidades donantes, reciclaje y reutilización del mismo y destrucción y entrega a centros de gestión de residuos del material desechado.

En cuanto a medidas de seguridad en las distintas instalaciones de la empresa, en la sede de dirección, el acceso se realiza por una única puerta blindada, que da paso al hall, donde está la recepción con personal de administración; la empresa dispone de cámaras de video vigilancia (grabación 24 horas) contratadas con una empresa de seguridad en sus instalaciones; además de un sistema de alarma de esta misma empresa de seguridad, con dispositivos volumétricos, magnetotérmicos y detectores de apertura en las puertas.

La apertura de la puerta de acceso para el horario de trabajo se realiza siempre por un responsable de departamento, o el Administrador Unión, existen pues copias de la llave distribuidas al Administrador, Responsable de Administración, Jefe de Estudios, Director Comercial y Responsable de Área Técnica. El sistema de seguridad contratado, dispone de un terminal de conexión-desconexión junto a la puerta de acceso, para nada más abrir la misma la persona responsable, desconecte la alarma con su clave exclusiva, igualmente al cerrar la sede al final de la jornada, deberá conectar la alarma, dejando registro así de quien abre la sede y a qué hora y quien cierra y a qué hora.

Los ventanales que dan al exterior del edificio, son de cristal anti-golpe categoría 3 (Seguridad Alta) y tienen rejas instaladas. Todos los despachos y aulas se cierran con llave cuando están vacíos. Cada responsable tiene una copia de la llave de su despacho y además en el departamento de Administración tienen copia de todas las llaves para abrir los despachos en caso de que sea necesario.

El CPD o Centro de Procesamiento de Datos, es la ubicación donde se encuentra toda la infraestructura a nivel de comunicaciones y servidores, estando cerrada con llave y climatizada; tienen copia de la llave de acceso el Responsable de Área Técnica además del departamento de Administración.

Toda la documentación impresa se encuentra almacenada en archivadores en el área de administración, no estando al alcance de cualquier persona, quedando bajo llave en armarios y archivadores al efecto.

En el Local dedicado a Taller de reparación y formación práctica, se siguen los mismos criterios de seguridad que en la sede principal, el acceso se realiza por una única puerta metálica, del tipo acceso vehículos (para carga o descarga) y puerta peatonal en la misma, su apertura se realiza accediendo por la puerta peatonal con llave y para poder abrir el acceso de vehículo, hay que desbloquear un control mecánico. Dispone de cámaras de video vigilancia (grabación 24 horas) contratadas con una empresa de seguridad en sus instalaciones; además de un sistema de alarma de esta misma empresa de seguridad, con dispositivos volumétricos, magnetotérmicos y detectores de apertura en las puertas.

La apertura de la puerta de acceso para se realiza siempre por el responsable de Área técnica, Formador de Practicas o el Administrador Unión, existen pues copias de la llave distribuidas al Administrador y Responsable de Área Técnica, con copia de la llave en el departamento de Administración, para el caso de precisar la apertura en su ausencia. El sistema de seguridad contratado, dispone de un terminal de conexión-desconexión junto a la puerta de acceso, para nada más abrir la misma la persona responsable, desconecte la alarma con su clave exclusiva, igualmente al cerrar el taller se deberá conectar la alarma, dejando registro así de quien abre el taller y a qué hora y quien cierra y a qué hora.

Igualmente al Taller funciona el local de la empresa que tiene dedicado a Almacén, con los mismos sistemas y medidas, con la única particularidad, de que también tiene la llave de acceso el responsable de Almacén y Reciclaje. Igualmente, también el Almacén tiene una copia de la llave que se guarda en el departamento de Administración.

En cuanto a los recursos que dispone la empresa, nos encontramos en la sede central con un sistema de aire acondicionado y calefacción centralizado, además de un sistema de climatización independiente para el CPD. El CPD cuenta con un SAI configurable, conectado a red, que proporciona una autonomía suficiente, con gestión de apagado configurado para si se produce corte en el suministro eléctrico superior a 10 minutos. En el CPD se dispone de un extintor adecuado al fuego de tipo E como marca la normativa al respecto.

Dentro del CPD nos encontramos los siguientes elementos informáticos:

- 2 Controladores de Dominio: Integrados en un mismo dominio Active Directory sobre sistemas operativos Windows Server 2008 Enterprise. Encargados de la estructura empresarial, validación LDAP corporativo.

- 1 Servidor DHCP, que también hará las funciones de proxy y filtro de contenidos. También realizan las tareas de servidores DNS y gestión de trafico.

- 1 Servidor de Datos, que proporciona acceso a toda la información compartida de los diferentes departamentos, que utiliza el sistema LDAP del dominio para accesos y privilegios sobre los diferentes recursos compartidos

- 1 Servidor de copias de seguridad, con la herramienta Acronis Backup Advanced configurada para realizar las copias y recuperarlas junto a la unidad de cintas externa.

- 1 Servidor ERP que ejecuta la "herramienta ERP propia de la empresa.

- 1 Servidor de Windows SQL 2008, sobre Windows Server 2008, que almacena toda la información que se gestiona en la empresa, en relación a bases de datos para la formación, personal, reciclados, clientes…

- La centralita telefónica Cisco Ip Fone, que ejecuta el sistema de cisco VozIP gestionando las extensiones, validaciones en la línea y conexiones telefónicas entrantes-salientes.

- 1 Router de conexión ADSL a Internet, para los sistemas corporativos. Soportando varias líneas telefónicas de voz.

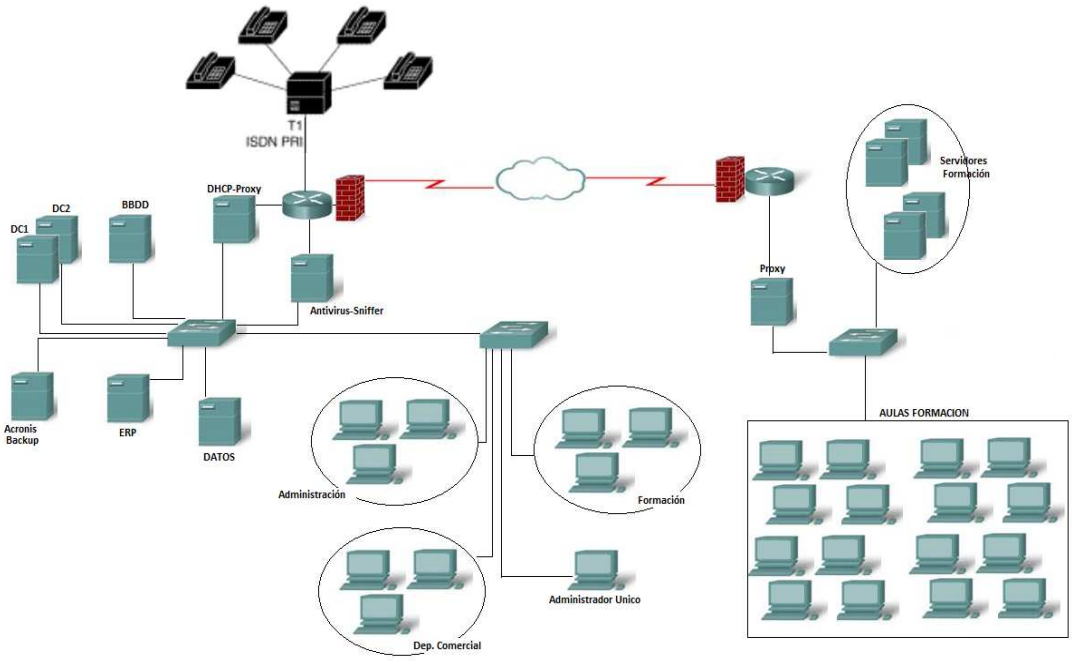
- 1 PC Firewal, snifer y antivirus conteniendo la aplicación Trend Micro corporativa.

- Varios servidores Windows y Linux, empleados para los cursos de formación.

- 1 Router de conexión ADSL a Internet para las aulas de formación.

Igualmente en la sede Central, cada puesto de usuario corporativo, tiene asignado un PC con Windows 7 Professional en el dominio corporativo e IP dinámica validado únicamente por el LDAP.

Para las aulas de formación, se disponen de puestos de usuario con arranques duales en sistemas Windows 7 y Ubuntu para realizar la formación que en cada momento se precise; contando con servidor propio que hace de Proxy y Filtro de contenidos, y una línea ADSL exclusiva para las aulas.




En el Taller de reparación y formación práctica, nos encontramos con una aula Taller con equipos sin software y sistemas operativos de prueba, para formaciones practicas; además de dos PCs instalados con sistema Windows 7 para su uso y utilización en las tareas propias del taller (búsqueda de información y/o drivers). La conexión a internet se realiza con una línea ADSL básica con un único teléfono, sin otra conexión empresarial.

En el Local de Almacén y reciclaje, nos encontramos con una pequeña oficina con dos PCs con Windows 7 instalado, para su uso y utilización en las tareas propias del Almacén-reciclaje (pequeña BBDD con equipos de Almacén y aplicación propia para control reciclaje de equipos y stocks). La conexión a internet se realiza con una línea ADSL básica con un único teléfono, sin otra conexión empresarial. Los datos que se comparten con la oficina de administración en la sede Central, se realizan a través del correo electrónico o en ficheros que se transportan en medios de almacenamiento portátiles.

## 2.2 Definición de los objetivos del Plan Director de Seguridad.

El objetivo principal consiste en el análisis de madurez de la organización, que siendo de pequeño tamaño, para la implantación de la ISO/IEC 27001 se deben aplicar todas las fases del SGSI; no solo para conocer el estado actual en Seguridad de la Información, si no para que se puedan ajustar todos los elementos que se necesitan para poder acceder a mediano plazo a una certificación en la norma ISO / IEC 27001 versión 2013.

La norma ISO 27001:2013 establece como requisitos para su definición que la organización debe determinar los límites y la aplicabilidad del

sistema de gestión de seguridad de la información para establecer su alcance.

Por ello, la organización debe considerar el entendimiento de la organización y su contexto, las expectativas de las partes interesadas y las interfaces y dependencias entre las actividades realizadas por la organización, y las que realizan otras organizaciones. El alcance debe estar disponible como información documentada.

## 2.3 Análisis diferencial con la norma ISO / IEC 27001: 2013 + ISO / IEC 27002: 2013.

Se realiza análisis diferencial del estado de la gestión de la seguridad de la información con la norma ISO/IEC 27001 y las mejores prácticas descritas con la ISO/IEC 27002 evaluando las capacidades de la empresa. Para ello, utilizo el modelo de Capacidad y Madurez CMM, con el que se puede averiguar el nivel de implementación existente.

### Análisis Diferencial respecto a la norma ISO 27001

| | | | |
|---|---|---|---|
| Clausula 4 | Contexto de la organización | | 30% |
| 4.1 | Entender la organización y su contexto | Definido | 80% |
| 4.2 | Entender las necesidades y expectativas de las partes interesadas | Inicial | 10% |
| 4.3 | Determinar el alcance del SGSI | Inexistente | 0% |
| Clausula 5 | Liderazgo | | 3% |
| 5.1 | Liderazgo y compromiso | Inicial | 10% |
| 5.2 | Política | Inexistente | 0% |
| 5.3 | Roles de la organización, responsabilidades y autoridad | Inexistente | 0% |
| Clausula 6 | Planificación | | 0% |
| 6.1 | Acciones para dirigir los riesgos y oportunidades | Inexistente | 0% |
| 6.2 | Objetivos y planes para lograrlos | Inexistente | 0% |
| Clausula 7 | Soporte | | 20% |
| 7.1 | Recursos | Inicial | 10% |
| 7.2 | Competencias | Limitado | 40% |
| 7.3 | Concienciación | Limitado | 40% |
| 7.4 | Comunicación | Inicial | 10% |
| 7.5 | Documentación | Inexistente | 0% |
| Clausula 8 | Operación | | 0% |
| 8.1 | Planificación operativa y control | Inexistente | 0% |
| 8.2 | Analisis del riesgo | Inexistente | 0% |
| 8.3 | Tratamiento del riesgo | Inexistente | 0% |
| Clausula 9 | Evaluación del rendimiento | | 0% |
| 9.1 | Monitorización, medición, analisis y evaluación | Inexistente | 0% |
| 9.2 | Auditoria interna | Inexistente | 0% |
| 9.3 | Revisión por Dirección | Inexistente | 0% |
| Clausula 10 | Mejora | | 0% |
| 10.1 | No conformidad y acción correctiva | Inexistente | 0% |
| 10.2 | Mejora continua | Inexistente | 0% |

Estado de la ISO 27001

| Sección | Nombre | % implementación |
|---|---|---|
| 4. | Contexto de la organización | 30% |
| 5. | Liderazgo | 3% |
| 6. | Planificación | 0% |
| 7. | Soporte | 20% |
| 8. | Operación | 0% |
| 9. | Evaluación del rendimiento | 0% |
| 10. | Mejora | 0% |

Diagrama de Barras de la implementación de controles de ISO 27001

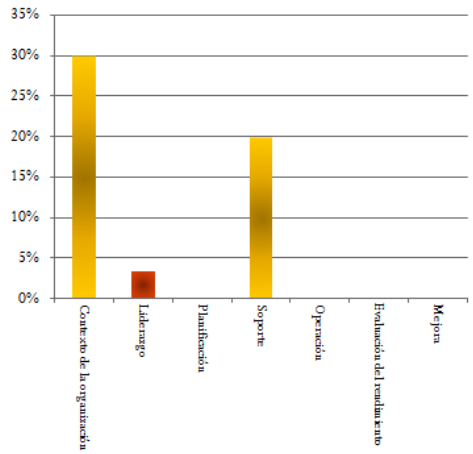
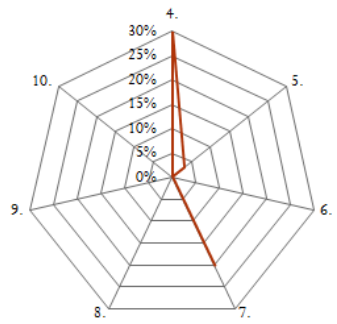



Diagrama de Radar de la implementación de controles de ISO 27001




## Análisis Diferencial respecto a la norma ISO 27002

| | | | |
|---|---|---|---|
| **5. POLITICA DE SEGURIDAD** | | | |
| **5.1 Dirección de la gestión de seguridad de la información.** | | | |
| 5.1.1 | Políticas de la seguridad de la información | No implementado | 0% |
| 5.1.2 | Revisión de las políticas de la seguridad de la información. | No implementado | 0% |
| **5. Política de Seguridad.** | | **No implementado** | 0% |
| **6. ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN** | | | |
| **6.1 Organización de la seguridad de la información.** | | | |
| 6.1.1 | Funciones y responsabilidades de seguridad de información. | Parcialmente implementado | 30% |
| 6.1.2 | Segregación de funciones. | Parcialmente implementado | 50% |
| 6.1.3 | Contacto con las autoridades. | No implementado | 0% |
| 6.1.4 | Contacto con grupos de especial interés. | No implementado | 0% |
| 6.1.5 | Seguridad de la información en la gestión de proyectos. | Parcialmente implementado | 20% |
| **6.2 Dispositivos moviles y teletrabajo.** | | | |
| 6.2.1 | Políticas de dispositivos moviles. | No implementado | 0% |
| 6.2.2 | Teletrabajo | No implementado | 0% |
| **6. Organización de la seguridad de la información.** | | **Parcialmente implementado** | 14% |
| **7. SEGURIDAD DE RECURSOS HUMANOS** | | | |
| **7.1 Antes de empleo.** | | | |
| 7.1.1 | Screening | No implementado | 0% |
| 7.1.2 | Terminos y condiciones de empleo | Parcialmente implementado | 50% |

| | | | |
|---|---|---|---|
| **7.2 Durante el empleo.** | | | |
| 7.2.1 | Responsabilidades de gestión | Parcialmente implementado | 10% |
| 7.2.2 | Conciencia de seguridad de la información y entrenamiento | Parcialmente implementado | 5% |
| 7.2.3 | Proceso disciplinario | Parcialmente implementado | 20% |
| **7.3 Terminación y cambio de empleo.** | | | |
| 7.3.1 | Terminación o cambio de las responsabilidades de empleo | No implementado | 0% |
| **7. Seguridad de recursos humanos.** | | **Parcialmente implementado** | 14% |
| **8. GESTION DE ACTIVOS** | | | |
| **8.1 Responsabilidad de los activos** | | | |
| 8.1.1 | Inventario de activos | No implementado | 0% |
| 8.1.2 | Propiedad de los activos | No implementado | 0% |
| 8.1.3 | Retorno de los activos | No implementado | 0% |
| **8.2 Clasificación de la información** | | | |
| 8.2.1 | Clasificación de la información | No implementado | 0% |
| 8.2.2 | Etiquetado de la información | No implementado | 0% |
| 8.2.3 | Manejo de activos | No implementado | 0% |
| **8.3 Manejo de Medios** | | | |
| 8.3.1 | Gestión de medios extraibles | Parcialmente implementado | 30% |
| 8.3.2 | Eliminación de medios | Parcialmente implementado | 30% |
| 8.3.3 | Transferencia de medios fisicos | Parcialmente implementado | 20% |
| **8. Gestión de activos.** | | **Parcialmente implementado** | 9% |
| **9. CONTROL DE ACCESO** | | | |
| **9.1 Business requirements of access control** | | | |
| 9.1.1 | Politica de control de acceso | Parcialmente implementado | 50% |
| 9.1.2 | Acceso a las redes y servicios de red | Parcialmente implementado | 50% |
| **9.2 Gestión de acceso de usuario** | | | |
| 9.2.1 | Registro de usuario y cancelación de registro | Parcialmente implementado | 50% |
| 9.2.2 | Acceso aprovisionamiento de usuario | Parcialmente implementado | 50% |
| 9.2.3 | Gestión de derechos de accesos privilegiados | Implementado | 70% |
| 9.2.4 | Gestión de la información de autentificación de secreto de los usuarios | Parcialmente implementado | 50% |
| 9.2.5 | Revisión de los derechos de acceso de usuario | Parcialmente implementado | 40% |
| 9.2.6 | Eliminación o ajuste de los derechos de acceso | Parcialmente implementado | 50% |
| **9.3 Responsabilidades del usuario** | | | |
| 9.3.1 | Uso de información secreta de autenticación | No implementado | 0% |
| **9.4 Control de sistemas y acceso a las aplicaciones** | | | |
| 9.4.1 | Restricción del acceso a la información | Parcialmente implementado | 50% |
| 9.4.2 | Procedimiento de inicio de sesión seguro | Implementado | 70% |
| 9.4.3 | Sistema de gestión de contraseñas | Implementado | 70% |
| 9.4.4 | Uso de programas de servicios publicos privilegiados | No implementado | 0% |
| 9.4.5 | Control de acceso al codigo fuente del programa | No implementado | 0% |
| **9. Control de acceso.** | | **Parcialmente implementado** | 43% |
| **10. CRIPTOGRAFIA** | | | |
| **10.1 Controles criptograficos** | | | |
| 10.1.1 | Politica sobre el uso de controles criptograficos | No implementado | 0% |
| 10.1.2 | Gestión de Claves | No implementado | 0% |
| **10. Criptografia.** | | **No implementado** | 0% |
| **10. Criptografia.** | | **No implementado** | 0% |
| **11. SEGURIDAD FISICA Y AMBIENTAL** | | | |
| **11.1 Areas seguras** | | | |
| 11.1.1 | Perímetro de seguridad física | Parcialmente implementado | 20% |
| 11.1.2 | Controles de entrada fisicas | Parcialmente implementado | 50% |
| 11.1.3 | Asegurar oficinas habitaciones e instalaciones | Parcialmente implementado | 40% |
| 11.1.4 | Protección contra amenazas externas y ambientales | Parcialmente implementado | 20% |
| 11.1.5 | Trabajar en zonas seguras | Parcialmente implementado | 20% |
| 11.1.6 | Zonas de entrega y carga | Parcialmente implementado | 30% |
| **11.2 Equipo** | | | |
| 11.2.1 | Ubicación y protección del equipo | Parcialmente implementado | 20% |
| 11.2.2 | Apoyo a los servicios publicos | No implementado | 0% |
| 11.2.3 | Seguridad de cableado | Implementado | 60% |
| 11.2.4 | Mantenimiento de los equipos | Implementado | 70% |
| 11.2.5 | Eliminación de los activos | Parcialmente implementado | 20% |
| 11.2.6 | Seguridad de equipo y activos fuera de las instalaciones | No implementado | 0% |
| 11.2.7 | Eliminación segura o reutilización de los equipos | Implementado | 80% |
| 11.2.8 | Equipos de usuario desatendidos | No implementado | 0% |
| 11.2.9 | Escritorio limpio y politica pantalla limpia | No implementado | 0% |
| **11. Seguridad fisica y ambiental.** | | **Parcialmente implementado** | 29% |

| | | | |
|---|---|---|---|
| **12. OPERACIONES DE SEGURIDAD** | | | |
| **12.1 Procedimientosy responsabilidades operacionales** | | | |
| 12.1.1 | Procedimientos operativos documentales | Parcialmente implementado | 20% |
| 12.1.2 | Gestión del cambio | Parcialmente implementado | 30% |
| 12.1.3 | Gestión de la capadidad | Parcialmente implementado | 20% |
| 12.1.4 | Separación de desarrollo, pruebas y entornos operativos | Parcialmente implementado | 30% |
| **12.2 Protección contra el malware** | | | |
| 12.2.1 | Controles contra el malware | Implementado | 90% |
| **12.3 Copias de seguridad** | | | |
| 12.3.1 | Copia de seguridad de la información | Implementado | 90% |
| **12.4 Registro y seguimiento** | | | |
| 12.4.1 | Registro de eventos | Parcialmente implementado | 20% |
| 12.4.2 | Protección de la información de los registros | Parcialmente implementado | 30% |
| 12.4.3 | Registros de administración y operación | Parcialmente implementado | 20% |
| 12.4.4 | Sincronización del reloj | Implementado | 100% |
| **12.5 Control del software operativo** | | | |
| 12.5.1 | Apoyo a los servicios publicos | No implementado | 0% |
| **12.6 Técnico de gestión de vulnerabilidades** | | | |
| 12.6.1 | Gestión de vulnerabilidades técnicas | Parcialmente implementado | 30% |
| 12.6.2 | Restricciones de instalación de software | Implementado | 70% |
| **12.7 Sistemas de la información consideraciones de auditoria** | | | |
| 12.7.1 | Sistemas de información controles de auditoria | No implementado | 0% |
| **12. Operaciones de seguridad.** | | **Parcialmente implementado** | 39% |
| **13. SEGURIDAD DE LAS COMUNICACIONES** | | | |
| **13.1 Gestión de la seguridad de la red** | | | |
| 13.1.1 | Funciones y responsabilidades de seguridad de información. | Parcialmente implementado | 30% |
| 13.1.2 | Segregación de funciones. | Parcialmente implementado | 30% |
| 13.1.3 | Contacto con las autoridades. | No implementado | 0% |
| **13.2 Transferencia de Información** | | | |
| 13.2.1 | Politicas y procedimientos de transferencia de información | Parcialmente implementado | 10% |
| 13.2.2 | Acuerdos sobre la transferencia de información | No implementado | 0% |
| 13.2.3 | Mensajería electrónica | No implementado | 0% |
| 13.2.4 | Acuerdos de confidenciabilidad o de no divulgación | No implementado | 0% |
| **13. Seguridad de las comunicaciones.** | | **Parcialmente implementado** | 10% |
| **14. SISTEMA DE ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO** | | | |
| **14.1 Security requirements of information system** | | | |
| 14.1.1 | Información de analisis de requisitos de seguridad y la especificación | Parcialmente implementado | 10% |
| 14.1.2 | Asegurar los servicios de aplicaciones en las redes publicas | Parcialmente implementado | 30% |
| 14.1.3 | Protección de las transacciones de servicios de aplicaciones | No implementado | 0% |
| **14.2 Seguridad en los procesos de desarrollo y de apoyo** | | | |
| 14.2.1 | Politica de desarrollo seguro | No implementado | 0% |
| 14.2.2 | Procedimientos de control de cambio del sistema | No implementado | 0% |
| 14.2.3 | Revisión técnica de las aplicaciones tras efectuar cambios en la plataforma operativo | No implementado | 0% |
| 14.2.4 | Restricciones a los cambios de los paquetes de software | No implementado | 0% |
| 14.2.5 | Principios de ingeniería de sistemas seguros | No implementado | 0% |
| 14.2.6 | Entorno de desarrollo seguro | No implementado | 0% |
| 14.2.7 | Desarrollo outsourced | No implementado | 0% |
| 14.2.8 | Pruabas de seguridad del sistema | | |
| 14.2.9 | Pruebas de aceptación del sistema | No implementado | 0% |
| **14.3 Datos de prueba** | | | |
| 14.3.1 | Protección de datos de prueba | No implementado | 0% |
| **14. Sistema de adquisición, desarrollo y mantenimiento.** | | **Parcialmente implementado** | 3% |

| | | | |
|---|---|---|---|
| **15.RELACIÓN CON PROVEEDORES** | | | |
| **15.1 Seguridad en la información en las relaciones con proveedores** | | | |
| 15.1.1 | Política de seguridad de la información para relaciones con los proveedores | Parcialmente implementado | 20% |
| 15.1.2 | Abordar la seguridad dentro de los acuerdos con proveedores | Parcialmente implementado | 30% |
| 15.1.3 | Cadena de la información y tecnología de comunicación de suministro | No implementado | 0% |
| **15.2 Gestión de la prestación de servicios de proveedores** | | | |
| 15.2.1 | Política de desarrollo seguro | No implementado | 0% |
| 15.2.2 | Procedimientos de control de cambio del sistema | No implementado | 0% |
| **15. Relación con los proveedores.** | | **Parcialmente implementado** | 10% |
| **16. INFORMACIÓN DE GESTIÓN DE INCIDENCIAS DE SEGURIDAD** | | | |
| **16.1 Gestión de incidencias de seguridad de la información y mejoras** | | | |
| 16.1.1 | Responsabilidades y procedimientos | No implementado | 0% |
| 16.1.2 | Presentación de informes de eventos de seguridad de información | No implementado | 0% |
| 16.1.3 | Informes debilides de seguridad de información | No implementado | 0% |
| 16.1.4 | Evaliación y decisión sobre los eventos de seguridad de información | No implementado | 0% |
| 16.1.5 | Respuestas a incidentes de seguridad de la información | No implementado | 0% |
| 16.1.6 | Aprendiendo de los incidentes de seguridad de la información | No implementado | 0% |
| 16.1.7 | Acopio de pruebas | No implementado | 0% |
| **16. Información de gestión de incidencias de seguridad.** | | **No implementado** | 0% |
| **17. ASPECTOS DE SEGURIDAD DE INFORMACIÓN DE LA GESTIÓN DE LA C** | | | |
| **17.1 Información continuidad seguridad** | | | |
| 17.1.1 | Planificación información continuidad seguridad | No implementado | 0% |
| 17.1.2 | Implementación de la información continuidad seguridad | No implementado | 0% |
| 17.1.3 | Verificar, revisar y evaluar la información de seguridad continuidad | No implementado | 0% |
| **17.2 Despidos** | | | |
| 17.2.1 | Disponibilidad de instalaciones de procesamiento de información | No implementado | 0% |
| **17. Aspectos de seguridad de información de la gestión de la continuidad de** | | **No implementado** | 0% |
| **18. CONFORMIDAD** | | | |
| **18.1 Cumplimiento de los requisitos legales y contractuales** | | | |
| 18.1.1 | Identificación de la legislación aplicable y requisitos contractuales | No implementado | 0% |
| 18.1.2 | Derechos de propiedad intelectual | No implementado | 0% |
| 18.1.3 | Protección de los registros | No implementado | 0% |
| 18.1.4 | Privacidad y protección de datos personales | No implementado | 0% |
| 18.1.5 | Reglamento de los controles criptograficos | No implementado | 0% |
| **18.2 Revisiones de seguridad de información** | | | |
| 18.2.1 | Revisión independiente de seguridad de la información | No implementado | 0% |
| 18.2.2 | Cumplimiento de las politicas y etandares de seguridad | No implementado | 0% |
| 18.2.3 | Revisión del cumplimiento técnico | No implementado | 0% |
| **17. Aspectos de seguridad de información de la gestión de la continuidad de** | | **No implementado** | 0% |

**Diagrama de Barras de la implementación de controles de ISO 27002**

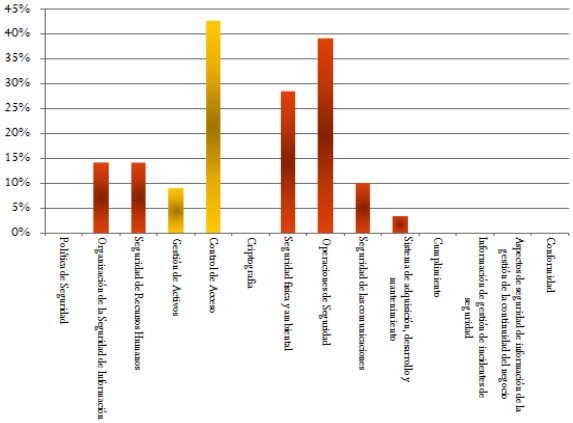
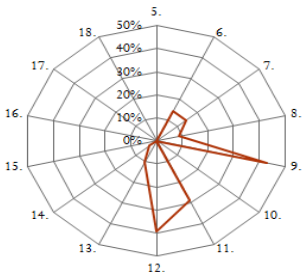



**Diagrama de Radar de la implementación de controles de ISO 27002**

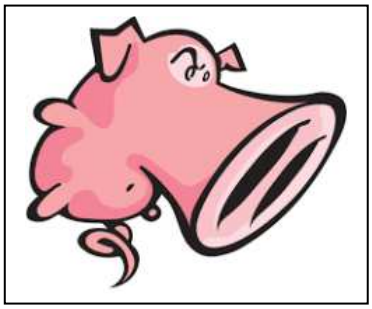


Estado de la ISO 27002

| Sección | Nombre | % implementación |
|---|---|---|
| 5. | Política de Seguridad | 0% |
| 6. | Organización de la Seguridad de Información | 14% |
| 7. | Seguridad de Recursos Humanos | 14% |
| 8. | Gestión de Activos | 9% |
| 9. | Control de Acceso | 43% |
| 10. | Criptografía | 0% |
| 11. | Seguridad física y ambiental | 29% |
| 12. | Operaciones de Seguridad | 39% |
| 13. | Seguridad de las comunicaciones | 10% |
| 14. | Sistema de adquisición, desarrollo y mantenimiento | 3% |
| 15. | Cumplimiento | 0% |
| 16. | Información de gestión de incidentes de seguridad | 0% |
| 17. | Aspectos de seguridad de información de la gestión de la continuidad del negocio | 0% |
| 18. | Conformidad | 0% |
| TOTAL S.G.S.I. | | 15% |

Tras un estudio de los resultados, verificamos lo que ya es conocido, la empresa en cuestión no cuenta con un SGSI establecido; y si bien se toman ciertas medidas destinadas a dotar de seguridad los sistemas de la organización y su estructura tecnológica, no tiene previstos unos controles sobre el cumplimiento de estas medidas ni cómo mejorarlas.

Como se indica en la definición de la estructura empresarial, está prevista la realización de copias de seguridad y existe un plan de copias, pero este se queda en esa, la realización de las copias, no teniéndose en cuenta riesgos posibles ni búsqueda de amenazas en los procesos.



No se tiene conocimiento de auditorías, internas o externas, ni se tiene un desarrollo sobre la resolución de los incidentes encontrados. Si existe un sistema de detección de amenazas (sniffer de red) pero no hay una planificación de cómo ir complementándolo y verificando realmente su utilidad y mejora.

Es claramente visible, que la planificación y elaboración de un SGSI en esta empresa, se lograrían mejoras sustanciales en la gestión de la información y en la seguridad de la misma; además en el sector en el que desarrolla su negocio, sería de gran relevancia disponer de una certificación en el estándar 27001:2013 ante los actuales clientes y futuros contratos con la administración pública.

# 3. Situación actual y análisis diferencial.

## 3.1 Introducción

Todos los Sistemas de Gestión se basan en un sistema documental siguiendo la normativa establecida en la norma ISO / IEC 27001. Además, cabe reseñar que atendiendo a la norma ISO 9000 sobre gestión de calidad, esta documentación mantiene una estructura piramidal de 4 niveles.


Documentos de Nivel 1

Manual de seguridad: Documento que inspira y dirige todo el sistema, el que expone y determina las intenciones, alcance, objetivos, responsabilidades, políticas y directrices principales, etc., del SGSI.

Documentos de Nivel 2

Procedimientos: Documentos en el nivel operativo, que aseguran que se realicen de forma eficaz la planificación, operación y control de los procesos de seguridad de la información.

Documentos de Nivel 3

Instrucciones, checklists y formularios: Documentos que describen cómo se realizan las tareas y las actividades específicas relacionadas con la seguridad de la información.

Documentos de Nivel 4

Registros: Documentos que proporcionan una evidencia objetiva del cumplimiento de los requisitos del SGSI; están asociados a documentos de

los otros tres niveles como output que demuestra que se ha cumplido lo indicado en los mismos.

## 3.2 Política de seguridad.

En este documento se especifica la normativa interna y la política de seguridad que puede tener la organización, y que los diferentes perfiles de trabajadores de la organización deben conocer y cumplir debidamente. Se especifican los términos relativos al acceso a la información, los recursos, o cómo actuar ante incidentes.

Este documento debe ser conocido por todo el personal afectado, evitándose pues ambigüedades o exceso de tecnicismos que lleven a malentendidos, además deberá revisarse periódicamente siendo aprobada su confección y revisiones por la dirección de la empresa.

Este documento de Políticas de Seguridad se encuentra en el Anexo 1 del presente proyecto.

## 3.3 Procedimiento de Auditorías Internas.

El Procedimiento de auditorías internas, es un requisito inherente dentro de un SGSI, dentro de lo que se entiende como revisión y mejora continua; es pues un mecanismo que permite conocer y evaluar el estado de nuestro Sistema de Gestión de la Seguridad y los elementos relacionados con la implantación, corrección y mejora de nuestros sistemas de información.

En este plan anual se definirá quien realizará las auditorías, los métodos que se utilizarán, criterios que se aplicarán, etc.**,** encargándose de validar todo el sistema de información de la empresa, controlar las vulnerabilidades detectadas, revisar los controles e indicadores que se hayan hecho servir para la implantación de la norma y la correspondiente documentación relativa a la normativa ISO

Este documento de Procedimiento de Auditorías Internas se encuentra en el Anexo 2 del presente proyecto.

## 3.4 Gestión de Indicadores.

La implementación de un SGSI incluye la definición de una serie de indicadores con los que se pueda determinar el nivel de cumplimiento de los controles de seguridad establecidos. Es necesario evaluar la eficacia de estos controles de seguridad de forma continuada y siguiendo siempre unos parámetros establecidos, que definan los mecanismos y periodicidad de estas mediciones.

Estos indicadores proporcionan una información muy valiosa para la toma de decisiones, la calidad de estas decisiones y su eficiencia efectiva.

Este documento de Gestión de Indicadores se encuentra en el Anexo 3 del presente proyecto.

## 3.5 Procedimiento de revisión por Dirección.

La Dirección como responsable de la aprobación del SGSI, debe realizar de con un periodo inferior a un año, una revisión al sistema, indicando los asuntos prioritarios de éste y aprobado los ajustes/acciones de mejora que se tengan, para verificar el cumplimiento de todos los estándares, normas y procedimientos establecidos en el SGSI. El Responsable de Seguridad será el encargado de realizar esta revisión.

El Responsable de Seguridad realizará un breve informe sobre la revisión realizada anualmente. En este se incluirán las incidencias y deficiencias detectadas y una relación de soluciones y propuestas de mejora; para ello, se debe convocar en plazo establecido una reunión y enviar los informes de gestión para ser revisados en los siguientes puntos:

- Indicadores y revisiones previas realizadas.
- Resultados de las auditorias.
- Revisión y estado de las políticas de seguridad.
- Estado de la gestión de riesgos e incidentes de seguridad.
- Nuevos requerimientos del SGSI.
- Estado de las acciones correctivas, preventivas y de mejora.
- Resultados de riesgos: Riesgos no tratados o resultado de los que no tuvieron la efectividad esperada.

Ejemplo de este informe re revisión por la dirección se encuentra en el Anexo 4 del presente proyecto.

## 3.6 Gestión de Roles y Responsabilidades.

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 la Dirección de la organización.

Todo el personal que tenga acceso a los sistemas de información está en la obligación de cumplir y respetar las normas, políticas definidas de forma general y específica, también deberán cumplir solo con las funciones que han sido brindadas en su contrato laboral con respecto a la seguridad de la información.

Para el SGSI se han definido los siguientes roles y responsabilidades:

**ROL: Dirección Social de la Empresa:**

- Aprobar los recursos financieros y humanos para el SGSI
- Aprobar y firmar las políticas de seguridad y sus actualizaciones.

- Aprobar en última instancia el SGSI y los procedimientos respectivos.
- Gestionar adecuadamente los riesgos de alto nivel que se hayan detectado.
- Revisar y ajustar los indicadores de su competencia.
- Aprobar los planes de continuidad de negocio.
- Participar activamente de las reuniones programadas.

**ROL: Comité de Seguridad:**

- Revisar, mantener y aprobar en primera instancia el SGSI.
- Revisar, gestionar y aprobar los planes de seguridad e implementaciones de controles.
- Gestionar las mediciones de los indicadores y presentarlos a las partes interesadas.
- Gestionar las acciones preventivas, correctivas y de mejora que surgen durante las revisiones periódicas.
- Gestionar adecuadamente los incidentes de seguridad y la continuidad del negocio.
- Participar activamente de las reuniones programadas.
- Analizar y establecer acciones frente a incumplimientos de las políticas definidas.

**ROL**: **Responsable de Seguridad:**

- Liderar la implementación y mantenimiento del SGSI.
- Liderar las reuniones del comité de seguridad.
- Participar de las capacitaciones programadas.
- Verificar los informes de la auditoria.
- Velar por la actualización, divulgación y concientización del modelo de seguridad de la información.
- Monitorear el nivel de implementación del SGSI y hacer seguimiento a las acciones correctivas y preventivas.
- Reportar al Comité de Seguridad de la Información los incidentes y riesgos más relevantes en cuanto a la seguridad de la información.

**ROL: Responsable de Recursos Humanos:**

- Diseñar e implementar programas de capacitación y concientización sobre Seguridad de la Información y el cumplimiento de la política definida.
- Reportar en los tiempos establecidos cualquier novedad relacionada con la contratación del personal, incluyendo vinculación, modificación de cargo, modificación de ubicación y desvinculación.
- Revisar el estado de los contratos de trabajo.
- Ejecutar los procesos administrativos y/o disciplinarios.
- Revisar periódicamente la legislación vigente.

**ROL: Responsable TIC en la empresa:**

- Coordinar el equipo de trabajo (equipo de seguridad).

- Gestionar la obtención de entradas para los indicadores, mapas de riesgos y demás informes.
- Recibir y asignar funciones y tareas a los miembros del equipo de seguridad.
- Coordinar y gestionar las capacitaciones en seguridad.
- Administrar las plataformas de seguridad como Firewall y el anti-virus
- Obtener y analizar reportes de seguridad
- Coordinar el monitoreo de eventos de seguridad.
- Administrar/gestionar el control de acceso a las redes y aplicativos.
- Implementar mecanismos de seguridad sobre redes y plataformas.
- Cumplir y hacer cumplir las políticas de control de acceso a las redes.

**ROL: Auditor Interno:**

- Llevar a cabo las auditorias del SGSI de manera periódica.
- Generar las respectivas acciones preventivas, correctivas y de mejora sobre el sistema.
- Convocar a las reuniones/comités de seguimientos.
- Liderar los planes de auditoría, retroalimentando al comité de seguridad.
- Ejecutar las acciones con ética, respeto, transparencia, independencia e imparcialidad.

**ROL: Jefe de departamento:**

- Apoyar al negocio en la identificación de riesgos de Seguridad de la Información y la generación de los respectivos planes de acción para mitigarlos razonablemente.
- Participar del SGSI cuando sean convocados.
- Analizar e implementar los hallazgos de los planes de auditoría que estén a su alcance.

**ROL: Director Comercial:**

- Participar del SGSI cuando sean convocados.
- Analizar e implementar los hallazgos de los planes de auditoría que estén a su alcance.
- Apoyar con estrategias comunicacionales y de cultura para la implementación y gestión del SGSI.
- Construir piezas publicitarias para la sensibilización y difusión de los planes de seguridad.
- Apoyar la redacción y revisión de los contratos con proveedores.
- Diseñar elementos de publicidad que se apropien de la estrategia de seguridad.
- Apoyar la implementación de los planes de cultura y sensibilización.

**ROL: Todo empleado de la empresa:**

- Conocer, cumplir y velar por el cumplimiento de la política de seguridad de la información.

- Velar por la protección de la información que manejan en el desempeño de sus responsabilidades.

- Reportar cualquier incumplimiento de la política de seguridad de la información o cualquier evento o situación relacionada con fuga o modificación no autorizada de información de la empresa o sus clientes.

## 3.7 Metodología de Análisis de Riesgos.

Hay que ver el análisis de riesgo como uno de los puntos clave en la implementación, mantenimiento y mejora de un Sistema de Gestión de la Seguridad de la Información (SGSI), dado que permite identificar los puntos débiles de la organización. El responsable de seguridad será la persona responsable de la definición del Análisis de Riesgos.

Este procedimiento será de aplicación para los activos implicados en la seguridad de la información, realizándose atendiendo a las normas ISO/IEC 27001: 2013, ISO/IEC 27002: 2013 y NIST 800-30 utilizando la metodología Magerit, para el análisis y gestión de riesgos en sistemas de información elaborada por el Consejo Superior de Administración Electrónica.

Para esta metodología elegida, se realizará la identificación de los activos, entre los que diferenciaremos entre activos físicos, lógicos, de personal e infraestructuras.

Igualmente se realizara la identificación de amenazas y vulnerabilidades, entendiendo por amenazas las situaciones que pueden dañar los activos y de las que se han de proteger; y siendo vulnerabilidades las diferentes debilidades que presentan los activos de la empresa.

Como se indica, la sistemática para calcular el riesgo, se basa en la relación entre activos, amenazas y vulnerabilidades. A la hora de realizar este cálculo utilizaremos como se indica la metodología NIST, determinando tres niveles diferentes en cuanto a la frecuencia y la criticidad observada, bajo, medio y alto. A partir de estos niveles se define el siguiente cuadro con los diferentes riesgos que se pueden dar en la empresa:

| CALCULO DEL RIESGO | Impacto | | |
|---|---|---|---|
| **Probabilidad de amenaza** | **Bajo** | **Medio** | **Alto** |
| **Baja** | Bajo | Bajo | Bajo |
| **Media** | Bajo | Medio | Medio |
| **Alta** | Bajo | Medio | Alto |

A continuación, se identificarán las características de la seguridad de la información afectadas por cada una de las posibles situaciones: confidencialidad, integridad y / o disponibilidad; y valorando esta información identificaremos la probabilidad de que esta situación se produzca, obteniendo de esta forma el riesgo.

Valoración de Activos:

| VALORACIÓN DE ACTIVOS | | |
|---|---|---|
| MA | 500.000,00 € | Muy Alto |
| A | 100.000,00 € | Alto |
| M | 30.000,00 € | Medio |
| B | 3.000,00 € | Bajo |
| N | 500,00 € | Muy Bajo |

Frecuencia:

| FRECUENCIA (en la que puede materializarse) | | | |
|---|---|---|---|
| EF | 0,9973 | Extremadamente frecuente | Menos que 1 día |
| MF | 0,1425 | Muy Frecuente | Menos que 1 semana |
| F | 0,0329 | Frecuente | Menos que un mes |
| FN | 0,0055 | Frecuencia Normal | Menos que medio año |
| PF | 0,0027 | Poco Frecuente | Menos que un año |
| EPF | 0,0003 | Extremadamente Poco Frecuente | Menos que diez años |

Impacto:

| IMPACTO | | | |
|---|---|---|---|
| C | Crítico | 90% | 90% de degradación |
| A | Alto | 75% | 75% de degradación |
| M | Medio | 50% | 50% de degradación |
| B | Bajo | 20% | 20% de degradación |

Disminución del Impacto:

| DISMINUCIÓN DEL IMPACTO | | |
|---|---|---|
| MA | Alta | 90% |
| A | Media | 60% |
| M | Baja | 30% |
| B | Nula | 0% |

Para realizar esta metodología de análisis de riesgos se han tomado algunos elementos como base de MAGERIT, pretendiendo conocer cuánto está en juego y como se protegerá.

Se pretende realizar unos pasos para determinar el riesgo que son:

- Determinar los activos relevantes para la Organización, su interrelación y su valor, y el coste supondría su degradación.
- Determinar las amenazas a la que están expuestos estos activos.
- Determinar salvaguardas dispuestas y efectividad ante el riesgo.
- Estimar el impacto, cuando se hace efectiva una amenaza sobre el activo.
- Estimar el riesgo, como el impacto ponderado con la tasa de ocurrencia de la amenaza.
- El análisis se realizará mediante tablas, que permiten la identificación de la importancia relativa de los diferentes activos sometidos a amenazas.

Se han de identificar los activos necesarios para llevar a cabo la actividad. La organización puede poseer distintos tipos de activos físicos, lógicos, infraestructura, intangibles y se valorarán teniendo en cuenta los parámetros de valoración de activos.

Seguidamente se realizará un análisis de amenazas, entendiendo como tales a aquellas situaciones que pueden provocar un problema de seguridad, según el método a emplear “MAGERIT” se clasifican en estos grupos:

Accidentes: Situaciones no provocadas voluntariamente y que la mayor parte de las veces no puede evitarse. Por ejemplo: incendio, inundación, etc.
Errores: Situaciones provocadas involuntariamente provocadas por el desarrollo de las actividades cotidianas ya sea por desconocimiento y/o descuido. Por ejemplo: Errores de desarrollo, errores de actualización, etc.
Amenazas intencionales presenciales: Son provocadas por el propio personal de la organización de forma voluntaria y conociendo el daño que puede ocasionar. Por ejemplo: Accesos no autorizados, filtración de datos, etc.
Amenazas intencionales remotas: Son provocadas por terceras personas ajenas a la organización con el objetivo de dañarla. Ejemplos: Suplantación de origen, gusanos, DoS, etc.

Las vulnerabilidades en cambio, son aquellos huecos de seguridad que permiten explotar una amenaza haciendo daño a un activo. En MAGERIT no es preciso enumerar las vulnerabilidades pero sí tenerlas identificadas para poder estimar su frecuencia sobre un activo.

Por último, se tomarán las decisiones que permitan aplicar las medidas de seguridad, teniendo en cuenta el riesgo aceptable y el costo de aplicar estas medidas de seguridad.

## 3.8 Declaración de Aplicabilidad.

La norma ISO/IEC 27001:2013 indica que entre la documentación propia de todo SGSI debe incluirse la declaración de aplicabilidad, que se trata de un documento que contiene el grado de aplicabilidad que se establecen en los controles de la guía de buenas prácticas de dicha norma en su anexo A.

Esta declaración, debe ser aprobada por el comité de seguridad de la organización, como el resto de documentación y será de revisión obligatoria periódica, para adecuarlo al modelo y procesos de la organización.

Dominios ISO 27002 declaración de aplicabilidad.

| CONTROL | | | Aplica? |
|---|---|---|---|
| **5. POLITICA DE SEGURIDAD** | | | |
| **5.1 Dirección de la gestión de seguridad de la información.** | | | |
| 5.1.1 | Politicas de la seguridad de la información | Debe ser definida y aprobada por la dirección; publicarla y comunicarla a todo el personal. | SI |
| 5.1.2 | Revisión de las politicas de la seguridad de la información. | Deben ser revisados a intervalos planificados o si se producen cambios significativos para asegurar su conveniencia, adecuación y eficacia. | SI |
| **6. ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN** | | | |
| **6.1 Organización de la seguridad de la información.** | | | |
| 6.1.1 | Funciones y responsabilidades de seguridad de información. | Todas deben ser definidos y asignados. | SI |
| 6.1.2 | Segregación de funciones. | Deben estar separados para reducir las modificaciones o mal uso de los activos no autorizado o involuntario. | SI |
| 6.1.3 | Contacto con las autoridades. | Hay que actuar en el margen del conocimiento de la ley y la normativa vigente | SI |
| 6.1.4 | Contacto con grupos de especial interés. | Es recomendable mantener los contactos con foros de seguridad y asociaciones profesionales. | SI |
| 6.1.5 | Seguridad de la información en la gestión de proyectos. | Debería abordarse independientemente del tipo de proyecto. | SI |

| | | | |
|---|---|---|---|
| **6.2 Dispositivos moviles y teletrabajo.** | | | |
| 6.2.1 | Politicas de dispositivos moviles. | Deben adoptarse para gestionar los riesgos introducidos por el uso de dispositivos móviles. | SI |
| 6.2.2 | Teletrabajo | No se contempla en teletrabajo en el diseño empresarial bigente. | NO |
| **7. SEGURIDAD DE RECURSOS HUMANOS** | | | |
| **7.1 Antes de empleo.** | | | |
| 7.1.1 | Screening | Es deseable establecer los controles legalmente permitidos para todos los candidatos de acuerdo a la legislación laboral vigente y normas de seguridad. | SI |
| 7.1.2 | Terminos y condiciones de empleo | Los acuerdos contractuales con los empleados deben indicar las responsabilidades con la organización para la seguridad de la información. | SI |
| **7.2 Durante el empleo.** | | | |
| 7.2.1 | Responsabilidades de gestión | Debe exigir a todos los empleados para aplicar seguridad de la información de acuerdo con las políticas y procedimientos establecidos. | SI |
| 7.2.2 | Conciencia de seguridad de la información y entrenamiento | Todos los empleados deben recibir una adecuada formación y actualizaciones periódicas en las políticas y procedimientos acordes a su función. | SI |
| 7.2.3 | Proceso disciplinario | Debe existir un proceso disciplinario formal y comunicado. | SI |
| **7.3 Terminación y cambio de empleo.** | | | |
| 7.3.1 | Terminación o cambio de las responsabilidades de empleo | Debería ser definido, comunicado al trabajador y ejecutado. | SI |
| **8. GESTION DE ACTIVOS** | | | |
| **8.1 Responsabilidad de los activos** | | | |
| 8.1.1 | Inventario de activos | Los activos asociados a las instalaciones de procesamiento de información y la información deben ser identificados y un inventario de estos activos deben elaborarse y mantenerse. | SI |
| 8.1.2 | Propiedad de los activos | Los activos mantenidos en el inventario deben ser de propiedad. | SI |
| 8.1.3 | Retorno de los activos | Todos los empleados deben devolver todos los activos de la organización en su poder a la terminación de su empleo o contrato. | SI |
| **8.2 Clasificación de la información** | | | |
| 8.2.1 | Clasificación de la información | La información debe ser clasificada en términos de requisitos legales, el valor, la criticidad y sensibilidad a la divulgación o modificación no autorizada. | SI |
| 8.2.2 | Etiquetado de la información | Debe ser desarrollado e implementado el procedimientos para el etiquetado de la información de acuerdo con el esquema de clasificación de la información adoptado por la empresa. | SI |
| 8.2.3 | Manejo de activos | La manipulación de los activos deben ser desarrollados e implementados de acuerdo con el esquema de clasificación de la información adoptado por la empresa. | SI |
| **8.3 Manejo de Medios** | | | |
| 8.3.1 | Gestión de medios extraibles | Deberían aplicarse procedimientos para la gestión de medios extraíbles de acuerdo con el esquema de clasificación adoptado por la empresa. | SI |
| 8.3.2 | Eliminación de medios | Los medios deben ser eliminados de forma segura cuando ya no es necesario, utilizando los procedimientos formales. | SI |
| 8.3.3 | Transferencia de medios fisicos | Los medios que contienen información deben estar protegidos contra el acceso no autorizado, mal uso o la corrupción durante el transporte. | SI |
| **9. CONTROL DE ACCESO** | | | |
| **9.1 Business requirements of access control** | | | |
| 9.1.1 | Politica de control de acceso | La política de control de acceso debe ser establecida, documentada y revisada en base a los requisitos de seguridad establecidos. | SI |
| 9.1.2 | Acceso a las redes y servicios de red | Los usuarios sólo deben contar con acceso a los servicios de la red que han sido autorizados previamente. | SI |
| **9.2 Gestión de acceso de usuario** | | | |
| 9.2.1 | Registro de usuario y cancelación de registro | Un proceso formal de registro de usuario y la cancelación del registro debe ser implementado para permitir la asignación de derechos de acceso. | SI |
| 9.2.2 | Acceso aprovisionamiento de usuario | Un proceso de provisión de acceso de usuarios formal debe ser implementado para asignar o revocar los derechos de acceso para todos los usuario a todos los sistemas y servicios. | SI |

| | | | |
|---|---|---|---|
| 9.2.3 | Gestión de derechos de accesos privilegiados | La asignación y utilización de los derechos de acceso privilegiados deben ser restringidas y controladas. | SI |
| 9.2.4 | Gestión de la información de autentificación de secreto de los usuarios | La asignación de la información de autenticación debe ser controlada a través de un proceso de gestión formal. | SI |
| 9.2.5 | Revisión de los derechos de acceso de usuario | Los propietarios de activos deben revisar los derechos de acceso de los usuarios a intervalos regulares. | SI |
| 9.2.6 | Eliminación o ajuste de los derechos de acceso | Los derechos de acceso de todos los empleados a las instalaciones de procesamiento de información y a la misma información en si, deben ser retirados a la terminación de su empleo o contrato. | SI |
| **9.3 Responsabilidades del usuario** | | | |
| 9.3.1 | Uso de información secreta de autenticación | Los usuarios deben ser obligados a seguir las prácticas de la organización en el uso de información secreta de autenticación. | SI |
| **9.4 Control de sistemas y acceso a las aplicaciones** | | | |
| 9.4.1 | Restricción del acceso a la información | El acceso a la información y sistema de aplicación debe limitarse de acuerdo con la política de control de acceso. | SI |
| 9.4.2 | Procedimiento de inicio de sesión seguro | El acceso a los sistemas y aplicaciones debe ser controlado por un procedimiento de conexión segura. | SI |
| 9.4.3 | Sistema de gestión de contraseñas | Deben ser un sistema que asegurarse de contraseñas de calidad. | SI |
| 9.4.4 | Uso de programas de servicios publicos privilegiados | El uso de estos programas capaces de anular sistemas y aplicaciones debe ser restringido y estrechamente controlado. | SI |
| 9.4.5 | Control de acceso al codigo fuente del programa | El acceso al código fuente del programa debe ser restringido. | SI |
| **10. CRIPTOGRAFIA** | | | |
| **10.1 Controles criptograficos** | | | |
| 10.1.1 | Politica sobre el uso de controles criptograficos | La política sobre el uso de controles criptográficos para la protección de la información debe ser desarrollado e implementado. | SI |
| 10.1.2 | Gestión de Claves | La política sobre uso, protección y duración de las claves de cifrado debe ser desarrollado e implementado. | SI |
| **11. SEGURIDAD FISICA Y AMBIENTAL** | | | |
| **11.1 Areas seguras** | | | |
| 11.1.1 | Perímetro de seguridad física | Debe definirse áreas protegidas de los lugares que contienen información y se procesa información, ya sea instalaciones sensibles o críticas. | SI |
| 11.1.2 | Controles de entrada fisicas | Se deben proteger las zonas de seguridad por los controles de entrada adecuados para garantizar el acceso sólo del personal autorizado. | SI |
| 11.1.3 | Asegurar oficinas habitaciones e instalaciones | Debe ser diseñada y aplicada una norma para la seguridad física de oficinas, salas e instalaciones. | SI |
| 11.1.4 | Protección contra amenazas externas y ambientales | Debe ser diseñada y aplicada una norma de protección física contra los desastres naturales, ataques maliciosos o accidentes. | SI |
| 11.1.5 | Trabajar en zonas seguras | Procedimientos para trabajar en zonas seguras deberían diseñarse y aplicarse. | SI |
| 11.1.6 | Zonas de entrega y carga | Los puntos de acceso, las zonas de entrega y de carga y otros puntos en los que personas no autorizadas puedan entrar en los locales deberán ser controlados y aislados de las instalaciones de procesamiento de información para evitar el acceso no autorizado. | SI |
| **11.2 Equipo** | | | |
| 11.2.1 | Ubicación y protección del equipo | El equipo debe estar ubicado y protegido para reducir los riesgos de las amenazas ambientales y los riesgos y las oportunidades de acceso no autorizado. | |
| 11.2.2 | Apoyo a los servicios publicos | El equipo debe ser protegido de fallas de energía y otros trastornos causados por fallas en el apoyo a los servicios públicos. | SI |
| 11.2.3 | Seguridad de cableado | El cableado que transporta datos debe estar debidamente protegido, igualmente aquel de apoyo a los servicios de información debe ser protegida de intercepción, interferencia o ataque | SI |
| 11.2.4 | Mantenimiento de los equipos | El equipo debe mantenerse correctamente para asegurar su disponibilidad e integridad continua. | SI |
| 11.2.5 | Eliminación de los activos | Debe contemplarse una normas para la elimi nación de los equipos y e informaciones obsoletas. | SI |
| 11.2.6 | Seguridad de equipo y activos fuera de las instalaciones | No esta contemplado en la organización | NO |

| | | | |
|---|---|---|---|
| 11.2.7 | Eliminación segura o reutilización de los equipos | Todos los artículos que contengan soportes de almacenamiento deben ser verificados para asegurar que los datos sensibles y software con licencia ha sido eliminado o sobrescrito de forma segura antes de su eliminación o reutilización. | SI |
| 11.2.8 | Equipos de usuario desatendidos | Se debe asegurar que el equipo desatendido tiene la protección adecuada. | SI |
| 11.2.9 | Escritorio limpio y politica pantalla limpia | Debe adoptase una política de escritorio limpio de papeles y soportes de almacenamiento extraíbles y una política clara pantalla para las instalaciones de procesamiento de la información. | SI |
| **12. OPERACIONE S DE SEGURIDAD** | | | |
| **12.1 Procedimientosy responsabilidades operacionales** | | | |
| 12.1.1 | Procedimientos operativos documentales | Los procedimientos operativos deben ser documentados y puestos a disposición de todos los usuarios que los necesitan. | SI |
| 12.1.2 | Gestión del cambio | Los cambios en la organización, procesos de negocio, instalaciones de procesamiento de información y sistemas que afectan a la seguridad de información deben ser controlados. | SI |
| 12.1.3 | Gestión de la capadidad | El uso de los recursos debe ser monitoreado, ajustandolo y anticipandose a las futuras necesidades de capacidad para garantizar el rendimiento del sistema requerido. | SI |
| 12.1.4 | Separación de desarrollo, pruebas y entornos operativos | Desarrollo, pruebas y entornos operativos deben ser separados para reducir los riesgos de acceso o cambios no autorizados al entorno operativo. | SI |
| **12.2 Protección contra el malware** | | | |
| 12.2.1 | Controles contra el malware | Detección, prevención y recuperación de controles para proteger contra el malware debe ser implementado, en combinación con el conocimiento | SI |
| **12.3 Copias de seguridad** | | | |
| 12.3.1 | Copia de seguridad de la información | Las copias de seguridad de la información, software y sistemas de imágenes deben ser tomadas y analizadas regularmente de acuerdo con una política de copia de seguridad convenido. | SI |
| **12.4 Registro y seguimiento** | | | |
| 12.4.1 | Registro de eventos | Los registros de eventos registran las actividades del usuario, excepciones, errores y eventos de seguridad de la información se deben producir, mantenidos y revisados con regularidad. | SI |
| 12.4.2 | Protección de la información de los registros | Registro de instalaciones y registrar la información debe ser protegida contra la manipulación y acceso no autorizado. | SI |
| 12.4.3 | Registros de administración y operación | Administrador del sistema y las actividades del operador del sistema deben ser registrados y sus troncos protegidos y regularmente revisados. | SI |
| 12.4.4 | Sincronización del reloj | Los relojes de todos los sistemas de procesamiento de información pertinentes dentro de una organización o dominio de seguridad deben estar sincronizados a una sola fuente de tiempo de referencia. | SI |
| **12.5 Control del software operativo** | | | |
| 12.5.1 | Apoyo a los servicios publicos | Deberían aplicarse procedimientos para controlar la instalación del software en los sistemas operativos. | SI |
| **12.6 Técnico de gestión de vulnerabilidades** | | | |
| 12.6.1 | Gestión de vulnerabilidades técnicas | Información acerca de las vulnerabilidades técnicas de los sistemas de información que se utilicen deben ser obtenidos de manera oportuna, la exposición de la organización a tales vulnerabilidades evaluado y tomado las medidas adecuadas para hacer frente a los riesgos asociados. | SI |
| 12.6.2 | Restricciones de instalación de software | Las normas que rigen la instalación de software los usuarios deben establecerse e implementarse. | SI |
| **12.7 Sistemas de la información consideraciones de auditoria** | | | |
| 12.7.1 | Sistemas de información controles de auditoria | Requisitos y actividades de verificación de los sistemas operativos de auditoría deben ser cuidadosamente planificadas y acordadas para reducir al mínimo las interrupciones de los procesos de | SI |
| **13. SEGURIDAD DE LAS COMUNICACIONE S** | | | |
| **13.1 Gestión de la seguridad de la red** | | | |
| 13.1.1 | Funciones y responsabilidades de seguridad de información. | Las redes deben ser gestionados y controlados para proteger la información en los sistemas y aplicaciones. | SI |
| 13.1.2 | Segregación de funciones. | Los mecanismos de seguridad, niveles de servicio y los requisitos de gestión de todos los servicios de la red deben ser identificados e incluidos en los acuerdos de servicios de red. | SI |

| | | | |
|---|---|---|---|
| 13.1.3 | Segregación en Redes. | Grupos de servicios de información, los usuarios y los sistemas de información deben ser segregados en las redes. | SI |
| **13.2 Transferencia de Información** | | | |
| 13.2.1 | Politicas y procedimientos de transferencia de información | Normas de transferencia de políticas, procedimientos y controles deben estar en su lugar para proteger la transferencia de información a través del uso de todo tipo de instalaciones de comunicación. | SI |
| 13.2.2 | Acuerdos sobre la transferencia de información | Los contratos deben abordar la transferencia segura de información comercial entre la organización y las partes externas. | SI |
| 13.2.3 | Mensajería electrónica | La información involucrado en la mensajería electrónica debe ser protegido de manera apropiada. | SI |
| 13.2.4 | Acuerdos de confidenciabilidad o de no divulgación | Deben ser identificados, revisados y documentados con regularidad los requisitos para los acuerdos de confidencialidad o de no divulgación que reflejen las necesidades de la organización para la protección de la información | SI |
| **14. SISTEMA DE ADQUISICIÓN, DESARROLLO Y MANTENIMIE** | | | |
| **14.1 Security requirements of information system** | | | |
| 14.1.1 | Información de analisis de requisitos de seguridad y la especificación | Los requisitos relacionados con la seguridad de la información deben ser incluidos en los requisitos para los nuevos sistemas de información o mejoras a los sistemas de información existentes. | SI |
| 14.1.2 | Asegurar los servicios de aplicaciones en las redes publicas | La Información involucrada en los servicios de aplicaciones que pasan a través de redes públicas debe protegerse de la actividad fraudulenta, disputa contractual y la divulgación no autorizada y modificación | SI |
| 14.1.3 | Protección de las transacciones de servicios de aplicaciones | La información involucrado en las transacciones de servicios de aplicación debe ser protegido para prevenir la transmisión incompleta, errónea enrutamiento, alteración mensaje no autorizado, revelación no autorizada, la duplicación de mensajes no autorizado o la repetición | SI |
| **14.2 Seguridad en los procesos de desarrollo y de apoyo** | | | |
| 14.2.1 | Politica de desarrollo seguro | No se el desarrollo de software en la organización. | NO |
| 14.2.2 | Procedimientos de control de cambio del sistema | No se el desarrollo de software en la organización. | NO |
| 14.2.3 | Revisión técnica de las aplicaciones tras efectuar cambios en la plataforma operativo | Cuando se cambian las plataformas que operan, aplicaciones críticas de negocio deben ser revisados y probados para asegurar que no hay impacto adverso en las operaciones de la organización o de seguridad | SI |
| 14.2.4 | Restricciones a los cambios de los paquetes de software | No se el desarrollo de software en la organización. | NO |
| 14.2.5 | Principios de ingeniería de sistemas seguros | No se el desarrollo de software en la organización. | NO |
| 14.2.6 | Entorno de desarrollo seguro | No se el desarrollo de software en la organización. | NO |
| 14.2.7 | Desarrollo outsourced | No se el desarrollo de software en la organización. | NO |
| 14.2.8 | Pruabas de seguridad del sistema | No se el desarrollo de software en la organización. | NO |
| 14.2.9 | Pruebas de aceptación del sistema | No se el desarrollo de software en la organización. | NO |
| **14.3 Datos de prueba** | | | |
| 14.3.1 | Protección de datos de prueba | Los datos de prueba deben seleccionarse cuidadosamente, protegidos y controlados. | SI |
| **15.RELACIÓN CON PROVEEDORES** | | | |
| **15.1 Seguridad en la información en las relaciones con provee** | | | |
| 15.1.1 | Politica de seguridad de la información para relaciones con los proveedores | Los requisitos de seguridad de la información para la mitigación de los riesgos asociados con el acceso del proveedor a los activos de la organización deben arreglarse con el proveedor y documentados | SI |
| 15.1.2 | Abordar la seguridad dentro de los acuerdos con proveedores | Todos los requisitos de seguridad de la información pertinentes deben ser establecidos y acordados con cada proveedor que pueden acceder, procesar, almacenar, comunicar, o proporcionar TI componentes de la infraestructura de información de la organización | SI |
| 15.1.3 | Cadena de la información y tecnologia de comunicación de suministro | Los acuerdos con los proveedores deberían incluir requisitos para hacer frente a los riesgos de seguridad de información asociados a los servicios de información y tecnología de las comunicaciones y de la cadena de suministro de productos | SI |
| **15.2 Gestión de la prestación de servicios de proveedores** | | | |
| 15.2.1 | Politica de desarrollo seguro | Se deben controlar regularmente, revisión y auditoría de proveedores la prestación de servicios. | SI |
| 15.2.2 | Procedimientos de control de cambio del sistema | Los cambios en la prestación de servicios por parte de los proveedores, incluyendo el mantenimiento y la mejora de las políticas, procedimientos y controles de seguridad de la información existentes, se deben manejar, teniendo en cuenta la criticidad de la información empresarial, los sistemas y los procesos involucrados y re-evaluación de los riesgos | SI |

| | | | |
|---|---|---|---|
| **16. INFORMACIÓN DE GESTIÓN DE INCIDENCIAS DE SEGURI** | | | |
| **16.1 Gestión de incidencias de seguridad de la información y** | | | |
| 16.1.1 | Responsabilidades y procedimientos | Responsabilidades y procedimientos de gestión deben ser establecidos para garantizar una respuesta rápida, eficaz y ordenada a los incidentes de seguridad de la información | SI |
| 16.1.2 | Presentación de informes de eventos de seguridad de información | Los eventos de seguridad de la información deben ser reportados a través de canales de gestión adecuadas tan pronto como sea posible. | SI |
| 16.1.3 | Informes debilides de seguridad de información | Los empleados que utilizan los sistemas y servicios de información de la organización deberían estar obligados a observar y reportar cualquier debilidad de seguridad de información observados o sospechados en los sistemas o servicios. | SI |
| 16.1.4 | Evaliación y decisión sobre los eventos de seguridad de información | Los eventos de seguridad de la información deben ser evaluados y que se deben decidir si han de ser clasificados como incidentes de seguridad de la información. | SI |
| 16.1.5 | Respuestas a incidentes de seguridad de la información | Los incidentes de seguridad de la información deben ser respondidos de acuerdo con los procedimientos documentados. | SI |
| 16.1.6 | Aprendiendo de los incidentes de seguridad de la información | Los conocimientos adquiridos desde el análisis y la resolución de los incidentes de seguridad de la información debe utilizarse para reducir la probabilidad o el impacto de futuros incidentes. | SI |
| 16.1.7 | Acopio de pruebas | La organización debe definir y aplicar procedimientos para la identificación, recolección, adquisición y conservación de la información, que puede servir como prueba. | SI |
| **17. ASPECTOS DE SEGURIDAD DE INFORMACIÓN DE LA GE** | | | |
| **17.1 Información continuidad seguridad** | | | |
| 17.1.1 | Planificación información continuidad seguridad | La organización debe determinar sus necesidades de seguridad de la información y la continuidad de la gestión de seguridad de la información en situaciones adversas. | SI |
| 17.1.2 | Implementación de la información continuidad seguridad | La organización debe establecer, documentar, implementar y mantener procesos, procedimientos y controles que garanticen el nivel necesario de continuidad para la seguridad de la información durante una situación adversa. | SI |
| 17.1.3 | Verificar, revisar y evaluar la información de seguridad continuidad | La organización debe verificar la información controles de continuidad de seguridad establecido y aplicado a intervalos regulares con el fin de asegurarse de que son válidos y eficaces en situaciones adversas. | SI |
| **17.2 Despidos** | | | |
| 17.2.1 | Disponibilidad de instalaciones de procesamiento de información | Las instalaciones de procesamiento de la información deben ser implementados con redundancia suficiente para satisfacer los requisitos de disponibilidad. | SI |
| **18. CONFORMIDAD** | | | |
| **18.1 Cumplimiento de los requisitos legales y contractuales** | | | |
| 18.1.1 | Identificación de la legislación aplicable y requisitos contractuales | La adecuadión a la leguislación vigente, los requisitos reglamentarios, contractuales y el enfoque de la organización para cumplir con estos requisitos deben ser identificados de manera explícita, documentados y actualizados a la fecha de cada sistema de información y la organización. | SI |
| 18.1.2 | Derechos de propiedad intelectual | Se deben implementar procedimientos apropiados para garantizar el cumplimiento de requisitos legales, reglamentarios y contractuales relacionados con los derechos de propiedad intelectual y el uso de productos de software privativo. | SI |
| 18.1.3 | Protección de los registros | Los registros deben estar protegidos contra pérdida, destrucción, falsificación, acceso no autorizado y la liberación no autorizada, de conformidad con los requisitos legiales, reglamentarios, contractuales y comerciales. | SI |
| 18.1.4 | Privacidad y protección de datos personales | Se debe garantizar lo dispuesto en la legislación y la regulación oportuna la privacidad y protección de la información de identificación personal que se maneje. | SI |
| 18.1.5 | Reglamento de los controles criptograficos | Los controles criptográficos deben ser utilizados en el cumplimiento de todos los acuerdos pertinentes, la legislación y los reglamentos. | SI |
| **18.2 Revisiones de seguridad de información** | | | |
| 18.2.1 | Revisión independiente de seguridad de la información | Los objetivos de control, controles, políticas, procesos y procedimientos de seguridad de la información, deben ser revisado de forma independiente a intervalos planificados o cuando se producen cambios significativos. | SI |
| 18.2.2 | Cumplimiento de las politicas y etandares de seguridad | La dirección debe comprobar periódicamente el cumplimiento de los procedimientos de procesamiento y la información dentro de su área de responsabilidad con las políticas de seguridad, las normas y otros requisitos de seguridad. | SI |
| 18.2.3 | Revisión del cumplimiento técnico | Los sistemas de información deben ser revisados regularmente por el cumplimiento de las políticas y normas de seguridad de la información de la organización. | SI |

# 4. Análisis de Riesgos.

## 4.1 Inventario de activos.

El propósito del análisis de riesgos es determinar, para intereses de la empresa, el nivel de riesgo que se enfrenta, con las salvaguardas implementadas.

El estudio de los activos vinculados a la información es el primer punto para el análisis de riesgos, para ello utilizaremos la metodología MAGERIT. En esta técnica se entiende como activo a aquellos recursos del sistema de información o relacionados con éste, necesarios para que la organización funcione correctamente y alcance los objetivos propuestos por su dirección. Igualmente, se puede definir activo como todo bien de la organización relacionados con la actividad de la misma.

La metodología MAGERIT agrupa estos activos en los siguientes grupos:

- Instalaciones. I
- Hardware. H
- Datos. D
- Red. R
- Servicios. S
- Equipamiento auxiliar. X
- Personas. P

El inventario de activos se muestra a continuación:

| Ambito | ID | Activo |
|---|---|---|
| Instalaciones | I1 | CPD |
| | I2 | Aulas Formación |
| | I3 | Taller reparación |
| | I4 | Almacen |
| | I5 | Armarios de Red |
| | I6 | Resto de habitaculos |
| Hardware | H1 | Controladores de Dominio 2008 Server (2) |
| | H2 | Servidor DHCP |
| | H3 | Servidor Datos departamentales |
| | H4 | Servidor Copias Seguridad |
| | H5 | Servidor ERP |
| | H6 | Servidsor Base de Datos SQl Server |
| | H7 | PC Firewall-Snifer |
| | H8 | Puestos de Usuario (26) |
| | H9 | PCs Aulas (40) |
| | H10 | Servidores Formación (Windows Linux) |
| | H11 | Proyectores aulas formación (2) |

| | | |
|---|---|---|
| Aplicación | S1 | Sistemas Microsoft Windows Server 2008 |
| | S2 | Software Microsoft SQL Server 2008 |
| | S3 | Acronis Backup Advanced |
| | S4 | Software ERP SAP |
| | S5 | Software Trend Micro System |
| | S6 | Sistema Operativo Linux Red-Hat |
| | S7 | Sistema Operativo Ubuntu |
| | S8 | Sistemas Microsoft Windows 7 |
| | S9 | Herramienta Microsoft Office 2010 |
| | S10 | Herramienta Open-Office |
| | S11 | Adobe acrobat professional |
| Datos | D1 | Base de datos SQl |
| | D2 | Base de datos SAP |
| Red | R1 | Cableado interior estructurado |
| | R2 | Conexión VDSL corportiva |
| | R3 | Conexión ADSL formación |
| | R4 | Conexión ADSL Taller |
| | R5 | Conexión ADSL Almacen |
| | R6 | Telefonia IP Sede Central |
| | R7 | Telefonia basica Taller |
| | R8 | Telefonia basica Almacen |
| | R9 | Red Electrica |
| E. Auxiliar | X1 | Sistema climatización centralizado |
| | X2 | Sistema detección Incendios |
| | X3 | Sistema Alimentación Ininterrumpido CPD |
| | X4 | Sistema de Alarma (Externo contratado) |
| | X5 | Sistema telefonico IP Cisco IP Fone |
| Personal | P1 | Administrador Único |
| | P2 | Responsable de Administración |
| | P3 | Jefe de Estudios |
| | P4 | Director Comercial |
| | P5 | Director TIC |
| | P6 | Responsable Área Técnica |
| | P7 | Responsable Almacen |
| | P8 | Personal Administración (3) |
| | P9 | Administrativos Formación (2) |
| | P10 | Comerciales (x) |
| | P11 | Personal técnico especialista (10) |
| | P12 | Personal técnico medio (5) |
| | P13 | Formadores (personal externo) |

## 4.2 Valoración de los activos.

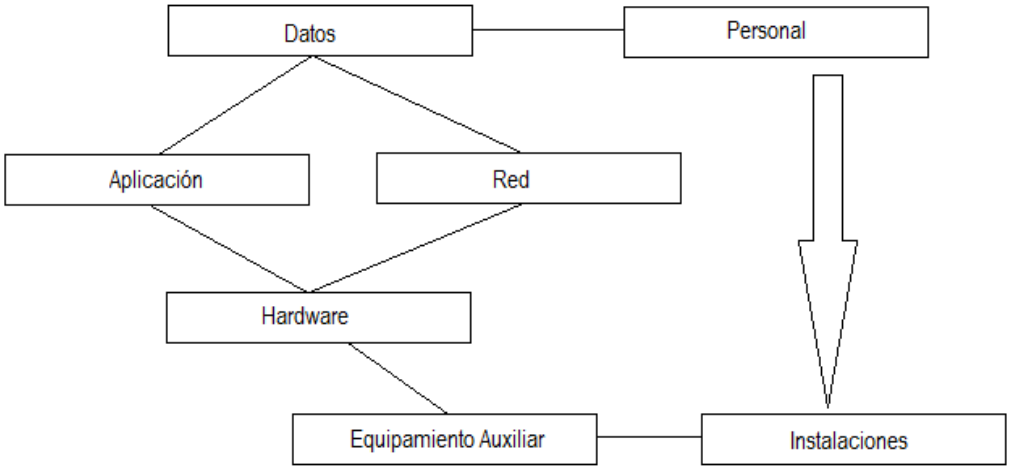
La valoración de los activos se basa en el coste presumido de cada uno de ellos, fijándonos en el coste que supondría para nuestra organización la reposición de cada activo, en caso de que se deba proceder a su reposición.

La valoración cuantitativa de los activos, se ha separado según las categorías que se definieron en la página 22 donde se indica la metodología para el análisis de riesgos:

| VALORACIÓN DE ACTIVOS | | |
|---|---|---|
| MA | 500.000,00 € | Muy Alto |
| A | 100.000,00 € | Alto |
| M | 30.000,00 € | Medio |
| B | 3.000,00 € | Bajo |
| N | 500,00 € | Muy Bajo |

La dependencia entre activos hace constatando su jerarquización, siendo el caso de que una amenaza que afecta a un activo del que dependa otro activo superior, tendrá impacto directo sobre este activo superior.

El resultado de este análisis será un árbol de dependencias de activos en el que se podrá ver la relación existente:




| Nº | ID | Grupo | Activo | Valoración |
|---|---|---|---|---|
| 1 | I1 | Instalaciones | CPD | MA |
| 2 | I2 | Instalaciones | Aulas Formación | A |
| 3 | I3 | Instalaciones | Taller reparación | M |
| 4 | I4 | Instalaciones | Almacen | M |
| 5 | I5 | Instalaciones | Armarios de Red | B |
| 6 | I6 | Instalaciones | Resto de habitaculos | M |
| 7 | H1 | Hardware | Controladores de Dominio 2008 Server (2) | MA |
| 8 | H2 | Hardware | Servidor DHCP | MA |
| 9 | H3 | Hardware | Servidor Datos departamentales | A |
| 10 | H4 | Hardware | Servidor Copias Seguridad | B |
| 11 | H5 | Hardware | Servidor ERP | M |
| 12 | H6 | Hardware | Servidsor Base de Datos SQL Server | A |

| | | | | |
|---|---|---|---|---|
| 13 | H7 | Hardware | PC Firewall-Snifer | B |
| 14 | H8 | Hardware | Puestos de Usuario (26) | B |
| 15 | H9 | Hardware | PCs Aulas (40) | MB |
| 16 | H10 | Hardware | Servidores Formación (Windows Linux) | M |
| 17 | H11 | Hardware | Proyectores aulas formación (2) | B |
| 18 | S1 | Aplicación | Sistemas Microsoft Windows Server 2008 | A |
| 19 | S2 | Aplicación | Software Microsoft SQL Server 2008 | A |
| 20 | S3 | Aplicación | Acronis Backup Advanced | A |
| 21 | S4 | Aplicación | Software ERP SAP | M |
| 22 | S5 | Aplicación | Software Trend Micro System | M |
| 23 | S6 | Aplicación | Sistema Operativo Linux Red-Hat | B |
| 24 | S7 | Aplicación | Sistema Operativo Ubuntu | B |
| 25 | S8 | Aplicación | Sistemas Microsoft Windows 7 | B |
| 26 | S9 | Aplicación | Herramienta Microsoft Office 2010 | B |
| 27 | S10 | Aplicación | Herramienta Open-Office | B |
| 28 | S11 | Aplicación | Adobe acrobat professional | B |
| 29 | D1 | Datos | Base de datos SQL | A |
| 30 | D2 | Datos | Base de datos SAP | A |
| 31 | R1 | Red | Cableado interior estructurado | M |
| 32 | R2 | Red | Conexión VDSL corportiva | M |
| 33 | R3 | Red | Conexión ADSL formación | B |
| 34 | R4 | Red | Conexión ADSL Taller | B |
| 35 | R5 | Red | Conexión ADSL Almacen | B |
| 36 | R6 | Red | Telefonia IP Sede Central | B |
| 37 | R7 | Red | Telefonia basica Taller | MB |
| 38 | R8 | Red | Telefonia basica Almacen | MB |
| 39 | R9 | Red | Red Electrica | MA |
| 40 | X1 | E. Auxiliar | Sistema climatización centralizado | M |
| 41 | X2 | E. Auxiliar | Sistema detección Incendios | A |
| 42 | X3 | E. Auxiliar | Sistema Alimentación Ininterrumpido CPD | A |
| 43 | X4 | E. Auxiliar | Sistema de Alarma (Externo contratado) | A |
| 44 | X5 | E. Auxiliar | Sistema telefonico IP Cisco IP Fone | A |
| 45 | P1 | Personal | Administrador Único | MA |
| 46 | P2 | Personal | Responsable de Administración | A |
| 47 | P3 | Personal | Jefe de Estudios | A |
| 48 | P4 | Personal | Director Comercial | A |
| 49 | P5 | Personal | Director TIC | A |
| 50 | P6 | Personal | Responsable Área Técnica | M |
| 51 | P7 | Personal | Responsable Almacen | M |
| 52 | P8 | Personal | Personal Administración (3) | M |
| 53 | P9 | Personal | Administrativos Formación (2) | M |
| 54 | P10 | Personal | Comerciales (x) | B |
| 55 | P11 | Personal | Personal técnico especialista (10) | M |
| 56 | P12 | Personal | Personal técnico medio (5) | B |
| 57 | P13 | Personal | Formadores (personal externo) | M |

## 4.3 Dimensiones de seguridad.

Una vez identificados los activos, hay que valorarlos según su impacto en las cinco dimensiones de la seguridad informática, autenticidad, confidencialidad, integridad, disponibilidad y trazabilidad, dicho de otro modo por sus siglas ACIDT.

| Dimensiones de seguridad | |
|---|---|
| A | Autenticidad |
| C | Confidencialidad |
| I | Integridad |
| D | Disponibilidad |
| T | Trazabilidad |

Autenticidad: perjuicio de no conocer quién es el autor de alguna acción sobre el activo o del propio activo.

Confidencialidad: perjuicio que ocasionaría que el archivo sea conocido por alguien que no deba

Integridad: perjuicio de que el archivo esté dañado o se corrompiera.

Disponibilidad: perjuicio de que tener acceso al archivo por no tenerlo o no poder utilizarlo.

Trazabilidad: perjuicio de no conocer a quien se le presta el activo, lo que se hace con él, cómo y cuándo. Así como desconocer quienes acceden a determinados archivos y para qué son utilizados.

Desde el punto de vista de la seguridad, junto a la valoración en sí de los activos debe indicarse cuál es el aspecto de la seguridad más crítico. Esto será de ayuda en el momento de pensar en posibles salvaguardas, ya que estas se enfocarán en los aspectos que más nos interesen.

El valor que reciba un activo puede ser propio o acumulado. El valor propio asignará a la información, quedando el resto de activos subordinados a las necesidades de explotación y protección de la información. Así, los activos inferiores en un esquema de dependencias acumulan el valor de los activos que se apoyan en ellos.

En este caso utilizaremos una escala de valoración de diez valores siguiendo los siguientes criterios:

| VALOR | CRITERIO |
|---|---|
| 10 | Daño muy grave a la organización |
| 7-9 | Daño grave a la organización |
| 4-6 | Daño importante a la organización |
| 1-3 | Daño menor a la organización |
| 0 | Irrelevante para la organización |

4.4 Tabla resumen de la valoración.

| Ambito | ID | Activo | Valor | ASPECTOS CRITICOS | | | | |
|---|---|---|---|---|---|---|---|---|
| | | | | A | C | I | D | T |
| Instalaciones | I1 | CPD | MA | 10 | 10 | 10 | 10 | 10 |
| Instalaciones | I2 | Aulas formación | A | 0 | 5 | 5 | 0 | 7 |
| Instalaciones | I3 | Taller reparación | M | 0 | 5 | 5 | 0 | 7 |
| Instalaciones | I4 | Almacen | M | 0 | 5 | 5 | 0 | 7 |
| Instalaciones | I5 | Armarios de red | B | 0 | 0 | 0 | 7 | 0 |
| Instalaciones | I6 | Resto de habitaculos | M | 0 | 5 | 5 | 0 | 6 |
| Hardware | H1 | Controladores de Dominio 2008 Server | MA | 9 | 8 | 8 | 10 | 7 |
| Hardware | H2 | Servidor DHCP | MA | 8 | 8 | 8 | 9 | 7 |
| Hardware | H3 | Servidor datos departamentales | A | 9 | 9 | 9 | 10 | 8 |
| Hardware | H4 | Servidor copias de seguridad | B | 5 | 5 | 7 | 7 | 7 |
| Hardware | H5 | Servidor ERP | M | 9 | 9 | 9 | 10 | 7 |
| Hardware | H6 | Servidor Base de Datos SQL Server | A | 9 | 7 | 9 | 10 | 8 |
| Hardware | H7 | PC Firewall-Snifer | B | 0 | 7 | 3 | 5 | 7 |
| Hardware | H8 | Puestos de Usuario | B | 7 | 9 | 7 | 7 | 9 |
| Hardware | H9 | PCs aulas | MB | 6 | 6 | 7 | 6 | 7 |
| Hardware | H10 | Servidores formación (Windows-Linux) | M | 6 | 6 | 7 | 6 | 7 |
| Hardware | H11 | Proyectores aulas formación | B | 5 | 5 | 7 | 5 | 5 |
| Aplicación | S1 | Sistemas Microsofft Windows Server 2008 | A | 7 | 7 | 7 | 9 | 9 |
| Aplicación | S2 | Software Microsoft SQL Server 2008 | A | 7 | 7 | 7 | 9 | 9 |
| Aplicación | S3 | Acronis Backup Advanced | A | 7 | 9 | 9 | 9 | 9 |
| Aplicación | S4 | Software ERP SAP | M | 7 | 9 | 9 | 9 | 9 |
| Aplicación | S5 | Software Trend Micro System | M | 7 | 9 | 7 | 9 | 7 |
| Aplicación | S6 | Sistemas operativo Linux Red-Hat | B | 7 | 7 | 7 | 7 | 7 |
| Aplicación | S7 | Sistema operativo Ubuntu | B | 7 | 7 | 7 | 7 | 7 |
| Aplicación | S8 | Sistemas Microsoft Windows 7 | B | 7 | 7 | 7 | 7 | 7 |
| Aplicación | S9 | Herramienta Microsoft Office 2010 | B | 7 | 7 | 7 | 7 | 7 |
| Aplicación | S10 | Herramienta Open-Office | B | 7 | 7 | 7 | 7 | 7 |
| Aplicación | S11 | Adobe acrobat professional | B | 5 | 5 | 5 | 5 | 5 |
| Datos | D1 | Base de datos SQL | A | 9 | 9 | 9 | 9 | 9 |
| Datos | D2 | Base de datos SAP | A | 9 | 9 | 9 | 9 | 9 |
| Red | R1 | Cableado interior estructurado | M | 3 | 3 | 6 | 7 | 5 |
| Red | R2 | Conexión VDSL corporativa | M | 5 | 5 | 8 | 8 | 8 |
| Red | R3 | Conexión ADSL formación | B | 5 | 5 | 7 | 7 | 7 |
| Red | R4 | Conexión ADSL Taller | B | 4 | 4 | 6 | 6 | 6 |
| Red | R5 | Conexión ADSL Almacen | B | 4 | 4 | 6 | 6 | 6 |
| Red | R6 | Telefonia IP Sede Central | B | 7 | 7 | 7 | 9 | 7 |
| Red | R7 | Telefonia basica Taller | MB | 7 | 7 | 7 | 9 | 7 |
| Red | R8 | Telefonia basica Almacen | MB | 7 | 7 | 7 | 9 | 7 |
| Red | R9 | Red Electrica | MA | 0 | 0 | 6 | 7 | 5 |
| E. Auxiliar | X1 | Sistema climatización centralizado | M | 0 | 0 | 0 | 9 | 0 |
| E. Auxiliar | X2 | Sistema detección incendios | A | 0 | 0 | 0 | 9 | 0 |
| E. Auxiliar | X3 | Sistema alimentación ininterrumpida CPD | A | 0 | 0 | 0 | 9 | 0 |
| E. Auxiliar | X4 | Sistema de Alarma (Externo contratado) | A | 0 | 0 | 0 | 9 | 0 |
| E. Auxiliar | X5 | Sistema telefonico IP Cisco IP Fone | A | 0 | 0 | 0 | 9 | 0 |
| Personal | P1 | Administrador único | MA | 0 | 0 | 0 | 8 | 0 |
| Personal | P2 | Responsable de administración | A | 0 | 0 | 0 | 7 | 0 |
| Personal | P3 | Jefe de estudios | A | 0 | 0 | 0 | 7 | 0 |
| Personal | P4 | Director comercial | A | 0 | 0 | 0 | 7 | 0 |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| Personal | P5 | Director TIC | A | 0 | 0 | 0 | 9 | 0 |
| Personal | P6 | Responsable Area Técnica | M | 0 | 0 | 0 | 7 | 0 |
| Personal | P7 | Responsable Almacen | M | 0 | 0 | 0 | 7 | 0 |
| Personal | P8 | Personal Administración | M | 0 | 0 | 0 | 7 | 0 |
| Personal | P9 | Administrativos formación | M | 0 | 0 | 0 | 7 | 0 |
| Personal | P10 | Comerciales | B | 0 | 0 | 0 | 7 | 0 |
| Personal | P11 | Personal técnico especialista | M | 0 | 0 | 0 | 7 | 0 |
| Personal | P12 | Personal técnico medio | B | 0 | 0 | 0 | 7 | 0 |
| Personal | P13 | Formadores | M | 0 | 0 | 0 | 7 | 0 |

## 4.5 Análisis de amenazas.

Se realiza este análisis, para establecer la estimación de vulnerabilidades de cada activo frente a la materialización de la amenaza, teniendo en cuenta la frecuencia con que pudiera producirse y el impacto de en caso de producirse incida sobre la seguridad. Utilizamos la tabla inicial de amenazas usada en MAGERIT libro 2 - punto 5 “Catalogo de elementos”, que clasifica las amenazas en cuatro bloques:

[N] Desastres Naturales.
[I] Desastres de origen Industrial.
[E] Errores y/o fallos no intencionados.
[A] Ataques intencionados.

Como indicamos en el punto anterior, los activos se valoran en cuanto a importancia en Muy Alta, Alta, Media, Baja o Despreciable; con los criterios que se señalaron en el cuadro al efecto.

En cuanto a la frecuencia, ya se indico la escala en el punto 32.7 de este trabajo, tratándose de una escala basada en la cantidad de incidencias en un periodo menos a un año:

| FRECUENCIA (en la que puede materializarse) | | | |
|---|---|---|---|
| EF | 0,9973 | Extremadamente frecuente | Menos que 1 día |
| MF | 0,1425 | Muy Frecuente | Menos que 1 semana |
| F | 0,0329 | Frecuente | Menos que un mes |
| FN | 0,0055 | Frecuencia Normal | Menos que medio año |
| PF | 0,0027 | Poco Frecuente | Menos que un año |
| EPF | 0,0003 | Extremadamente Poco Frecuente | Menos que diez años |

Tabla resumen Análisis de amenazas:

| | Amenaza | Tipo de activo | Frecuencia | [A] | [C] | [I] | [D] | [T] |
|---|---|---|---|---|---|---|---|---|
| [N] | Desastres narutales. | | | | | | | |
| [N.1] | Fuego | Hardware | 1 | | | | 60% | |
| | | Media | 1 | | | | 60% | |
| | | Equipamiento Auxiliar | 1 | | | | 60% | |
| | | Instalaciones | 1 | | | | 30% | |
| [N.2] | Daños por agua | Hardware | 1 | | | | 60% | |
| | | Media | 1 | | | | 60% | |
| | | Equipamiento Auxiliar | 1 | | | | 60% | |
| | | Instalaciones | 1 | | | | 30% | |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| [N.*] | Desastres narutales. | Hardware | 1 | | | | 30% | |
| | | Media | 1 | | | | 40% | |
| | | Equipamiento Auxiliar | 1 | | | | 30% | |
| | | Instalaciones | 1 | | | | 20% | |
| [I] | De origen industrial. | | | | | | | |
| [I.1] | Fuego | Hardware | 1 | | | | 60% | |
| | | Media | 1 | | | | 60% | |
| | | Equipamiento Auxiliar | 1 | | | | 60% | |
| | | Instalaciones | 1 | | | | 30% | |
| [I.2] | Daños por agua | Hardware | 1 | | | | 60% | |
| | | Media | 1 | | | | 60% | |
| | | Equipamiento Auxiliar | 1 | | | | 60% | |
| | | Instalaciones | 1 | | | | 30% | |
| [I.3] | Contaminación mecánica | Hardware | 1 | | | | 40% | |
| | | Media | 1 | | | | 40% | |
| | | Equipamiento Auxiliar | 1 | | | | 40% | |
| [I.4] | Contaminación electromagnética | Hardware | 1 | | | | 20% | |
| | | Media | 1 | | | | 20% | |
| | | Equipamiento Auxiliar | 1 | | | | 20% | |
| [I.5] | Averia de Origen físico o lógico | Hardware | 1 | | | | 50% | |
| | | Media | 1 | | | | 50% | |
| | | Equipamiento Auxiliar | 1 | | | | 50% | |
| | | Instalaciones | 1 | | | | 50% | |
| [I.6] | Corte del suministro eléctrico | Hardware | 2 | | | | 70% | |
| | | Media | 2 | | | | 50% | |
| | | Equipamiento Auxiliar | 2 | | | | 60% | |
| [I.7] | Condiciones inadecuadas de temperatura o humedad | Hardware | 1 | | | | 20% | |
| | | Media | 1 | | | | 20% | |
| | | Equipamiento Auxiliar | 1 | | | | 20% | |
| [I.8] | Fallo de servicios de comunicaciones | Redes | 2 | | | | 50% | |
| [I.9] | Interrupción de otros servicios y suministros esenciales | Equipamiento Auxiliar | 0 | | | | 30% | |
| [I.10] | Degradación de los soportes de almacenamiento de la información | Media | 1 | | | | 10% | |
| [I.11] | Emanaciones electromagneticas | Hardware | 1 | | | | 30% | |
| | | Media | 1 | | | | 70% | |
| | | Equipamiento Auxiliar | 1 | | | | 30% | |
| | | Instalaciones | 1 | | | | 40% | |
| [E] | Errores y fallos no intencionados. | | | | | | | |
| [E.1] | Errores de los usuarios | Datos / Información | 10 | | 80% | 90% | 70% | |
| | | Claves Criptograficas | 10 | | 80% | 90% | 70% | |
| | | Servicios | 10 | | 10% | 10% | 10% | |
| | | Aplicaciones | 10 | | 60% | 70% | 50% | |
| | | Media | 10 | | 70% | 80% | 60% | |
| [E.2] | Errores del Administrador | Datos / Información | 3 | | 60% | 70% | 80% | |
| | | Claves Criptograficas | 3 | | 50% | 60% | 70% | |
| | | Servicios | 3 | | 10% | 10% | 10% | |
| | | Aplicaciones | 3 | | 40% | 50% | 60% | |
| | | Hardware | 3 | | 40% | 50% | 60% | |
| | | Redes | 3 | | 30% | 40% | 50% | |
| | | Media | 3 | | 20% | 30% | 40% | |
| [E.3] | Errores de monitorización | Registros de Actividad | 4 | | | 70% | | |
| [E.4] | Errores de configuración | Datos de configuración | 4 | | | 60% | | |
| [E.7] | Deficiencias en la organización | Personal | 2 | | | | 40% | |
| [E.8] | Difusión de software dañino | Aplicaciones | 15 | | 50% | 70% | 90% | |
| [E.9] | Errores de [re-]encaminamiento | Servicios | 5 | | 10% | | | |
| | | Aplicaciones | 5 | | 60% | | | |
| | | Redes | 5 | | 50% | | | |
| [E.10] | Errores de secuencia | Servicios | 2 | | | 10% | | |
| | | Aplicaciones | 2 | | | 30% | | |
| | | Redes | 2 | | | 20% | | |
| [E.15] | Alteración accidental de la información | Datos / Información | 5 | | | 80% | | |
| | | Claves Criptograficas | 5 | | | 80% | | |
| | | Servicios | 5 | | | 10% | | |
| | | Aplicaciones | 5 | | | 50% | | |
| | | Redes | 5 | | | 40% | | |
| | | Media | 5 | | | 40% | | |
| | | Instalaciones | 5 | | | 10% | | |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| [E.18] | Destrucción de información | Datos / Información | 3 | | | | 50% | |
| | | Claves Criptograficas | 3 | | | | 70% | |
| | | Servicios | 3 | | | | 10% | |
| | | Aplicaciones | 3 | | | | 60% | |
| | | Redes | 3 | | | | 50% | |
| | | Media | 3 | | | | 50% | |
| | | Instalaciones | 3 | | | | 10% | |
| [E.19] | Fugas de información | Datos / Información | 5 | | 80% | | | |
| | | Claves Criptograficas | 5 | | 80% | | | |
| | | Servicios | 5 | | 10% | | | |
| | | Aplicaciones | 5 | | 60% | | | |
| | | Redes | 5 | | 60% | | | |
| | | Media | 5 | | 60% | | | |
| | | Instalaciones | 5 | | 30% | | | |
| | | Personal | 5 | | 30% | | | |
| [E.20] | Vulnerabilidades de los programas | Aplicaciones | 5 | | 40% | 80% | 60% | |
| [E.21] | Errores de mantenimiento / actualización de programas | Aplicaciones | 3 | | 50% | 70% | | |
| [E.23] | Errores de mantenimiento / actualización de equipos | Hardware | 5 | | | | 60% | |
| | | Media | 5 | | | | 40% | |
| | | Equipamiento Auxiliar | 5 | | | | 50% | |
| [E.24] | Caída del sistema por agotamiento de recursos | Servicios | 1 | | | | 10% | |
| | | Hardware | 1 | | | | 60% | |
| | | Redes | 1 | | | | 60% | |
| [E.25] | Pérdida de equipos | Hardware | 1 | | | | 50% | |
| | | Media | 1 | | | | 60% | |
| | | Equipamiento Auxiliar | 1 | | | | 40% | |
| [E.28] | Indisponibilidad del personal | Personal | 10 | | | | 80% | |
| [A] | Ataques intencionados | | | | | | | |
| [A.3] | Manipulación de los registros de actividad | Registros de Actividad | 3 | | | 70% | | |
| [A.4] | Manipulación de la configuración | Registros de Actividad | 3 | 50% | 70% | 70% | | |
| [A.5] | Suplantación de la identidad del usuario | Datos / Información | 10 | 80% | 90% | 80% | | |
| | | Claves Criptograficas | 10 | 80% | 90% | 80% | | |
| | | Servicios | 10 | 10% | 10% | 10% | | |
| | | Aplicaciones | 10 | 60% | 70% | 60% | | |
| | | Redes | 10 | 60% | 60% | 60% | | |
| [A.6] | Abuso de privilegios de acceso | Datos / Información | 10 | 80% | 90% | 80% | | |
| | | Claves Criptograficas | 10 | 80% | 90% | 80% | | |
| | | Servicios | 10 | 10% | 10% | 10% | | |
| | | Aplicaciones | 10 | 60% | 70% | 60% | | |
| | | Hardware | 10 | 60% | 60% | 60% | | |
| | | Redes | 10 | 60% | 60% | 60% | | |
| [A.7] | Uso no previsto | Servicios | 10 | | 10% | 10% | 10% | |
| | | Aplicaciones | 10 | | 50% | 40% | 60% | |
| | | Hardware | 10 | | 40% | 30% | 50% | |
| | | Redes | 10 | | 30% | 20% | 40% | |
| | | Media | 10 | | 30% | 20% | 40% | |
| | | Equipamiento Auxiliar | 10 | | 10% | 10% | 20% | |
| | | Instalaciones | 10 | | 20% | 20% | 30% | |
| [A.8] | Difusión de software dañino | Aplicaciones | 10 | | 50% | 70% | 90% | |
| [A.9] | Errores de [re-]encaminamiento | Servicios | 10 | | 10% | | | |
| | | Aplicaciones | 10 | | 70% | | | |
| | | Redes | 10 | | 50% | | | |
| [A.10] | Alteración de secuencia | Servicios | 9 | | | 10% | | |
| | | Aplicaciones | 9 | | | 60% | | |
| | | Redes | 9 | | | 50% | | |
| [A.11] | Acceso no autorizado | Datos / Información | 10 | | 50% | 90% | | |
| | | Claves Criptograficas | 10 | | 60% | 80% | | |
| | | Servicios | 10 | | 10% | 10% | | |
| | | Aplicaciones | 10 | | 50% | 70% | | |
| | | Hardware | 10 | | 50% | 70% | | |
| | | Redes | 10 | | 50% | 70% | | |
| | | Media | 10 | | 50% | 70% | | |
| | | Equipamiento Auxiliar | 10 | | 40% | 60% | | |
| | | Instalaciones | 10 | | 50% | 50% | | |
| [A.12] | Análisis de tráfico | Redes | 10 | | 80% | | | |
| [A.13] | Repudio | Servicios | 10 | | | | | 10% |
| | | Registros de Actividad | 10 | | | | | 60% |
| [A.14] | Interceptación de información | Redes | 10 | | 90% | | | |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| [A.15] | Modificación deliberada de la información | Datos / Información | 10 | | | 50% | | |
| | | Claves Criptograficas | 10 | | | 90% | | |
| | | Servicios | 10 | | | 10% | | |
| | | Aplicaciones | 10 | | | 70% | | |
| | | Redes | 10 | | | 70% | | |
| | | Media | 10 | | | 70% | | |
| | | Instalaciones | 10 | | | 20% | | |
| [A.18] | Destrucción de información | Datos / Información | 10 | | | | 50% | |
| | | Claves Criptograficas | 10 | | | | 70% | |
| | | Servicios | 10 | | | | 10% | |
| | | Aplicaciones | 10 | | | | 60% | |
| | | Media | 10 | | | | 50% | |
| | | Instalaciones | 10 | | | | 10% | |
| [A.19] | Divulgación de información | Datos / Información | 10 | | 50% | | | |
| | | Claves Criptograficas | 10 | | 90% | | | |
| | | Servicios | 10 | | 10% | | | |
| | | Aplicaciones | 10 | | 70% | | | |
| | | Redes | 10 | | 70% | | | |
| | | Media | 10 | | 70% | | | |
| | | Instalaciones | 10 | | 50% | | | |
| [A.22] | Manipulación de programas | Aplicaciones | 10 | | 80% | 70% | 60% | |
| [A.23] | Manipulación de equipos | Hardware | 10 | | 80% | | 70% | |
| | | Media | 10 | | 80% | | 70% | |
| | | Equipamiento Auxiliar | 10 | | 80% | | 60% | |
| [A.24] | Denegación de servicio | Servicios | 10 | | | | 10% | |
| | | Hardware | 10 | | | | 70% | |
| | | Redes | 10 | | | | 70% | |
| [A.25] | Robo | Hardware | 10 | | 50% | | 50% | |
| | | Media | 10 | | 50% | | 50% | |
| | | Equipamiento Auxiliar | 10 | | 50% | | 50% | |
| [A.26] | Ataque destructivo | Hardware | 10 | | | | 50% | |
| | | Media | 10 | | | | 50% | |
| | | Equipamiento Auxiliar | 10 | | | | 50% | |
| | | Instalaciones | 10 | | | | 70% | |
| [A.27] | Ocupación enemiga | Instalaciones | 10 | | 80% | | 80% | |
| [A.28] | Indisponibilidad del personal | Personal | | | | | 50% | |
| [A.29] | Estorsión | Personal | | | 50% | 70% | 60% | |
| [A.30] | Ingeniería social | Personal | | | 80% | 80% | 80% | |

## 4.6 Impacto potencial.

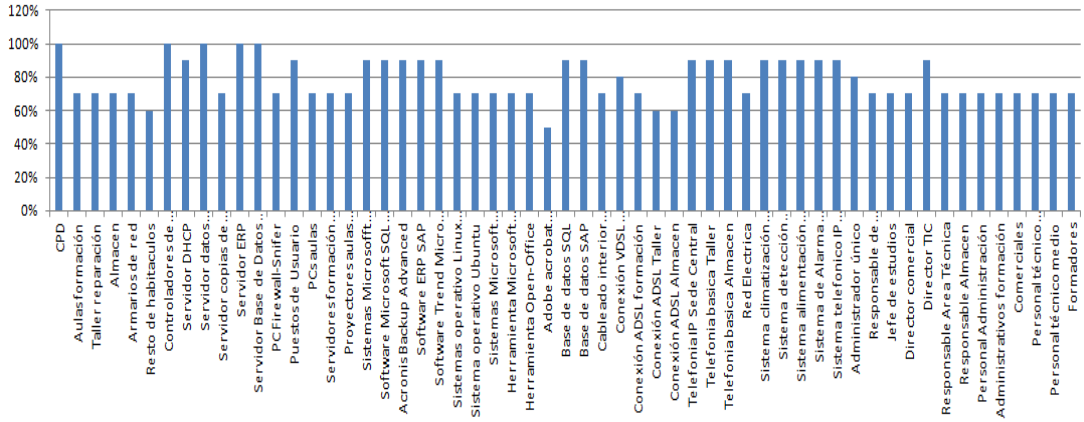
Entendiendo por impacto el nivel de daño que pueda sufrir un activo después de la sucesibilidad de una amenaza, en la organización que estudiamos analizaremos el impacto potencial por cada activo de información. Para realizar el cálculo, tomaremos en cuenta cada activo que detallamos analizándolo con cada amenaza del listado sugerido por MAGERIT (libro 2 apartado 5); valoraremos el impacto tomando a cada activo en sus 5 dimensiones (Autenticidad, Confidencialidad, Integridad, Disponibilidad y Trazabilidad) en la escala de 0 a 10, según la tabla siguiente, ya antes expresada.

| VALOR | CRITERIO |
|---|---|
| 10 | Daño muy grave a la organización |
| 7-9 | Daño grave a la organización |
| 4-6 | Daño importante a la organización |
| 1-3 | Daño menor a la organización |
| 0 | Irrelevante para la organización |

El cálculo del impacto lo calculamos trasladando directamente el mayor valor del impacto en cualquiera de las dimensiones de seguridad del activo

descrito en los puntos anteriores de valoración de riesgos tratados en porcentaje.

El cálculo del impacto se encuentra detallado en la pestaña Impacto del archivo Excel adjunto análisis_de_amenazas.xlsx.




4.7 Nivel de Riesgo.

Para calcular el valor del riesgo por activo mediante este método MAGERIT, se realiza en base al valor del mismo activo, a la máxima frecuencia de la ocurrencia de una amenaza y al impacto antes calculado para cada activo. Según los patrones anteriormente definidos:

| VALORACIÓN DE ACTIVOS | | |
|---|---|---|
| MA | 500.000,00€ | Muy Alto |
| A | 100.000,00€ | Alto |
| M | 30.000,00€ | Medio |
| B | 3.000,00€ | Bajo |
| N | 500,00€ | Muy Bajo |

| FRECUENCIA (en la que puede materializarse) | | | |
|---|---|---|---|
| EF | 0,9973 | Extremadamente frecuente | Menos que 1 día |
| MF | 0,1425 | Muy Frecuente | Menos que 1 semana |
| F | 0,0329 | Frecuente | Menos que un mes |
| FN | 0,0055 | Frecuencia Normal | Menos que medio año |
| PF | 0,0027 | Poco Frecuente | Menos que un año |
| EPF | 0,0003 | Extremadamente Poco Frecuente | Menos que diez años |

Este cálculo de valoración del riesgo, se encuentra detallado en la pestaña valoración del riesgo del archivo Excel adjunto análisis_de_amenazas.xlsx.

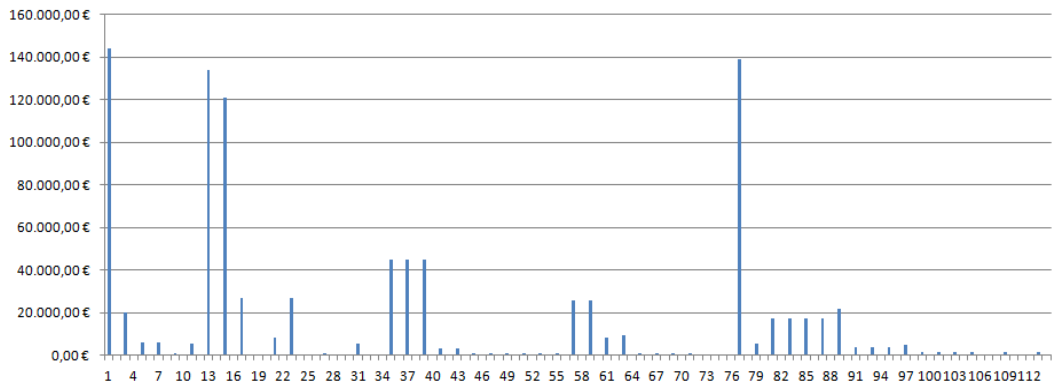
Utilizaremos la tabla descrita de la siguiente forma:

| | Activo1 | | Activo2 | | Activo... | |
|---|---|---|---|---|---|---|
| Riesgo 1 | Valor Activo1 | | Valor Activo2 | | Valor Activo... | |
| | Frecuencia | Impacto | Frecuencia | Impacto | Frecuencia | Impacto |
| | Valor del Riesgo | | Valor del Riesgo | | Valor del Riesgo | |
| Riesgo 2 | Valor Activo1 | | Valor Activo2 | | Valor Activo... | |
| | Frecuencia | Impacto | Frecuencia | Impacto | Frecuencia | Impacto |
| | Valor del Riesgo | | Valor del Riesgo | | Valor del Riesgo | |
| Riesgo 3 | Valor Activo1 | | Valor Activo2 | | Valor Activo... | |
| | Frecuencia | Impacto | Frecuencia | Impacto | Frecuencia | Impacto |
| | Valor del Riesgo | | Valor del Riesgo | | Valor del Riesgo | |

## 4.8 Resultados.

A continuación se muestra captura de la hoja de cálculo realizada para hallar la valuación del riesgo intrínseco de los activos, junto al grafico de valoración resultante de las operaciones antes reseñadas:

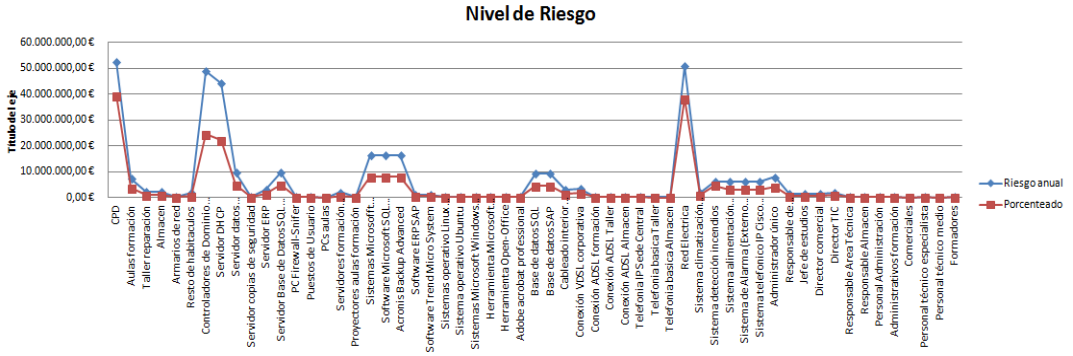
| | CPD | | Aulas formación | | Taller reparación | | Almacen | | Armarios de red | | Resto de habitaculos | | Contr Domin |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | MA | | A | | M | | M | | B | | M | | |
| Fuego | PF | 100% | PF | 70% | PF | 70% | PF | 70% | PF | 70% | PF | 60% | PF |
| | 1350 | | 189 | | 56,7 | | 56,7 | | 5,67 | | 48,6 | | |
| | MA | | A | | M | | M | | B | | M | | |
| Daños por agua | PF | 100% | PF | 70% | PF | 70% | PF | 70% | PF | 70% | PF | 60% | PF |
| | 1350 | | 189 | | 56,7 | | 56,7 | | 5,67 | | 48,6 | | |
| | MA | | A | | M | | M | | B | | M | | |
| Desastres narutales. | PF | 100% | PF | 70% | PF | 70% | PF | 70% | PF | 70% | PF | 60% | PF |
| | 1350 | | 189 | | 56,7 | | 56,7 | | 5,67 | | 48,6 | | |
| Contaminación mecánica | | | | | | | | | | | | | PF |
| | | | | | | | | | | | | | |
| | MA | | A | | M | | M | | B | | M | | |
| Averia de Origen físico o lógico | PF | 100% | PF | 70% | PF | 70% | PF | 70% | PF | 70% | PF | 60% | PF |
| | 1350 | | 189 | | 56,7 | | 56,7 | | 5,67 | | 48,6 | | |
| Corte del suministro eléctrico | | | | | | | | | | | | | FN |
| | | | | | | | | | | | | | |
| Condiciones inadecuadas de temperatura o humedad | | | | | | | | | | | | | PF |
| | | | | | | | | | | | | | |
| Fallo de servicios de comunicaciones | | | | | | | | | | | | | |
| | | | | | | | | | | | | | |
| Interrupción de otros servicios y suministros esenciales | | | | | | | | | | | | | |
| | | | | | | | | | | | | | |
| Degradación de los soportes de almacenamiento de la | | | | | | | | | | | | | |
| | | | | | | | | | | | | | |
| | MA | | A | | M | | M | | B | | M | | |
| Emanaciones electromagneticas | PF | 100% | PF | 70% | PF | 70% | PF | 70% | PF | 70% | PF | 60% | |
| | 1350 | | 189 | | 56,7 | | 56,7 | | 5,67 | | 48,6 | | |
| Errores de los usuarios | | | | | | | | | | | | | |
| | | | | | | | | | | | | | |




El nivel aceptable del riesgo se establece manualmente y analizando concienzudamente cada activo de los anteriormente analizados. Estableciéndose tres niveles de riesgo Bajo=75%, Medio=50%, Alto=25%, que se pretenden aplicar sobre el riesgo intrínseco anual del activo, a partir de este resultado se establecerán las medidas necesarias para gestionar el riesgo.

| | Activo | | Nivel de riesgo aceptable |
|---|---|---|---|
| Instalaciones | I1 | CPD | Bajo |
| | I2 | Aulas formación | Medio |
| | I3 | Taller reparación | Medio |
| | I4 | Almacen | Medio |
| | I5 | Armarios de red | Medio |
| | I6 | Resto de habitaculos | Alto |
| Hardware | H1 | Controladores de Dominio 2008 Server | Medio |
| | H2 | Servidor DHCP | Medio |
| | H3 | Servidor datos departamentales | Medio |
| | H4 | Servidor copias de seguridad | Medio |
| | H5 | Servidor ERP | Medio |
| | H6 | Servidor Base de Datos SQL Server | Medio |
| | H7 | PC Firewall-Snifer | Alto |
| | H8 | Puestos de Usuario | Medio |
| | H9 | PCs aulas | Alto |
| | H10 | Servidores formación (Windows-Linux) | Alto |
| | H11 | Proyectores aulas formación | Alto |
| Aplicación | S1 | Sistemas Microsofft Windows Server 2008 | Medio |
| | S2 | Software Microsoft SQL Server 2008 | Medio |
| | S3 | Acronis Backup Advanced | Medio |
| | S4 | Software ERP SAP | Medio |
| | S5 | Software Trend Micro System | Medio |
| | S6 | Sistemas operativo Linux Red-Hat | Medio |
| | S7 | Sistema operativo Ubuntu | Medio |
| | S8 | Sistemas Microsoft Windows 7 | Medio |
| | S9 | Herramienta Microsoft Office 2010 | Medio |
| | S10 | Herramienta Open-Office | Alto |
| | S11 | Adobe acrobat professional | Alto |
| Datos | D1 | Base de datos SQL | Medio |
| | D2 | Base de datos SAP | Medio |
| Red | R1 | Cableado interior estructurado | Medio |
| | R2 | Conexión VDSL corporativa | Medio |
| | R3 | Conexión ADSL formación | Medio |
| | R4 | Conexión ADSL Taller | Medio |
| | R5 | Conexión ADSL Almacen | Medio |
| | R6 | Telefonia IP Sede Central | Medio |
| | R7 | Telefonia basica Taller | Medio |
| | R8 | Telefonia basica Almacen | Medio |
| | R9 | Red Electrica | Bajo |
| E. Auxiliar | X1 | Sistema climatización centralizado | Medio |
| | X2 | Sistema detección incendios | Bajo |
| | X3 | Sistema alimentación ininterrumpida CPD | Medio |
| | X4 | Sistema de Alarma (Externo contratado) | Medio |
| | X5 | Sistema telefonico IP Cisco IP Fone | Medio |
| Personal | P1 | Administrador único | Medio |
| | P2 | Responsable de administración | Medio |
| | P3 | Jefe de estudios | Medio |
| | P4 | Director comercial | Medio |
| | P5 | Director TIC | Medio |
| | P6 | Responsable Area Técnica | Medio |
| | P7 | Responsable Almacen | Medio |
| | P8 | Personal Administración | Medio |
| | P9 | Administrativos formación | Medio |
| | P10 | Comerciales | Medio |
| | P11 | Personal técnico especialista | Medio |
| | P12 | Personal técnico medio | Medio |
| | P13 | Formadores | Medio |

El siguiente gráfico muestra los valores de los riesgos de los activos medidos anualmente y su variación respecto al nivel de riesgo aceptable.




Dados estos cálculos se determina que todo riesgo superior 10.000.000 € anuales será tratado con una muy alta prioridad, que todo riesgo superior a 200.000 € será tratado con prioridad media y todo aquel riesgo que se menor a 200.000 € no será tratado y por lo tanto será aceptado por la dirección de la empresa. Es decir, todo riesgo que sea por lo menos de nivel Bajo será catalogado como riesgo aceptable.

# 5. Propuesta de Proyectos.

## 5.1 Introducción.

Durante el análisis de riesgo desarrollado a lo largo del punto anterior, conocimos el nivel de riesgo actual de los activos en la organización; identificado también cuáles son las principales amenazas que atentan contra estos activos. Ahora la intención es mitigar el riesgo actual en la organización y evolucionar el cumplimiento ISO hasta su nivel adecuado.

Ya en la declaración de aplicabilidad se definieron todos los controles que son de aplicación y por tanto es necesario elaborar los procedimientos correspondientes para dotarnos de dichos controles. Ahora pues lo que se realiza es agrupar este conjunto de recomendaciones, para facilitar su ejecución.

## 5.2 Estructura de las propuestas.

Cada uno de los paroyectos que detallamos, se cuantifican economicamente, contando ademas con una planificación temporal, estableciendo los periodos de consecución de objetivos, donde incluimos una serie de puntos de control, que permitan considerar la mejora continua de la implementación del SGSI.

Cada Proyecto contendra:

- Nombre del Proyecto en cuestión.
- Objetivos del Proyecto.
- Descripción del Proyecto.
- Referencia ISO 27002 que cumplimenta.
- Planificación temporal.
- Presupuesto necesario.
- Indicadores verificación.

## 5.3 Propuesta de Proyectos.

A continuación se detallan los diferentes proyectos aportados:

| I. Organización de las políticas de seguridad y sus políticas de aplicación | | | | |
|---|---|---|---|---|
| **Planificación temporal** | **Inicio** | **Fin** | **Referencia ISO** | 5. Políticas de seguridad |
| | 01/07/2015 | 10/09/2015 | **Presupuesto estimado** | 3.500 € |
| **Objetivos** | | | | |
| Desarrollar el plan director de políticas de seguridad y sus políticas de aplicación, basándose en la normativa ISO aplicable. | | | | |
| **Descripción** | | | | |
| Se elaborará un plan de seguridad, según la política diseñada, que deberá ser aceptado y debidamente comunicado; donde se dirimirán las respectivas responsabilidades definiendo un organigrama acorde a la estructura de la organización.<br>En este proyecto, además definiremos la metodología de seguridad, con sus procesos y medidas destinadas al aseguramiento del plan de seguridad decidido. | | | | |
| **Indicadores verificación** | | | | |
| Verificación Inicio de proyecto, con firma acuerdo con consultor externo especializado.<br>Firma de aprobación del plan de seguridad a Un mes de inicio del proyecto.<br>Documentación de acuerdo finalización y conformidad, firmado por la dirección y comité de seguridad a fecha fin del proyecto. | | | | |
| **Riesgos a Mitigar** | | | | |
| La definición de las Políticas de seguridad, es paso fundamental y necesario para poder crear el SGSI en cualquier organización.<br>Se trata por tanto de mitigar los riesgos de infringir los niveles de confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad | | | | |

| II. Identificación y manejo de activos empresariales. | | | | |
|---|---|---|---|---|
| **Planificación temporal** | **Inicio** | **Fin** | **Referencia ISO** | 8.1 Responsabilidad de los activos.<br>8.3 Manejo de Medios |
| | 11/09/2015 | 11/10/2015 | **Presupuesto estimado** | 1.000 € |
| **Objetivos** | | | | |
| Asegurar una correcta clasificación de los activos por tipo, departamento y responsables dentro de toda la organización, tratando de detectar errores o dependencias erróneas para su mas pronta resolución.<br>Actualización de los activos cuando sean modificados, creados o eliminados en el entorno organizativo. | | | | |
| **Descripción** | | | | |
| Definición de los diferentes activos por tipo, dotándolos de políticas de creación, modificaión y eliminación.<br>Control efectivo y actualizado de todos los activos para el correcto funcionamiento de los mismos por parte de sus usuarios y en especial de sus responsables. | | | | |
| **Indicadores verificación** | | | | |
| Con carácter trimestral, registro de estado de los activos y su clasificación.<br>Con carácter semestral verificación de la correcta asignación de responsables de cada activo.<br>Mensualmente se realizara un registro de incidencias de uso de los activos. | | | | |

| Riesgos a Mitigar |
|---|
| [A.11] Acceso no autorizado<br>[A.14] Interceptación de información<br>[A.15] Modificación deliberada de la información<br>[A.18] Destrucción de información<br>[A.6] Abuso de privilegios de acceso<br>[A.7] Uso no previsto<br>[E.1] Errores de los usuarios<br>[E.15] Alteración accidental de la información<br>[E.18] Destrucción de información<br>[E.19] Fugas de información<br>[E.2] Errores del Administrador<br>[E.3] Errores de monitorización<br>[E.4] Errores de configuración<br>[E.7] Deficiencias en la organización |

| III. Clasificación de la Información | | | | |
|---|---|---|---|---|
| **Planificación temporal** | **Inicio** | **Fin** | **Referencia ISO** | 8.2 Clasificación de la Información |
| | 12/10/2015 | 30/11/2015 | **Presupuesto estimado** | 1.700 € |
| **Objetivos** | | | | |
| Asegurar la información clasificandola en base a las fuentes que la generan | | | | |
| **Descripción** | | | | |
| Proceder a organizar la información en la forma que se trata y genera dentro de la organización, atendiendo a su valor económico, requisitos legales y lo critico de su contenido.<br>Hay que diseñar y asegurar las medidas necesarias de control y seguridad necesarias para el aseguramiento de toda la información de la organización. | | | | |
| **Indicadores verificación** | | | | |
| Anualmente se verificara la correcta clasificación de todos los activos de la organización.<br>Mensualmente se verificaran todas las incidencias producidas sobre estos activos. | | | | |
| **Riesgos a Mitigar** | | | | |
| [A.15] Modificación deliberada de la información<br>[A.22] Manipulación de programas<br>[A.4] Manipulación de la configuración<br>[A.8] Difusión de software dañino<br>[E.15] Alteración accidental de la información<br>[E.18] Destrucción de información<br>[E.19] Fugas de información<br>[E.20] Vulnerabilidades de los programas<br>[E.21] Errores de mantenimiento / actualización de programas<br>[E.7] Deficiencias en la organización<br>[E.8] Difusión de software dañino | | | | |

| VI. Actuaciones en CPD y áreas seguras. | | | | |
|---|---|---|---|---|
| **Planificación temporal** | **Inicio** | **Fin** | **Referencia ISO** | 11.1 Áreas seguras |
| | 01/12/2015 | 30/01/2016 | **Presupuesto estimado** | 4.700 € |
| **Objetivos** | | | | |
| Control efectivo y procedimental del acceso a la información y zonas seguras, mejorando el actual sistema de monitorizaciones (fisicas y lógicas) de acceso a CPD y zonas clasificadas seguras dentro de la organización. | | | | |

| Descripción |
|---|
| Objetivo de protección el acceso físico y remoto a los sistemas de gestión y control del CPD, garantizando accesos seguros y protegiéndose de entradas no autorizadas a los sistemas. Se trata de impedir accesos no autorizados a los sistemas y robos/manipulaciones de información critica de la organización. |
| **Indicadores verificación** |
| Con frecuencia trimestral se realizara un seguimiento de los acceso (físico y lógico) a los sistemas basado en los roles declarados.<br>Mensualmente se revisara el registro de incidencias de accesos no autorizados. |
| **Riesgos a Mitigar** |
| [A.11] Acceso no autorizado<br>[A.15] Modificación deliberada de la información<br>[A.18] Destrucción de información<br>[A.22] Manipulación de programas<br>[A.23] Manipulación de equipos<br>[A.25] Robo<br>[A.26] Ataque destructivo<br>[A.3] Manipulación de los registros de actividad<br>[A.4] Manipulación de la configuración<br>[A.7] Uso no previsto<br>[E.18] Destrucción de información<br>[E.25] Pérdida de equipos<br>[E.7] Deficiencias en la organización<br>[I.6] Corte del suministro eléctrico |

| V. Formación y concienciación de seguridad. | | | | |
|---|---|---|---|---|
| **Planificación temporal** | **Inicio** | **Fin** | **Referencia ISO** | 12.1 Procedimientos y responsabilidades operacionales.<br>7.2.2 Concienciación de seguridad. |
| | 01/02/2016 | 01/03/2016 | **Presupuesto estimado** | 3.500 € |
| **Objetivos** | | | | |
| Definir, documentar y planificar un plan de formación adecuado, para los empleados de la organización, adecuado a los distintos roles asignados. | | | | |
| **Descripción** | | | | |
| Todo empleado, según su categoría y puesto asignado, deberá ser instruido en las funciones y responsabilidades que tiene respecto a la seguridad de los activos de la organización. Por ello, se pantas la creación de una formación continuada en el tiempo, con presupuesto anual compatible y adecuada a las labores del personal de la organización. | | | | |
| **Indicadores verificación** | | | | |
| Anualmente se verificaran las acciones formativas impartidas, evaluando su funcionalidad.<br>Anualmente se revisará la actualización de los planes dotándolo de las mejoras oportunas. | | | | |
| **Riesgos a Mitigar** | | | | |
| [A.18] Destrucción de información<br>[A.19] Divulgación de información<br>[A.3] Manipulación de los registros de actividad<br>[A.30] Ingeniería social<br>[A.4] Manipulación de la configuración<br>[E.1] Errores de los usuarios<br>[E.15] Alteración accidental de la información<br>[E.19] Fugas de información<br>[E.2] Errores del Administrador<br>[E.3] Errores de monitorización<br>[I.7] Condiciones inadecuadas de temperatura o humedad | | | | |

| VI. Cumplimiento de requisitos legales. | | | | |
|---|---|---|---|---|
| **Planificación temporal** | **Inicio** | **Fin** | **Referencia ISO** | 18. Conformidad |
| | 02/03/2016 | 30/03/2016 | **Presupuesto estimado** | 2.000 € |
| **Objetivos** | | | | |
| Asegurar el correcto cumplimiento de la LOPD y demás requisitos legales establecidos, adaptándose a la normativa ISO aplicable en cada momento. | | | | |
| **Descripción** | | | | |
| Se debe adaptar todo el sistema organizativo y de producción a la normativa legal aplicable, tanto en materia de seguridad como laboral. Actualizando mediante verificaciones los sistemas a la ISO correspondiente para superar las auditorias oportunas. | | | | |
| **Indicadores verificación** | | | | |
| Semestralmente se realizara una verificación de cumplimiento de los requisitos legales. Anualmente se realizara una junto a la auditoria programada un registro de no conformidades/acciones correcticas sobre los requisitos legales establecidos. | | | | |

**Planificación temporal**

| | | Julio | Agosto | Septiembre | Octubre | Noviembre | Diciembre | Enero | Febrero | Marzo |
|---|---|---|---|---|---|---|---|---|---|---|
| Proyecto I | 01/07 - 10/09 | | | | | | | | | |
| Proyecto II | 11/09 - 11/10 | | | | | | | | | |
| Proyecto III | 12/10 - 30/11 | | | | | | | | | |
| Proyecto IV | 01/12 - 30/01 | | | | | | | | | |
| Proyecto V | 01/02 - 01/03 | | | | | | | | | |
| Proyecto IV | 02/03 - 30-03 | | | | | | | | | |

## 5.4 Resumen de resultados.

El plan de acción propuesto a través de la realización de los proyectos indicados, está definido por en orden a la importancia de los riesgos localizados y la implementación de un plan de seguridad del que carecía la organización.

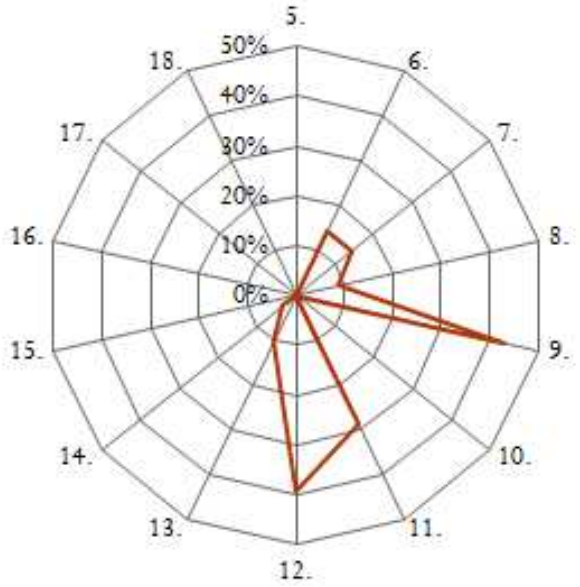
En un primer lugar, se tendrá en cuenta la propia creación del plan de seguridad, definiendo las políticas de seguridad, aspectos organizativos y la gestión de los activos de la organización. El objetivo de estos primeros puntos, es mejorar el estado de la seguridad de la información dentro de la organización implementando las medidas y acciones que den lugar a la capacitación del personal en relación al rol de cada cual dentro de la organización.

El desarrollo del plan presentado, no solo atañe a los activos TIC, sino que debe repercutir en el trasfondo de la organización, aunando un conjunto de medidas que engloba los proyectos II, III y IV medias que comparten su importancia en cuanto la seguridad física de los activos, como a la seguridad técnica de los mismos, con medidas de verificación y control de usos inadecuados, para poder subsanar posible errores en el diseño o ejecución de los planes establecidos.

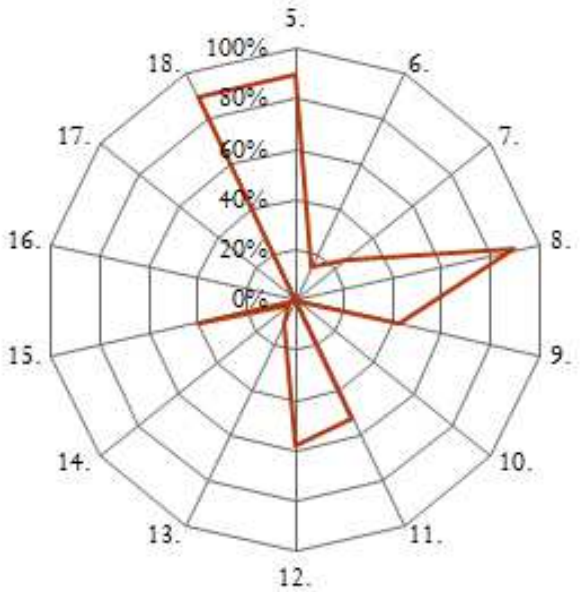
Junto a este diseño de un adecuado plan de seguridad y medidas señaladas para afianzar la seguridad, establecemos también un proyecto de formación continuada en la materia, adaptada a cada nivel de rol de los usuarios y responsable que van a tratar los activos de la organización, con las medidas correctoras en cada escalón de la cadena. Todo ello, sin olvidarse de adaptar la organización a la normativa legal aplicable, con

cumplimiento de la ISO relacionada, pasando auditorias de cumplimiento para un mayor desarrollo organizativo.

Como resultado de las propuestas de proyecto presentadas, se tiende a obtener una mejora considerable del Análisis diferencial respecto a la norma ISO 27002 presentada al inicio, cuyo diagrama radar era:




Con los cambios proyectados, modificados según la valoración que se muestra a continuación, se observa una nueva proyección del estado de los activos en relación al nivel de riesgo, la cual se ve ilustrada en siguiente Diagrama de Radar de la implementación de controles de ISO 27002 cuya captura a continuación se muestra:




Nuevo análisis diferencia indicado, aplicando los proyectos presentados:

| | | | |
|---|---|---|---|
| **5. POLITICA DE SEGURIDAD** | | | |
| **5.1 Dirección de la gestión de seguridad de la información.** | | | |
| 5.1.1 | Políticas de la seguridad de la información | Implementado | 90% |
| 5.1.2 | Revisión de las políticas de la seguridad de la información. | No Implementado | 90% |
| **5. Política de Seguridad.** | | **Implementado** | 90% |
| **6. ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN** | | | |
| **6.1 Organización de la seguridad de la información.** | | | |
| 6.1.1 | Funciones y responsabilidades de seguridad de información. | Parcialmente Implementado | 30% |
| 6.1.2 | Segregación de funciones. | Parcialmente Implementado | 50% |
| 6.1.3 | Contacto con las autoridades. | No Implementado | 0% |
| 6.1.4 | Contacto con grupos de especial interés. | No Implementado | 0% |
| 6.1.5 | Seguridad de la información en la gestión de proyectos. | Parcialmente Implementado | 20% |
| **6.2 Dispositivos moviles y teletrabajo.** | | | |
| 6.2.1 | Políticas de dispositivos moviles. | No Implementado | 0% |
| 6.2.2 | Teletrabajo | No Implementado | 0% |
| **6. Organización de la seguridad de la información.** | | **Parcialmente Implementado** | 14% |
| **7. SEGURIDAD DE RECURSOS HUMANOS** | | | |
| **7.1 Antes de empleo.** | | | |
| 7.1.1 | Screening | No Implementado | 0% |
| 7.1.2 | Terminos y condiciones de empleo | Parcialmente Implementado | 50% |
| **7.2 Durante el empleo.** | | | |
| 7.2.1 | Responsabilidades de gestión | Parcialmente Implementado | 10% |
| 7.2.2 | Conciencia de seguridad de la información y entrenamiento | Implementado | 70% |
| 7.2.3 | Proceso disciplinario | Parcialmente Implementado | 20% |
| **7.3 Terminación y cambio de empleo.** | | | |
| 7.3.1 | Terminación o cambio de las responsabilidades de empleo | No Implementado | 0% |
| **7. Seguridad de recursos humanos.** | | **Parcialmente Implementado** | 25% |
| **8. GESTION DE ACTIVOS** | | | |
| **8.1 Responsabilidad de los activos** | | | |
| 8.1.1 | Inventario de activos | Implementado | 90% |
| 8.1.2 | Propiedad de los activos | Implementado | 90% |
| 8.1.3 | Retorno de los activos | Implementado | 80% |
| **8.2 Clasificación de la información** | | | |
| 8.2.1 | Clasificación de la información | Implementado | 90% |
| 8.2.2 | Etiquetado de la información | Implementado | 90% |
| 8.2.3 | Manejo de activos | Implementado | 90% |
| **8.3 Manejo de Medios** | | | |
| 8.3.1 | Gestión de medios extraibles | Implementado | 90% |
| 8.3.2 | Eliminación de medios | Implementado | 90% |
| 8.3.3 | Transferencia de medios físicos | Implementado | 90% |
| **8. Gestión de activos.** | | **Implementado** | 90% |
| **9. CONTROL DE ACCESO** | | | |
| **9.1 Business requirements of access control** | | | |
| 9.1.1 | Política de control de acceso | Parcialmente Implementado | 50% |
| 9.1.2 | Acceso a las redes y servicios de red | Parcialmente Implementado | 50% |
| **9.2 Gestión de acceso de usuario** | | | |
| 9.2.1 | Registro de usuario y cancelación de registro | Parcialmente Implementado | 50% |
| 9.2.2 | Acceso aprovisionamiento de usuario | Parcialmente Implementado | 50% |
| 9.2.3 | Gestión de derechos de accesos privilegiados | Implementado | 70% |
| 9.2.4 | Gestión de la información de autentificación de secreto de los usuarios | Parcialmente Implementado | 50% |
| 9.2.5 | Revisión de los derechos de acceso de usuario | Parcialmente Implementado | 40% |
| 9.2.6 | Eliminación o ajuste de los derechos de acceso | Parcialmente Implementado | 50% |
| **9.3 Responsabilidades del usuario** | | | |
| 9.3.1 | Uso de información secreta de autenticación | No Implementado | 0% |
| **9.4 Control de sistemas y acceso a las aplicaciones** | | | |
| 9.4.1 | Restricción del acceso a la información | Parcialmente Implementado | 50% |
| 9.4.2 | Procedimiento de inicio de sesión seguro | Implementado | 70% |
| 9.4.3 | Sistema de gestión de contraseñas | Implementado | 70% |
| 9.4.4 | Uso de programas de servicios publicos privilegiados | No Implementado | 0% |
| 9.4.5 | Control de acceso al codigo fuente del programa | No Implementado | 0% |
| **9. Control de acceso.** | | **Parcialmente Implementado** | 43% |

| | | | |
|---|---|---|---|
| **10. CRIPTOGRAFIA** | | | |
| **10.1 Controles criptograficos** | | | |
| 10.1.1 | Politica sobre el uso de controles criptograficos | No Implementado | 0% |
| 10.1.2 | Gestión de Claves | No Implementado | 0% |
| **10. Criptografia.** | | **No implementado** | 0% |
| **11. SEGURIDAD FISICA Y AMBIENTAL** | | | |
| **11.1 Areas seguras** | | | |
| 11.1.1 | Perimetro de seguridad fisica | Implementado | 90% |
| 11.1.2 | Controles de entrada fisicas | Implementado | 90% |
| 11.1.3 | Asegurar oficinas habitaciones e instalaciones | Implementado | 90% |
| 11.1.4 | Protección contra amenazas externas y ambientales | Implementado | 90% |
| 11.1.5 | Trabajar en zonas seguras | Implementado | 90% |
| 11.1.6 | Zonas de entrega y carga | Implementado | 90% |
| **11.2 Equipo** | | | |
| 11.2.1 | Ubicación y protección del equipo | Parcialmente Implementado | 20% |
| 11.2.2 | Apoyo a los servicios publicos | No Implementado | 0% |
| 11.2.3 | Seguridad de cableado | Implementado | 60% |
| 11.2.4 | Mantenimiento de los equipos | Implementado | 70% |
| 11.2.5 | Eliminación de los activos | Parcialmente Implementado | 20% |
| 11.2.6 | Seguridad de equipo y activos fuera de las instalaciones | No Implementado | 0% |
| 11.2.7 | Eliminación segura o reutilización de los equipos | Implementado | 80% |
| 11.2.8 | Equipos de usuario desatendidos | No Implementado | 0% |
| 11.2.9 | Escritorio limpio y politica pantalla limpia | No Implementado | 0% |
| **11. Seguridad fisica y ambiental.** | | **Parcialmente implementado** | 53% |
| **12. OPERACIONES DE SEGURIDAD** | | | |
| **12.1 Procedimientosy responsabilidades operacionales** | | | |
| 12.1.1 | Procedimientos operativos documentales | Implementado | 90% |
| 12.1.2 | Gestión del cambio | Implementado | 90% |
| 12.1.3 | Gestión de la capacidad | Implementado | 90% |
| 12.1.4 | Separación de desarrollo, pruebas y entornos operativos | Implementado | 90% |
| **12.2 Protección contra el malware** | | | |
| 12.2.1 | Controles contra el malware | Implementado | 90% |
| **12.3 Copias de seguridad** | | | |
| 12.3.1 | Copia de seguridad de la información | Implementado | 90% |
| **12.4 Registro y seguimiento** | | | |
| 12.4.1 | Registro de eventos | Parcialmente Implementado | 20% |
| 12.4.2 | Protección de la información de los registros | Parcialmente Implementado | 30% |
| 12.4.3 | Registros de administración y operación | Parcialmente Implementado | 20% |
| 12.4.4 | Sincronización del reloj | Implementado | 100% |
| **12.5 Control del software operativo** | | | |
| 12.5.1 | Apoyo a los servicios publicos | No Implementado | 0% |
| **12.6 Tecnico de gestion de vulnerabilidades** | | | |
| 12.6.1 | Gestión de vulnerabilidades técnicas | Parcialmente Implementado | 30% |
| 12.6.2 | Restricciones de instalación de software | Implementado | 70% |
| **12.7 Sistemas de la Información consideraciones de auditoria** | | | |
| 12.7.1 | Sistemas de información controles de auditoria | No Implementado | 0% |
| **12. Operaciones de seguridad.** | | **Parcialmente implementado** | 58% |
| **13. SEGURIDAD DE LAS COMUNICACIONES** | | | |
| **13.1 Gestion de la seguridad de la red** | | | |
| 13.1.1 | Funciones y responsabilidades de seguridad de información. | Parcialmente Implementado | 30% |
| 13.1.2 | Segregación de funciones. | Parcialmente Implementado | 30% |
| 13.1.3 | Contacto con las autoridades | No Implementado | 0% |
| **13.2 Transferencia de Información** | | | |
| 13.2.1 | Politicas y procedimientos de transferencia de Información | Parcialmente Implementado | 10% |
| 13.2.2 | Acuerdos sobre la transferencia de Información | No Implementado | 0% |
| 13.2.3 | Mensajeria electrónica | No Implementado | 0% |
| 13.2.4 | Acuerdos de confidencialidad o de no divulgación | No Implementado | 0% |
| **13. Seguridad de las comunicaciones.** | | **Parcialmente implementado** | 10% |

| | | | |
|---|---|---|---|
| **14. SISTEMA DE ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO** | | | |
| **14.1 Security requirements of information system** | | | |
| 14.1.1 | Información de analisis de requisitos de seguridad y la especificación | Parcialmente Implementado | 10% |
| 14.1.2 | Asegurar los servicios de aplicaciones en las redes publicas | Parcialmente Implementado | 30% |
| 14.1.3 | Protección de las transacciones de servicios de aplicaciones | No Implementado | 0% |
| **14.2 Seguridad en los procesos de desarrollo y de apoyo** | | | |
| 14.2.1 | Politica de desarrollo seguro | No Implementado | 0% |
| 14.2.2 | Procedimientos de control de cambio del sistema | No Implementado | 0% |
| 14.2.3 | Revisión técnica de las aplicaciones tras efectuar cambios en la plataforma operativo | No Implementado | 0% |
| 14.2.4 | Restricciones a los cambios de los paquetes de software | No Implementado | 0% |
| 14.2.5 | Principios de Ingeniería de sistemas seguros | No Implementado | 0% |
| 14.2.6 | Entorno de desarrollo seguro | No Implementado | 0% |
| 14.2.7 | Desarrollo outsourced | No Implementado | 0% |
| 14.2.8 | Pruebas de seguridad del sistema | | |
| 14.2.9 | Pruebas de aceptación del sistema | No Implementado | 0% |
| **14.3 Datos de prueba** | | | |
| 14.3.1 | Protección de datos de prueba | No Implementado | 0% |
| **14. Sistema de adquisición, desarrollo y mantenimiento.** | | **Parcialmente Implementado** | 3% |
| **15.RELACIÓN CON PROVEEDORES** | | | |
| **15.1 Seguridad en la información en las relaciones con proveedores** | | | |
| 15.1.1 | Politica de seguridad de la información para relaciones con los proveedores | Parcialmente Implementado | 20% |
| 15.1.2 | Abordar la seguridad dentro de los acuerdos con proveedores | Parcialmente Implementado | 30% |
| 15.1.3 | Cadena de la información y tecnologia de comunicación de suministro | No Implementado | 0% |
| **15.2 Gestion de la prestación de servicios de proveedores** | | | |
| 15.2.1 | Politica de desarrollo seguro | No Implementado | 0% |
| 15.2.2 | Procedimientos de control de cambio del sistema | No Implementado | 0% |
| **15. Relación con los proveedores.** | | **Parcialmente Implementado** | 10% |
| **16. INFORMACIÓN DE GESTIÓN DE INCIDENCIAS DE SEGURIDAD** | | | |
| **16.1 Gestión de incidencias de seguridad de la información y mejoras** | | | |
| 16.1.1 | Responsabilidades y procedimientos | Parcialmente Implementado | 40% |
| 16.1.2 | Presentación de informes de eventos de seguridad de información | Parcialmente Implementado | 40% |
| 16.1.3 | Informes debilides de seguridad de información | Parcialmente Implementado | 40% |
| 16.1.4 | Evaliación y decisión sobre los eventos de seguridad de información | Parcialmente Implementado | 40% |
| 16.1.5 | Respuestas a incidentes de seguridad de la información | Parcialmente Implementado | 40% |
| 16.1.6 | Aprendiendo de los incidentes de seguridad de la información | Parcialmente Implementado | 40% |
| 16.1.7 | Acopio de pruebas | Parcialmente Implementado | 40% |
| **16. Información de gestión de incidencias de seguridad.** | | **Parcialmente Implementado** | 40% |
| **17. ASPECTOS DE SEGURIDAD DE INFORMACIÓN DE LA GESTIÓN DE LA C** | | | |
| **17.1 Información continuidad seguridad** | | | |
| 17.1.1 | Planificación información continuidad seguridad | No Implementado | 0% |
| 17.1.2 | Implementación de la información continuidad seguridad | No Implementado | 0% |
| 17.1.3 | Verificar, revisar y evaluar la información de seguridad continuidad | No Implementado | 0% |
| **17.2 Despidos** | | | |
| 17.2.1 | Disponibilidad de instalaciones de procesamiento de información | No Implementado | 0% |
| **17. Aspectos de seguridad de información de la gestión de la continuidad de** | | **No Implementado** | 0% |
| **18. CONFORMIDAD** | | | |
| **18.1 Cumplimiento de los requisitos legales y contractuales** | | | |
| 18.1.1 | Identificación de la legislación aplicable y requisitos contractuales | Implementado | 90% |
| 18.1.2 | Derechos de propiedad intelectual | Implementado | 90% |
| 18.1.3 | Protección de los registros | Implementado | 90% |
| 18.1.4 | Privacidad y protección de datos personales | Implementado | 90% |
| 18.1.5 | Reglamento de los controles criptograficos | Implementado | 90% |
| **18.2 Revisiones de seguridad de información** | | | |
| 18.2.1 | Revisión independiente de seguridad de la información | Implementado | 90% |
| 18.2.2 | Cumplimiento de las politicas y etandares de seguridad | Implementado | 90% |
| 18.2.3 | Revisión del cumplimiento técnico | Implementado | 90% |
| **17. Aspectos de seguridad de información de la gestión de la continuidad de** | | **Implementado** | 90% |

# 6. Auditoria del Cumplimiento.

## 6.1 Introducción.

En esta parte final del proyecto conocemos los activos de la empresa y hemos evaluado las amenazas sobre ellos, en el análisis de riesgo. De este análisis han aparecido proyectos para resolver las carencias, donde se ha visto una muestra de los más importantes y cómo se aplican sobre la ISO 27002. Ahora es el momento de hacer un alto y evaluar hasta qué punto la empresa cumple con las "buenas prácticas" en materia de seguridad. Una auditoría con la ISO 27002 nos servirá como marco de control del estado de la seguridad.

## 6.2 Metodología.

En este apartado describiremos brevemente la metodología de la auditoría utilizada para llevar a cabo el análisis de madurez y cumplimiento de la ISO / IEC 27002: 2013 sobre sus 114 controles o medidas preventivas sobre las buenas prácticas para la Gestión de la Seguridad de la Información, organizados en 14 áreas y 35 objetivos de control. Este estándar es internacionalmente conocido y es perfectamente válido para la mayoría de las organizaciones.
Hay diferentes aspectos sobre los que las medidas preventivas actúan reduciendo el riesgo:

- Formalización de las prácticas mediante documentos escritos o aprobados
- Políticas del personal de la empresa.
- Solicitudes técnicas de software, hardware y comunicaciones.
- Seguridad física.

## 6.3 Evaluación de la madurez.

Para evaluar la madurez de la seguridad de la organización, se analizarán los siguientes dominios de la ISO / IEC 27002: 2013:

- Política de seguridad
- Organización de la seguridad de la información
- Gestión de activos
- Seguridad a los recursos humanos
- Seguridad física y ambiental
- Gestión de comunicaciones y operaciones
- Control de acceso
- Adquisición, desarrollo y mantenimiento de Sistemas de Información
- Gestión de incidentes

- Gestión de continuidad de negocio
- Cumplimiento

En el estudio se realizará una revisión de los 114 controles planteados por la norma a cumplir, con los diferentes objetivos de control. La siguiente tabla, que se basa en el Modelo de Madurez de la Capacidad (CMM), nos permite ver la metodología que se utilizará para describir el cumplimiento de los diferentes controles de la ISO / IEC 27001.

| EFECTIVIDAD | CMM | SIGNIFICADO | DESCRIPCIÓN |
|---|---|---|---|
| 0% | L0 | Inexistente | Carencia completa de cualquier proceso reconocible.<br>No se ha reconocido siquiera que existe un problema a resolver. |
| 10% | L1 | Inicial / Ad-hoc | Estado inicial donde el éxito de las actividades de los procesos se basa la mayoría de las veces en el esfuerzo personal.<br>Los procedimientos son inexistentes o localizados en áreas concretas. |
| 50% | L2 | Reproducible, pero intuitivo | Los procesos similares se llevan en forma similar por diferentes personas con la misma tarea.<br>Se normalizan las buenas prácticas en base a la experiencia y al método.<br>No hay comunicación o entrenamiento formal, las responsabilidades quedan a cargo de cada individuo.<br>Se depende del grado de conocimiento de cada individuo. |
| 90% | L3 | Proceso definido | La organización entera participa en el proceso.<br>Los procesos están implantados, documentados y comunicados mediante entrenamiento. |
| 95% | L4 | Gestionado y medible | Se puede seguir con indicadores numéricos y estadísticos la evolución de los procesos.<br>Se dispone de tecnología para automatizar el flujo de trabajo, se tienen herramientas para mejorar la calidad y la eficiencia. |
| 100% | L5 | Optimizado | Los procesos están bajo constante mejora.<br>En base a criterios cuantitativos se determinan las desviaciones más comunes y se optimizan los procesos. |

Evaluamos el cumplimiento de los diferentes sub-apartados a raíz de los cuales se realizará el cálculo de nivel de cumplimiento del objeto a estudio, bloque a bloque, según la siguiente descripción de los controles:

**(5) Política de seguridad**

Objetivo: Proporcionar la dirección de gestión y apoyo a la seguridad de la información de acuerdo con los requerimientos de la organización y la legislación vigente.

**(6) Organización de la seguridad de la información.**

Objetivo 6.1: Establecer un marco de gestión para iniciar y controlar la implementación y operación de seguridad de la información dentro de la organización.

Objetivo 6.2: Garantizar la seguridad del teletrabajo y el uso de dispositivos móviles.

**7) Seguridad de Recursos Humanos**

Objetivo 7.1: Asegurarse de que los empleados y contratistas entiendan sus responsabilidades y son adecuados para las funciones para las que se consideran.

Objetivo 7.2: Asegurarse de que los empleados y contratistas conozcan y cumplan con sus responsabilidades de seguridad de la información.

Objetivo 7.3: Proteger los intereses de la organización, como parte del proceso de cambiar o terminar el empleo.

**(8) Gestión de Activos**

Objetivo 8.1: Identificar activos de la organización y definir las responsabilidades de protección adecuados.

Objetivo 8.2: Asegurar que la información recibe un nivel adecuado de protección de acuerdo con su importancia para la organización.

Objetivo 8.3: Evitar la divulgación no autorizada, modificación, eliminación o destrucción de la información almacenada en los medios de comunicación.

**(9) Control de Acceso**

Objetivo 9.1: Limitar el acceso a las instalaciones de procesamiento de la información y de la información.

Objetivo 9.2: Garantizar el acceso del usuario autorizado y evitar el acceso no autorizado a sistemas y servicios.

Objetivo 9.3: Hacer que los usuarios sean responsables de salvaguardar su información de autenticación.

Objetivo 9.4: Prevenir el acceso no autorizado a los sistemas y aplicaciones.

**(10) Criptografía**

Objetivo 10.1: Garantizar un uso adecuado y eficaz de la criptografía para proteger la confidencialidad, autenticidad y / o integridad de la información.

**(11) Seguridad física y ambiental**

Objetivo 11.1: Evitar autorizado física de acceso, daños e interferencia a la información y procesamiento de información sobre las instalaciones de la organización.

Objetivo 11.2: Evitar la pérdida, daño, robo o el compromiso de los activos y la interrupción de las operaciones de la organización.

**(12) Operaciones de seguridad**

Objetivo 12.1: Asegurar operaciones correctas y seguras de instalaciones de procesamiento de información.

Objetivo 12.2: Asegurar que las instalaciones de procesamiento de información y la información están protegidos contra el malware.

Objetivo 12.3: Evitar la pérdida de datos.

Objetivo 12.4: Registrar eventos y generar evidencia.

Objetivo 12.5: Garantizar la integridad de los sistemas operativos.

Objetivo 12.6: prevenir la explotación de vulnerabilidades técnicas.

Objetivo 12.7: Minimizar el impacto de las actividades de auditoría en los sistemas operativos.

**(13) Seguridad de las comunicaciones**

Objetivo 13.1: Garantizar la protección de la información en las redes y sus instalaciones de apoyo de procesamiento de información.

Objetivo 13.2: Mantener la seguridad de la información transferida dentro de una organización y con cualquier entidad externa.

**(14) Sistema de adquisición, desarrollo y mantenimiento**

Objetivo 14.1: Asegurarse de que la seguridad informática es una parte integral de los sistemas de información a través de todo el ciclo de vida. Esto también incluye los requisitos para los sistemas de información que proporcionan los servicios a través de redes públicas.

Objetivo 14.2: Garantizar la seguridad de la información que se diseña e implementa dentro del ciclo de vida de desarrollo de sistemas de información.

**(15) Relaciones con los proveedores**

Objetivo 15.1: Garantizar la protección de los activos de la organización que sea accesible por los proveedores.

Objetivo 15.2: Mantener un nivel acordado de seguridad de la información y la prestación de servicios en línea con los acuerdos con proveedores.

**(16) Información de gestión de incidentes de seguridad**

Objetivo 16.1: Garantizar un enfoque coherente y eficaz para la gestión de incidentes de seguridad de la información, incluidos los de comunicación en los eventos de seguridad y debilidades.

**(17) Los aspectos de seguridad de información de la gestión de la continuidad del negocio**

Objetivo 17.1: Información continuidad de seguridad debe estar integrada en los sistemas de gestión de continuidad de negocio de la organización.

Objetivo 17.2: Asegurar la disponibilidad de instalaciones de procesamiento de información.

**(18) Conformidad**

Objetivo 18.1: Evitar incumplimientos de las obligaciones legales, estatutarias, reglamentarias o contractuales en materia de seguridad de la información y de las exigencias de seguridad.

Objetivo 18.2: Garantizar la seguridad de la información que se implementa y opera de acuerdo con las políticas y procedimientos de la organización.

**Tabla cumplimiento de los controles ISO / IEC 27002: 2013**

A continuación se ve la tabla de cumplimiento de la ISO / IEC 27002: 2013, con los valores de efectividad y el valor CMM estimado para cada uno de los controles.

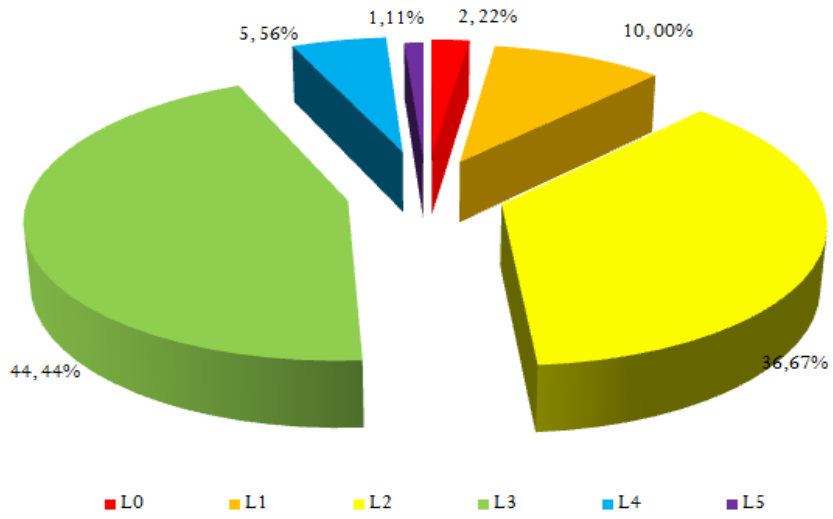
| CONTROL | | Efectividad | CMM |
|---|---|---|---|
| **5. POLITICA DE SEGURIDAD** | | | **L2** |
| **5.1 Dirección de la gestión de seguridad de la información.** | | | |
| 5.1.1 | Políticas de la seguridad de la información | 50% | L2 |
| 5.1.2 | Revisión de las políticas de la seguridad de la información. | 50% | L2 |
| **6. ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN** | | | |
| **6.1 Organización de la seguridad de la información.** | | | |
| 6.1.1 | Funciones y responsabilidades de seguridad de información. | 10% | L1 |
| 6.1.2 | Segregación de funciones. | 50% | L2 |
| 6.1.3 | Contacto con las autoridades. | 10% | L1 |
| 6.1.4 | Contacto con grupos de especial interés. | 0% | L0 |
| 6.1.5 | Seguridad de la información en la gestión de proyectos. | 10% | L1 |
| **6.2 Dispositivos moviles y teletrabajo.** | | | |
| 6.2.1 | Políticas de dispositivos moviles. | NO APLICA | |
| 6.2.2 | Teletrabajo | NO APLICA | |
| **7. SEGURIDAD DE RECURSOS HUMANOS** | | | |
| **7.1 Antes de empleo.** | | | |
| 7.1.1 | Screening | 50% | L2 |
| 7.1.2 | Terminos y condiciones de empleo | 95% | L4 |
| **7.2 Durante el empleo.** | | | |
| 7.2.1 | Responsabilidades de gestión | 20% | L1 |
| 7.2.2 | Conciencia de seguridad de la información y entrenamiento | 50% | L2 |
| 7.2.3 | Proceso disciplinario | 5% | L0 |
| **7.3 Terminación y cambio de empleo.** | | | |
| 7.3.1 | Terminación o cambio de las responsabilidades de empleo | 90% | L3 |
| **8. GESTION DE ACTIVOS** | | | |
| **8.1 Responsabilidad de los activos** | | | |
| 8.1.1 | Inventario de activos | 95% | L4 |
| 8.1.2 | Propiedad de los activos | 90% | L3 |
| 8.1.3 | Retorno de los activos | 90% | L3 |

| | | | |
|---|---|---|---|
| **8.2 Clasificación de la información** | | | |
| 8.2.1 | Clasificación de la información | 60% | L2 |
| 8.2.2 | Etiquetado de la información | 50% | L2 |
| 8.2.3 | Manejo de activos | 25% | L1 |
| **8.3 Manejo de Medios** | | | |
| 8.3.1 | Gestión de medios extraibles | 70% | L2 |
| 8.3.2 | Eliminación de medios | 70% | L2 |
| 8.3.3 | Transferencia de medios fisicos | 70% | L2 |
| **9. CONTROL DE ACCESO** | | | |
| **9.1 Business requirements of access control** | | | |
| 9.1.1 | Politica de control de acceso | 95% | L4 |
| 9.1.2 | Acceso a las redes y servicios de red | 90% | L3 |
| **9.2 Gestión de acceso de usuario** | | | |
| 9.2.1 | Registro de usuario y cancelación de registro | 90% | L3 |
| 9.2.2 | Acceso aprovisionamiento de usuario | 90% | L3 |
| 9.2.3 | Gestión de derechos de accesos privilegiados | 90% | L3 |
| 9.2.4 | Gestión de la información de autentificación de secreto de los usuarios | 90% | L3 |
| 9.2.5 | Revisión de los derechos de acceso de usuario | 90% | L3 |
| 9.2.6 | Eliminación o ajuste de los derechos de acceso | 90% | L3 |
| **9.3 Responsabilidades del usuario** | | | |
| 9.3.1 | Uso de información secreta de autenticación | 10% | L1 |
| **9.4 Control de sistemas y acceso a las aplicaciones** | | | |
| 9.4.1 | Restricción del acceso a la información | 90% | L3 |
| 9.4.2 | Procedimiento de inicio de sesión seguro | 95% | L4 |
| 9.4.3 | Sistema de gestión de contraseñas | 95% | L4 |
| 9.4.4 | Uso de programas de servicios publicos privilegiados | 10% | L1 |
| 9.4.5 | Control de acceso al codigo fuente del programa | NO APLICA | |
| **10. CRIPTOGRAFIA** | | | |
| **10.1 Controles criptograficos** | | | |
| 10.1.1 | Politica sobre el uso de controles criptograficos | NO APLICA | |
| 10.1.2 | Gestión de Claves | NO APLICA | |
| **11. SEGURIDAD FISICA Y AMBIENTAL** | | | |
| **11.1 Areas seguras** | | | |
| 11.1.1 | Perímetro de seguridad fisica | 90% | L3 |
| 11.1.2 | Controles de entrada fisicas | 90% | L3 |
| 11.1.3 | Asegurar oficinas habitaciones e instalaciones | 90% | L3 |
| 11.1.4 | Protección contra amenazas externas y ambientales | 80% | L2 |
| 11.1.5 | Trabajar en zonas seguras | 90% | L3 |
| 11.1.6 | Zonas de entrega y carga | 90% | L3 |
| **11.2 Equipo** | | | |
| 11.2.1 | Ubicación y protección del equipo | 90% | L3 |
| 11.2.2 | Apoyo a los servicios publicos | 10% | L1 |
| 11.2.3 | Seguridad de cableado | 90% | L3 |
| 11.2.4 | Mantenimiento de los equipos | 90% | L3 |
| 11.2.5 | Eliminación de los activos | 90% | L3 |
| 11.2.6 | Seguridad de equipo y activos fuera de las instalaciones | NO APLICA | |
| 11.2.7 | Eliminación segura o reutilización de los equipos | 90% | L3 |
| 11.2.8 | Equipos de usuario desatendidos | NO APLICA | |
| 11.2.9 | Escritorio limpio y politica pantalla limpia | 90% | L3 |

| | | | |
|---|---|---|---|
| **12. OPERACIONES DE SEGURIDAD** | | | |
| **12.1 Procedimientos y responsabilidades operacionales** | | | |
| 12.1.1 | Procedimientos operativos documentales | 90% | L3 |
| 12.1.2 | Gestión del cambio | 80% | L2 |
| 12.1.3 | Gestión de la capadidad | 80% | L2 |
| 12.1.4 | Separación de desarrollo, pruebas y entornos operativos | 50% | L2 |
| **12.2 Protección contra el malware** | | | |
| 12.2.1 | Controles contra el malware | 90% | L3 |
| **12.3 Copias de seguridad** | | | |
| 12.3.1 | Copia de seguridad de la información | 100% | L5 |
| **12.4 Registro y seguimiento** | | | |
| 12.4.1 | Registro de eventos | 80% | L2 |
| 12.4.2 | Protección de la información de los registros | 70% | L2 |
| 12.4.3 | Registros de administración y operación | 70% | L2 |
| 12.4.4 | Sincronización del reloj | 90% | L3 |
| **12.5 Control del software operativo** | | | |
| 12.5.1 | Apoyo a los servicios publicos | NO APLICA | |
| **12.6 Técnico de gestión de vulnerabilidades** | | | |
| 12.6.1 | Gestión de vulnerabilidades técnicas | 90% | L3 |
| 12.6.2 | Restricciones de instalación de software | 90% | L3 |
| **12.7 Sistemas de la información consideraciones de auditoria** | | | |
| 12.7.1 | Sistemas de información controles de auditoria | 90% | L3 |
| **13. SEGURIDAD DE LAS COMUNICACIONES** | | | |
| **13.1 Gestión de la seguridad de la red** | | | |
| 13.1.1 | Funciones y responsabilidades de seguridad de información. | 90% | L3 |
| 13.1.2 | Segregación de funciones. | 90% | L3 |
| 13.1.3 | Segregación en Redes. | 90% | L3 |
| **13.2 Transferencia de Información** | | | |
| 13.2.1 | Politicas y procedimientos de transferencia de información | 80% | L2 |
| 13.2.2 | Acuerdos sobre la transferencia de información | 80% | L2 |
| 13.2.3 | Mensajería electrónica | 10% | L1 |
| 13.2.4 | Acuerdos de confidenciabilidad o de no divulgación | 70% | L2 |
| **14. SISTEMA DE ADQUISICIÓN, DE SARROLLO Y MANTENIMIENTC** | | | |
| **14.1 Requerimientos de seguridad de los sistemas de información** | | | |
| 14.1.1 | Información de analisis de requisitos de seguridad y la especificación | 80% | L2 |
| 14.1.2 | Asegurar los servicios de aplicaciones en las redes publicas | 80% | L2 |
| 14.1.3 | Protección de las transacciones de servicios de aplicaciones | 70% | L2 |
| **14.2 Seguridad en los procesos de desarrollo y de apoyo** | | | |
| 14.2.1 | Politica de desarrollo seguro | NO APLICA | |
| 14.2.2 | Procedimientos de control de cambio del sistema | NO APLICA | |
| 14.2.3 | Revisión técnica de las aplicaciones tras efectuar cambios en la plataforma operativo | NO APLICA | |
| 14.2.4 | Restricciones a los cambios de los paquetes de software | NO APLICA | |
| 14.2.5 | Principios de ingeniería de sistemas seguros | NO APLICA | |
| 14.2.6 | Entorno de desarrollo seguro | NO APLICA | |
| 14.2.7 | Desarrollo outsourced | NO APLICA | |
| 14.2.8 | Pruabas de seguridad del sistema | NO APLICA | |
| 14.2.9 | Pruebas de aceptación del sistema | NO APLICA | |

| | | | |
|---|---|---|---|
| **14.3 Datos de prueba** | | | |
| 14.3.1 | Protección de datos de prueba | NO APLICA | |
| **15.RELACIÓN CON PROVEEDORES** | | | |
| **15.1 Seguridad en la información en las relaciones con proveedore** | | | |
| 15.1.1 | Politica de seguridad de la información para relaciones con los proveedores | 60% | L2 |
| 15.1.2 | Abordar la seguridad dentro de los acuerdos con proveedores | 50% | L2 |
| 15.1.3 | Cadena de la información y tecnologia de comunicación de suministro | NO APLICA | |
| **15.2 Gestión de la prestación de servicios de proveedores** | | | |
| 15.2.1 | Politica de desarrollo seguro | NO APLICA | |
| 15.2.2 | Procedimientos de control de cambio del sistema | NO APLICA | |
| **16. INFORMACIÓN DE GESTIÓN DE INCIDENCIAS DE SEGURIDAD** | | | |
| **16.1 Gestión de incidencias de seguridad de la información y mejo** | | | |
| 16.1.1 | Responsabilidades y procedimientos | 60% | L2 |
| 16.1.2 | Presentación de informes de eventos de seguridad de información | 70% | L2 |
| 16.1.3 | Informes debilides de seguridad de información | 70% | L2 |
| 16.1.4 | Evaliación y decisión sobre los eventos de seguridad de información | 90% | L3 |
| 16.1.5 | Respuestas a incidentes de seguridad de la información | 80% | L2 |
| 16.1.6 | Aprendiendo de los incidentes de seguridad de la información | 90% | L3 |
| 16.1.7 | Acopio de pruebas | 70% | L2 |
| **17. ASPECTOS DE SEGURIDAD DE INFORMACIÓN DE LA GESTIÓ** | | | |
| **17.1 Información continuidad seguridad** | | | |
| 17.1.1 | Planificación información continuidad seguridad | 80% | L2 |
| 17.1.2 | Implementación de la información continuidad seguridad | 80% | L2 |
| 17.1.3 | Verificar, revisar y evaluar la información de seguridad continuidad | 80% | L2 |
| **17.2 Redundancias** | | | |
| 17.2.1 | Disponibilidad de instalaciones de procesamiento de información | 90% | L3 |
| **18. CONFORMIDAD** | | | |
| **18.1 Cumplimiento de los requisitos legales y contractuales** | | | |
| 18.1.1 | Identificación de la legislación aplicable y requisitos contractuales | 90% | L3 |
| 18.1.2 | Derechos de propiedad intelectual | 90% | L3 |
| 18.1.3 | Protección de los registros | 90% | L3 |
| 18.1.4 | Privacidad y protección de datos personales | 90% | L3 |
| 18.1.5 | Reglamento de los controles criptograficos | NO APLICA | |
| **18.2 Revisiones de seguridad de información** | | | |
| 18.2.1 | Revisión independiente de seguridad de la información | NO APLICA | |
| 18.2.2 | Cumplimiento de las politicas y etandares de seguridad | 90% | L3 |
| 18.2.3 | Revisión del cumplimiento técnico | 90% | L3 |

Como resumen, en el siguiente gráfico se muestra cómo se encuentra el cumplimiento de la tabla de controles de la ISO / IEC 27001: 2013 donde tenemos un 2,22% de madurez de nivel L0, un 10% de madurez nivel L1, con un 36,67% tenemos un L2, con un 44,44% un L3, con un 5,56% un L4 y con un 1,11% un L5.




Una visión más detallada se ve en la siguiente gráfica diagrama de radar, donde se puede apreciar el nivel de cumplimiento por capítulos de los dominios de la ISO / IEC 27003, donde los niveles deseados, deberían ser los mas próximos al 100% de cumplimiento.

| | | Nivel de cumplimiento |
|---|---|---|
| 5. | Política de Seguridad | 50% |
| 6. | Organización de la Seguridad de Información | 13% |
| 7. | Seguridad de Recursos Humanos | 52% |
| 8. | Gestión de Activos | 62% |
| 9. | Control de Acceso | 79% |
| 11. | Seguridad física y ambiental | 76% |
| 12. | Operaciones de Seguridad | 76% |
| 13. | Seguridad de las comunicaciones | 73% |
| 14. | Sistema de adquisición, desarrollo y mantenimiento | 77% |
| 15. | Cumplimiento | 37% |
| 16. | Información de gestión de incidentes de seguridad | 76% |
| 17. | Aspectos de seguridad de información de la gestión de | 83% |
| 18. | Conformidad | 90% |

## 6.3 Resultados.

Tras finalizar la auditoría de cumplimiento ISO / IEC 27002: 2013 observamos que la organización ha experimentado una importante mejora en cuanto a términos de seguridad de la información respecto a su situación inicial, donde era prácticamente inexistente en relación a la situación actual.

Destacando obviamente, que en esta primera auditoría aún aparecen dominios con niveles de madurez bastante bajos, en los que habrá que seguir trabajando y modificando hasta obtener la oportuna mejora.

También hay que destacar que los valores obtenidos son estimados ya que sólo se han hecho en función de los proyectos presentados en esta memoria aún no implementados; estando en previsión de implantación una vez se hayan aprobado el preceptivo plan de SGSI como se detallo en la organización y dotado de los presupuestos oportunos.

Tal como se ha indicado tenemos un 2,22% de madurez de nivel L0, un 10% de madurez nivel L1, con un 36,67% tenemos un L2, con un 44,44% un L3, con un 5,56% un L4 y con un 1,11% un L5, demostrando estos datos, que a día de hoy estamos superando un 60% del cumplimiento de la ISO.

***Presentamos documento de Auditoría realizada en el Anexo VI del presente proyecto.***

# 7. Conclusiones.

Finalizado el presente proyecto, podemos concluir principalmente que la información de esta Organización (ampliable a cualquier otra), puede llegar a ser invaluable, ya que su correcta gestión de seguridad pudiera marcar la diferencia entre el éxito y el fracaso. Es claramente comprensible que ha de comenzarse a realizar toda actividad necesaria para establecer un SGSI y posteriormente poder aplicar a la certificación de la norma ISO/IEC 27001:2013.

Tras esta aseveración, un Sistema de Gestión de Seguridad de la Información (SGSI) será un apoyo muy importante que ayudaría a organizar los procesos, controles y salvaguardas con los que se mantendría la información bajo medidas de seguridad que garanticen su integridad, confidencialidad y autenticidad. Establecimiento de un plan de auditoría, informe de auditoría y programa de auditoría.

Para asegurarse de que se mantiene un SGSI adecuado, la implementación debe superar una auditoría de certificación bajo la norma ISO/IEC 27001:2013, norma que impone al SGSI que implemente una serie de requisitos antes de ser sometido a dicha auditoría.

Para poder cumplir con estos requerimientos hemos contado con la norma ISO/IEC 27002:2013 que nos facilita controles que son implementados a nivel técnico. Estas dos norma juntas facilitan el trabajo de la implementación del SGSI dentro de nuestra organización.

Este trabajo puede servir como base para que la organización continúe en las tareas que deben ser realizadas con el fin de a mediano plazo acceder a la certificación ISO/IEC 27001:2013

# 8. Glosario.

**Activo de información**: cualquier información que tiene un valor para la Organización.

**Activos Informáticos**: Son los bienes de la organización que se encuentran relacionados de manera directa o indirecta con la actividad informática.

**Antivirus**: Software diseñado para prevenir, detectar y eliminar malware (software dañino) de varias categorías.

**Autenticidad y no repudio**: Característica que garantiza que la identidad de los usuarios o procesos que tratan la información y de la autoría de una determinada acción

**Autenticación**: procedimiento de comprobación de la identidad de un usuario.

**Backup o copia de Seguridad**: Procesos de copia de la información a medios de almacenamiento como medidas de precaución que facilitan su recuperación en caso de incidentes.

**COBIT**: Control Objectives for Information and related Technology.

**Confidencialidad**: Propiedad de la información que garantiza que la misma solo es accedida por las personas que cuentan autorización para ello.

**Control de acceso**: mecanismo que en función de la identificación ya autenticada permite acceder a datos o recursos.

**Contraseña**: información confidencial, frecuentemente constituida por una cadena de caracteres, que puede ser usada en la autenticación de un usuario.

**CPD**: Centro de Proceso (o de Procesamiento) de Datos.

**Datacenter**: (o también denominado CPD) Ubicación acondicionada para albergar el equipamiento informático (normalmente servidores) que realiza el procesamiento de la información de la organización.

**Directorio Activo**: Servicio de Directorio utilizado en redes de Microsoft que permite una administración y gestión de los nodos y usuarios de la red.

**ERP**: Sistema de gestión para planificar y gestionar los recursos de la empresa (Enterprise Resource Planning).

**Firewall**: Cortafuegos o Firewall es un software que se implementa con el fin de hacer segregación de redes a nivel de comunicaciones, para permitir o denegar los accesos basados en conjuntos de reglas desde y hacia los sistemas que está protegiendo.

**Identificación**: procedimiento de reconocimiento de la identidad de un usuario.

**IDS/IPS**: Intrusion Detection System / Intrusion Prevention System, sistema de prevención y/o detección de intrusos, es un sistema que revisa el tráfico en busca de patrones que coincidan con firmas de ataques conocidos con el fin de detector acciones maliciosas hacia los sistemas que protege.

**ISO**: International Organization for Standardization.

**Integridad**: Propiedad de la información que asegura que la información y sus métodos de procesamiento son exactos y completos y que la misma no se puede manipular sin autorización.

**LOPD**: Ley Orgánica 15/1.999, de 13 de Diciembre, de Protección de Datos de Carácter Personal.

**Privacidad**: Propiedad de la información que garantiza que solo las personas debidamente autorizadas, tendrán acceso a la misma con los permisos requeridos

**Riesgo Intrínseco**: Es el riesgo calculado sin tener en consideración las diferentes medidas de seguridad que ya están implantadas en la organización
**Riesgo Residual**: Es el riesgo calculado tras la aplicación de las salvaguardas o controles, será un riesgo que la organización deba asumir ante la imposibilidad de proteger los activos al 100%.

**Salvaguarda o Contramedida**: Es la medida o medidas de control que se establecen para evitar una situación de riesgo.

**SGSI**: Sistema de Gestión de Seguridad de la Información.

**Software**: Conjunto lógico de instrucciones que los sistemas de cómputo interpretan y/o ejecutan para llevar a cabo determinadas tareas.

**Soporte**: objeto físico que almacena o contiene datos o documentos, u objeto susceptible de ser tratado en un sistema de información y sobre el cual se pueden grabar y recuperar datos.

**Trazabilidad**: Propiedad de la información que garantiza el seguimiento en la creación, manipulación o eliminación de la misma de los diferentes medios en donde se crea, almacena y/o transmite.
**Usuario**: sujeto o proceso autorizado para acceder a datos o recursos de los sistemas de información.

**Virtualización**: Es la creación a través de herramientas software (aplicaciones de virtualización) de la versión virtual de una máquina física o un entorno.

# 9. Bibliografía.

ISO27001
http://www.iso27000.es
http://www.iso27000.es/sgsi_implantar.html#seccion1

Margerit y análisis de riesgos:
http://www.securityartwork.es/2012/04/24/analisis-de-riesgos-con-magerit-en-el-ens-i/
http://www.securityartwork.es/2012/04/26/analisis-de-riesgos-con-magerit-en-el-ens-ii/

PAE – Portal administración electrónica
http://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html#.VH9LC4t9rKM

Inteco – MARGERIT
https://www.incibe.es/extfrontinteco/img/File/intecocert/sgsi/swf/video_07.swf

Inteco – SGSI
www.inteco.es
http://administracionelectronica.gob.es

Otros:
http://seguinfo.wordpress.com/2006/08/02/iso-9001-indicadores-de-gestion/

http://www.iso27000.es/download/HowCanSecurityBeMeasured-SP.pdf

http://www.qualypedia.org/ISO%2027001.S-7-REVISION-POR-LADIRECCION.

https://www.linkedin.com/groups/Sobre-informe-revisi%C3%B3n-direcci%C3%B3n-4115297.S.85458302

http://www.isotools.org/2015/02/04/iso-27001-papel-alta-direccion-sgsi/

http://gestioncalidadiso.blogspot.com.es/2012/05/sistema-de-gestion-de-la-seguridad-de.html

Material de estudio asignatura Sistemas de Gestión de Seguridad de Información

# 10. Anexos.

| | |
|---|---|
| Anexo I | Documento de Políticas de Seguridad. |
| Anexo II | Procedimiento de Auditorías Internas. |
| Anexo III | Gestión de indicadores. |
| Anexo IV | Revisión por la Dirección. |
| Anexo V | Hoja Excel análisis_de_amenazas.xlsx |
| Anexo VI | Auditoria del Cumplimiento. |

**ANEXO I**

**POLITICAS DE SEGURIDAD DE LA INFORMACIÓN.**

| | |
|---|---|
| **Organización** | |
| **Documento** | **Políticas de Seguridad de la Información** |
| **Fecha documento** | **26 Marzo 2015** |

**Contenido.**

1. Introducción.
2. Alcance.
3. Objetivos.
4. Responsabilidad.
5. Organización de la seguridad.
6. Compromisos.
7. Política General de Seguridad de la Información.

## 1. Introducción.

La información es un recurso que, como el resto de los activos, tiene valor para la organización y por consiguiente debe ser debidamente protegida. Las Políticas de Seguridad de la Información protegen a la misma de una amplia gama de amenazas, a fin de garantizar la continuidad de los sistemas de información, minimizar los riesgos de daño y asegurar el eficiente cumplimiento de los objetivos del Organismo.

Es importante que los principios de la Política de Seguridad sean parte de la cultura Empresarial, para ello se debe asegurar un compromiso manifiesto de todos los implicados de la organización y de los responsables de las distintos departamentos.

## 2. Alcance.

Esta Política se aplica en todo el ámbito organizativo, a sus recursos y a la totalidad de los procesos, ya sean internos o externos vinculados a la entidad a través de contratos o acuerdos con terceros.

Nuestra organización tiene como alcance la formación en nuevas tecnologías, reparación y comercialización de sistemas informáticos y redes, así como el soporte técnico en locales propios o del cliente.

## 3. Objetivos.

La política de seguridad elaborada, tiene como objetivos proteger los recursos de información de la organización y la tecnología utilizada para su procesamiento, frente a amenazas, internas o externas, deliberadas o accidentales, con el fin de asegurar el cumplimiento de la confidencialidad, integridad, disponibilidad, legalidad y confiabilidad de la información.

Igualmente, se pretende asegurar la implementación de las medidas de seguridad comprendidas en esta Política, identificando los recursos sin que ello implique necesariamente la asignación de partidas adicionales.

Se ha de mantener la Política de Seguridad de la organización actualizada, a efectos de asegurar su vigencia y nivel de eficacia, garantizando el cumplimiento de las diferentes normativas y estándares aplicables.

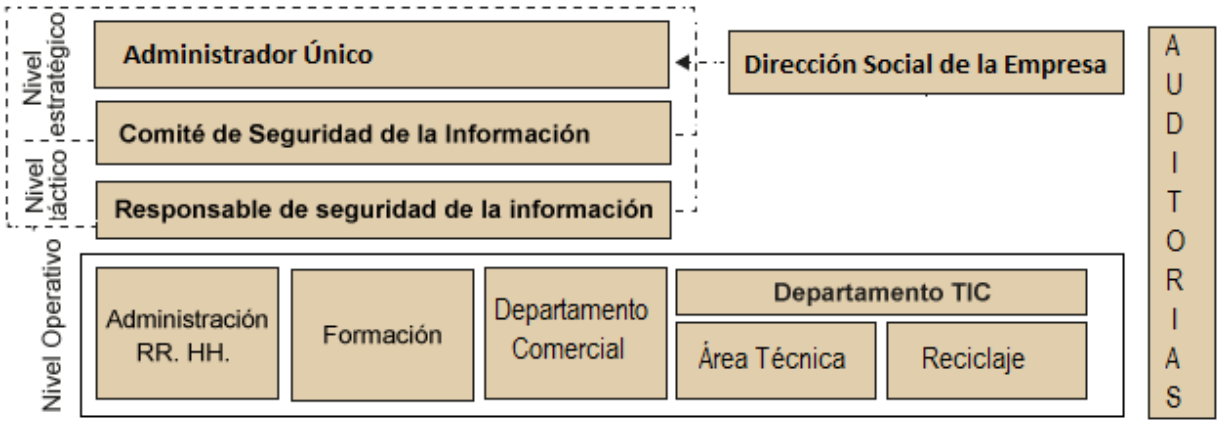
## 4. Responsabilidad.

La organización de la seguridad de la información es una de las primeras tareas a abordar en la implantación del SGSI. Todos los esfuerzos en materia de seguridad de la información serán inútiles o muy poco eficaces si la compañía no tiene claro quién tiene autoridad, sobre qué aspectos y quién es responsable de qué tareas o ámbitos.

Todos los responsables de la organización, son responsables de la implementación de esta Política de Seguridad de la Información dentro de sus áreas de responsabilidad, así como del cumplimiento de dicha Política por parte de su equipo de trabajo.

La Política de Seguridad de la Información es de aplicación obligatoria para todo el personal de la organización, cualquiera que sea su situación en la misma, el área a la cual se encuentre afectado y cualquiera que sea el nivel de las tareas que desempeñe.

A continuación se expone la estructura organizativa de seguridad de la información:




La Dirección social de la empresa, a través del Administrador único forma el Comité de Dirección, cuyas misiones son comenzar a organizar el SGSI nombrando a los miembros del Comité de Seguridad de la Información, dotar este comité de recursos y establecer sus directrices.

El Comité de Seguridad de la Información es el principal órgano del gobierno de seguridad de la información, encargado del direccionamiento estratégico de seguridad y de garantizar que la seguridad de la información se encuentra siempre alineada con los objetivos y estrategias del negocio.

El **Comité de Seguridad de la Información,** procederá a revisar y proponer a la comité de dirección para su aprobación, la Política de Seguridad de la Información y las funciones generales en materia de seguridad de la información.

El **Coordinador del Comité de Seguridad de la Información** será el responsable de coordinar las acciones del Comité de Seguridad de la Información y de impulsar la implementación y cumplimiento de la presente Política.

El **Responsable de Seguridad Informática** cumplirá funciones relativas a la seguridad de los sistemas de información del Organismo, lo cual incluye la supervisión de todos los aspectos inherentes a los temas tratados en la presente Política.

El comité de Seguridad de la información dentro de la organización estará formado por una serie de miembros responsables con capacidad decisoria y otros miembros técnicos con la responsabilidad de asesorar y apoyar la toma de decisiones.

Miembros con capacidad decisoria:

- Coordinador del Comité de Seguridad (Administrador único).
- Director Comercial.
- Responsable de Área Técnica (Jefe seguridad Informática).
- Responsable de Administración.
- Responsable de Formación.

Miembros con la responsabilidad de asesorar y apoyar la toma de decisiones:

- Responsable de de Seguridad de la Información.
- Auditores.

El Responsable de Seguridad de la Información, debe ser nuevo cargo dentro de la empresa e independiente, siendo el encargado de liderar las propuestas y la agenda del Comité.

Los Auditores, podrán ser de una empresa de auditoría externa o en caso de ser seleccionado de entre el personal del departamento técnico, deberá realizar las labores de este cometido de forma totalmente autónoma e independiente, para mantener una postura totalmente objetiva.

## 5. Organización de la seguridad.

La presente Política de Seguridad establece la administración de la seguridad de la información, como parte fundamental de los objetivos y actividades. Por ello, se definirá formalmente un ámbito de gestión para efectuar tareas tales como la aprobación de la Política, la coordinación de su implementación y la asignación de funciones y responsabilidades.

Por otro lado debe tenerse en cuenta que ciertas actividades pueden requerir que terceros accedan a información interna, o bien puede ser necesaria la tercerización de ciertas funciones relacionadas con el procesamiento de la información. En estos casos se considerará que la información puede ponerse en riesgo si el acceso de dichos terceros se produce en el marco de una inadecuada administración de la seguridad, por lo que se establecerán las medidas adecuadas para la protección de la información.

Esta Política se aplica a todos los recursos de la organización y a todas sus relaciones con terceros que impliquen el acceso a sus datos, recursos y/o a la administración y control de sus sistemas de información.

La seguridad de la información es una responsabilidad compartida por todos los responsables y directivos, por lo cual se crea el Comité de Seguridad de la Información, integrado por representantes de todos los departamentos, destinado a garantizar el apoyo manifiesto de todo el personal. El mismo contará con un Coordinador, quien cumplirá la función de impulsar la implementación de la presente Política.

Este Comité de Seguridad, tendrá entre sus funciones:

- Revisar y proponer a la dirección de la organización para su aprobación, la Política y las funciones generales en materia de seguridad de la información.
- Monitorizar cambios significativos en los riesgos que afectan a los recursos de información frente a las amenazas más importantes.
- Tomar conocimiento y supervisar la investigación y monitorización de los incidentes relativos a la seguridad.
- Aprobar las principales iniciativas para incrementar la seguridad de la información, de acuerdo a las competencias y responsabilidades asignadas a cada área.
- Acordar y aprobar metodologías y procesos específicos relativos a la seguridad de la información.
- Garantizar que la seguridad sea parte del proceso de planificación de la información.
- Evaluar y coordinar la implementación de controles específicos de seguridad de la información para nuevos sistemas o servicios.
- Promover la difusión y apoyo a la seguridad de la información dentro del Organismo.
- Coordinar el proceso de administración de la continuidad de los sistemas de tratamiento de la información del Organismo frente a interrupciones imprevistas.

El Comité de Seguridad de la Información propondrá a la autoridad que corresponda para su aprobación la definición y asignación de las responsabilidades que surjan del presente Modelo. De igual forma, seguidamente se detallan los propietarios de la información, quienes serán los Responsables de los departamentos a cargo del manejo de la misma.

Los propietarios de de cada información, pueden delegar la administración de sus funciones a personal idóneo a su cargo, pero siempre conservarán la responsabilidad del cumplimiento de las mismas. Esta delegación de la administración por parte de los propietarios de la información será documentada por los mismos y proporcionada al Responsable de Seguridad Informática.

Los nuevos recursos de procesamiento de información serán autorizados por los Responsables de las Unidades Organizativas involucradas, considerando su propósito y uso, conjuntamente con el Responsable de Seguridad Informática, a fin de garantizar que se cumplan todas las Políticas y requerimientos de seguridad pertinentes.

Cuando corresponda, se verificará el hardware y software para garantizar su compatibilidad con los componentes de otros sistemas de la organización.

El uso de recursos personales de procesamiento de información en el lugar de trabajo puede ocasionar nuevas vulnerabilidades. En consecuencia, su uso será evaluado en cada caso por el Responsable de Seguridad Informática y deberá ser autorizado por el Responsable del Área Informática y por el responsable del área al que se destinen los recursos.

La persona responsable de la Auditoría Interna o en su defecto quien sea propuesto por el Comité de Seguridad de la Información realizará revisiones independientes sobre la vigencia e implementación de la Política de Seguridad de la Información, a efectos de garantizar que las prácticas de la organización reflejan adecuadamente sus disposiciones.

## 6. Compromisos.

La dirección de esta empresa reconoce que la información es un activo vital para la operación del negocio y por lo se compromete con su protección de acuerdo con su valor y sensibilidad, independientemente del medios en que se encuentre, velando por su confidencialidad, integridad y disponibilidad.

Desde la dirección, se dará cumplimiento a todas las regulaciones, leyes y normativas vigentes relacionadas con Seguridad de la Información, igualmente se signarán los recursos requeridos para la implementación, mantenimiento y mejora del Sistema de Gestión de Seguridad de la Información.

Se realizará una evaluación periódicamente el estado general del Sistema de Gestión de Seguridad de la Información, por parte del Comité de Seguridad de la Información relativa a los principales riesgos identificados, haciéndose un seguimiento detallado a los correspondientes planes de acción.

La organización tendrá un detallado conocimiento sobre los activos que posee como parte importante de la administración de riesgos. Clasificándose estos activos en:

- *Recursos de información:* bases de datos y archivos, documentación de sistemas, manuales de usuario, material de capacitación, procedimientos operativos o de soporte, planes de continuidad, información archivada, etc.

- *Recursos de software:* software de aplicaciones, sistemas operativos, herramientas de desarrollo, utilitarios, etc.

- *Activos físicos*: equipamiento informático (servidores, PCs, monitores, portátiles, etc.), equipos de comunicaciones (routers, Switch, fax, telefonía IP,…), medios magnéticos (cintas, discos), otros equipos técnicos (relacionados con el suministro eléctrico, unidades de aire acondicionado), mobiliario, lugares de emplazamiento, etc.

- *Servicios:* servicios informáticos y de comunicaciones, de uso genera.

Se identificarán los activos importantes asociados a cada sistema de información, sus respectivos propietarios y su ubicación, para luego elaborar un inventario con dicha información. El mismo será actualizado ante cualquier modificación de la información registrada y revisado con una periodicidad de 6 meses. El encargado de elaborar el inventario y mantenerlo actualizado es cada Responsable de departamento.

La seguridad de la información se basa en la capacidad para preservar su integridad, confidencialidad y disponibilidad, por parte de los elementos involucrados en su tratamiento: equipamiento, software, procedimientos, así como de los recursos humanos que utilizan dichos componentes.

En este sentido, es fundamental educar e informar al personal desde su ingreso y en forma continua, cualquiera sea su situación de revista, acerca de las medidas de seguridad que afectan al desarrollo de sus funciones y de las expectativas depositadas en ellos en materia de seguridad y asuntos de confidencialidad. De la misma forma, es necesario definir las sanciones que se aplicarán en caso de incumplimiento.

El Responsable de Personal (Recursos Humanos) incluirá las funciones relativas a la seguridad de la información en las descripciones de puestos de los empleados, informará a todo el personal que ingresa de sus obligaciones respecto del cumplimiento de la Política de Seguridad de la Información, gestionará los Compromisos de Confidencialidad con el personal y coordinará las tareas de capacitación de usuarios respecto de la presente Política.

A falta de departamento Legal, igualmente el departamento de Personal participará en la confección del Compromiso de Confidencialidad a firmar por los empleados y terceros que desarrollen funciones en la empresa, recurriendo si fuera preciso a personal externo (despacho abogados) en el asesoramiento sobre las sanciones a ser aplicadas por incumplimiento de la presente Política y en el tratamiento de incidentes de seguridad que requieran de su intervención.

Como parte de sus términos y condiciones iniciales de empleo, los empleados, cualquiera sea su situación, firmarán un Compromiso de Confidencialidad o no divulgación, en lo que respecta al tratamiento de la información del Organismo. La copia firmada del Compromiso deberá ser retenida en forma segura por el departamento de Personal.

Los incidentes relativos a la seguridad serán comunicados tan pronto como sea posible, estableciéndose un procedimiento formal de comunicación y de respuesta a incidentes, indicando la acción que ha de emprenderse al recibir un informe sobre incidentes. Dicho procedimiento deberá contemplar que ante la detección de un supuesto incidente o violación de la seguridad, el Responsable de Seguridad Informática sea informado tan pronto como se haya tomado conocimiento.

El responsable de Seguridad indicará los recursos necesarios para la investigación y resolución del incidente, y se encargará de su monitoreo. Asimismo, mantendrá al Comité de Seguridad al tanto de la ocurrencia de incidentes de seguridad.

## 7. Política General de Seguridad de la Información.

Se establecen las siguientes Políticas Generales de Seguridad de la Información, las cuales representan la visión de la organización en cuanto a la protección de sus activos de Información:

1. Existirá un Comité de Seguridad de la Información, que será el responsable del mantenimiento, revisión y mejora del Sistema de Gestión de Seguridad de la Información.

2. Los activos de información serán identificados y clasificados para establecer los mecanismos de protección necesarios.

3. Se definirá e implantará controles para proteger la información contra violaciones de autenticidad, accesos no autorizados, la perdida de integridad y que garanticen la disponibilidad requerida por los clientes y usuarios de los servicios ofrecidos por la Entidad.

4. Todos los empleados y personal externo serán responsables de proteger la información a la cual accedan y procesen, para evitar su pérdida, alteración, destrucción o uso indebido.

5. Se realizarán auditorías y controles periódicos sobre el modelo de gestión de Seguridad de la Información.

6. Únicamente se permitirá el uso de software autorizado que haya sido adquirido legalmente por la Institución.

7. Es responsabilidad de todos los empleados y personal externo reportar los Incidentes de Seguridad, eventos sospechosos y el mal uso de los recursos que identifique.

8. Las violaciones a las Políticas y Controles de Seguridad de la Información serán reportadas, registradas y monitoreadas.

9. La organización contará con un Plan de Continuidad del Negocio que asegure la continuidad de las operaciones, ante la ocurrencia de eventos no previstos o desastres naturales.

Además, se establecen políticas específicas y un conjunto de estándares y procedimientos que soportan la política corporativa:

***Acuerdos de confidencialidad.***
Todos los empleados y personal externo deben aceptar los acuerdos de confidencialidad definidos por la organización, los cuales reflejan los compromisos de protección y buen uso de la información de acuerdo con los criterios establecidos en ella.

***Acceso a Internet.***
Internet es una herramienta de trabajo que permite navegar en muchos sitios relacionados o no con las actividades propias del negocio, por lo cual el uso adecuado de este recurso se debe controlar, verificar y monitorear, considerando, para todos los casos, los siguientes lineamientos:

a) No está permitido:

- El acceso a páginas relacionadas con pornografía, drogas, alcohol, webproxys, hacking y/o cualquier otra página que vaya en contra de la ética moral, las leyes vigentes o políticas aquí establecidas.

- El acceso y el uso de servicios interactivos o mensajería instantánea como Facebook, Kazaa, MSN Messenger, Yahoo, Skype, Net2phone y otros similares, que tengan como objetivo crear comunidades para intercambiar información, o bien para fines diferentes a las actividades propias de la organización.

- El intercambio no autorizado de información de propiedad de la empresa, de sus clientes y/o de sus empleados, con terceros.

- La descarga, uso, intercambio y/o instalación de juegos, música, películas, protectores y fondos de pantalla, software de libre distribución, información y/o productos que de alguna forma atenten contra la propiedad intelectual, o que contengan archivos ejecutables y/o herramientas que atenten contra la integridad, disponibilidad y/o confidencialidad de la infraestructura tecnológica (hacking), entre otros.

b) Se debe realizar monitoreo permanente de tiempos de navegación y páginas visitadas por parte de los trabajadores y/o terceros. Así mismo, puede inspeccionar, registrar y evaluar las actividades realizadas durante la navegación, de acuerdo a la legislación vigente.

c) Cada uno de los usuarios es responsable de dar un uso adecuado a este recurso y en ningún momento puede ser usado para realizar prácticas ilícitas o mal intencionadas que atenten contra terceros o la legislación vigente.

d) Los trabajadores y terceros, no pueden asumir en nombre de la empresa, posiciones personales en encuestas de opinión, foros u otros medios similares.

e) El uso de Internet no considerado dentro de las restricciones anteriores, es permitido siempre y cuando se realice de manera ética, razonable, responsable, no abusiva y sin afectar la productividad ni la protección de la información de nuestra organización.

***Correo electrónico.***
Los empleados de la organización y terceros autorizados a quienes se les asigne una cuenta de correo deberán seguir los siguientes lineamientos:

a) La cuenta de correo electrónico debe ser usada exclusivamente para el desempeño de las funciones asignadas.

b) Los mensajes y la información contenida en los buzones de correo son propiedad de la organización y cada usuario, como responsable de su buzón, debe mantener solamente los mensajes relacionados con el desarrollo de sus funciones.

c) El tamaño de los buzones de correo es determinado por el Departamento TIC de acuerdo con las necesidades de cada usuario y previa autorización del Jefe de la dependencia correspondiente.

d) El tamaño de envío y recepción de mensajes, sus contenidos y demás características propios de estos deberán ser definidos e implementados por la Dirección TIC.

e) No es permitido:

- Enviar cadenas de correo, mensajes con contenido religioso, político, racista, sexista, pornográfico, publicitario no corporativo o cualquier otro tipo de mensajes que atenten contra la dignidad y la productividad de la empresa.

- Utilizar la dirección de correo electrónico asignada como punto de contacto en comunidades interactivas de contacto social, o cualquier otro sitio que no tenga que ver con las actividades laborales.

- El envío de archivos que contengan extensiones ejecutables, bajo ninguna circunstancia.

- El envío de archivos de música y videos. En caso de requerir hacer un envío de este tipo de archivos deberá ser autorizado por la dirección respectiva y la Dirección TIC.

f) El envío de información corporativa debe ser realizado exclusivamente desde la cuenta de correo proporcionada. De igual manera, las cuentas de correo genéricas no se deben emplear para uso personal.

g) Toda información de la empresa generada con los diferentes programas computacionales (Ej. Office, Project, Access, Wordpad, etc.), que requiera ser enviada fuera de la Entidad, y que por sus características de confidencialidad e integridad deba ser protegida, debe estar en formatos no editables.

h) Todos los mensajes enviados deben respetar el estándar de formato e imagen corporativa definido por la organización y deben conservar en todos los casos el mensaje legal corporativo de confidencialidad.

***Recursos tecnológicos.***
El uso adecuado de los recursos tecnológicos asignados a los trabajadores y/o terceros se reglamenta bajo las siguientes condiciones:

a) La instalación de cualquier tipo de software o hardware en los equipos de es responsabilidad del departamento TIC, y por tanto son los únicos autorizados para realizar esta labor.

b) Los usuarios no deben realizar cambios en las estaciones de trabajo relacionados con la configuración del equipo. Estos cambios pueden ser realizados únicamente por el departamento TIC.

c) La Dirección del departamento TIC debe definir y actualizar, de manera periódica, la lista de software y aplicaciones autorizadas que se encuentran permitidas para ser instaladas en las estaciones de trabajo de los usuarios.

e) La conexión a redes inalámbricas externas para usuarios con equipos portátiles que estén fuera de la oficina y que requieran establecer una conexión a la infraestructura tecnológica de la organización, deben utilizar una conexión bajo los esquemas y herramientas de seguridad autorizados y establecidos por la Dirección del departamento TIC.

f) Sólo personal autorizado puede realizar actividades de administración remota de dispositivos, equipos o servidores de la infraestructura de procesamiento de información; las conexiones establecidas para este fin, deben utilizar los esquemas y herramientas de seguridad y administración definidos por la Dirección del departamento TIC.

***Control de acceso físico.***
Todas las áreas destinadas al procesamiento o almacenamiento de información sensible, así como aquellas en las que se encuentren los equipos y demás infraestructura de soporte a los sistemas de información y comunicaciones, se consideran áreas de acceso restringido. Debiendo contar con medidas de control de acceso físico en el perímetro tales que puedan ser auditadas, así como con procedimientos de seguridad operacionales que permitan proteger la información, el software y el hardware de daños intencionales o accidentales.

De igual forma, el centro de proceso de datos (CPD), cableado y cuartos técnicos de las oficinas deben contar con mecanismos que permitan garantizar que se cumplen los requerimientos ambientales (temperatura, humedad, etc.), especificados por los fabricantes de los equipos que albergan y que pueden responder de manera adecuada ante incidentes como incendios e inundaciones.

***Protección y ubicación de los equipos.***
Los equipos que forman parte de la infraestructura tecnológica tales como, servidores, equipos de comunicaciones y seguridad electrónica, centros de cableado, UPS, aires acondicionados, así como estaciones de trabajo y dispositivos de almacenamiento que contengan y/o brinden servicios de soporte a la información crítica de las dependencias, deben ser ubicados y protegidos adecuadamente para prevenir la pérdida, daño, robo o acceso no autorizado de los mismos.

De igual manera, se debe adoptar los controles necesarios para mantener los equipos alejados de sitios que puedan tener riesgo de amenazas potenciales como

fuego, explosivos, agua, polvo, vibración, interferencia electromagnética y vandalismo, entre otros.

***Protección contra software malicioso.***
Se establece que todos los recursos informáticos deben estar protegidos mediante herramientas y software de seguridad como antivirus, antispam, antispyware y otras aplicaciones que brindan protección contra código malicioso, contándose con los controles adecuados para detectar, prevenir y recuperar posibles fallos causados por código malicioso. Será responsabilidad de la Dirección de Tecnología autorizar el uso de las herramientas y asegurar que estas y el software de seguridad no sean deshabilitados bajo ninguna circunstancia, así como de su actualización permanente.

Así mismo no está permitido:

- La desinstalación y/o desactivación de software y herramientas de seguridad configuradas por la organización.

- Utilizar medios de almacenamiento físico o virtual que no sean de carácter corporativo.

.

***Copias de respaldo.***
Se debe asegurar que la información de alto nivel de clasificación, definida por la Dirección del departamento TIC y las dependencias responsables de la misma, contenida en la plataforma tecnológica de la Institución, como servidores, dispositivos de red para almacenamiento de información, estaciones de trabajo, archivos de configuración de dispositivos de red y seguridad, entre otros, sea periódicamente resguardada mediante mecanismos y controles adecuados que garanticen su identificación, protección, integridad y disponibilidad.

Se deberá establecer un plan de restauración de copias de seguridad que serán probados a intervalos regulares con el fin de asegurar que son confiables en caso de emergencia y retenidas por un periodo de tiempo determinado.

La Dirección TIC establecerá procedimientos explícitos de resguardo y recuperación de la información que incluyan especificaciones acerca del traslado, frecuencia, identificación y definirá conjuntamente con las dependencias los períodos de retención de la misma.

Los medios magnéticos que contienen la información crítica deben ser almacenados en otra ubicación diferente a las instalaciones donde se encuentra dispuesta. El sitio externo donde se resguardan dichas copias, debe tener los controles de seguridad adecuados, cumplir con máximas medidas de protección y seguridad física apropiados.

***Gestión de medios removibles.***
El uso de medios de almacenamiento removibles (CDs, DVDs, USBs, memorias flash, discos duros externos, cintas) sobre la infraestructura para el procesamiento de la información, estará autorizado para aquellos funcionarios cuyo perfil del cargo y funciones lo requiera.

La Dirección de TIC es responsable de implementar los controles necesarios para asegurar que en los sistemas de información el personal autorizado puede hacer uso de los medios de almacenamiento removibles. Igualmente, este personal autorizado se comprometerá a asegurar física y lógicamente el dispositivo a fin de no poner en riesgo la información que éste contiene.

***Control de acceso lógico.***
El acceso a plataformas, aplicaciones, servicios y en general cualquier recurso de información debe ser asignado de acuerdo a la identificación previa de requerimientos de seguridad y del utilización que se definan por las diferentes dependencias de la organización, así como normas legales y leyes aplicables a la protección de acceso a la información presente en los sistemas de información.

Los responsables de la administración de la infraestructura tecnológica asignan los accesos a plataformas, usuarios y segmentos de red de acuerdo a procesos formales de autorización los cuales deben ser revisados de manera periódica por la Dirección TIC.

La autorización para el acceso a los sistemas de información debe ser definida y aprobada por la dirección del departamento propietario de la información y se debe otorgar de acuerdo con el nivel de clasificación de la información identificada, según la cual se deben determinar los controles y privilegios de acceso que se pueden otorgar a cada usuario e implementada por la Dirección de Tecnología.

Cualquier usuario interno o externo que requiera acceso remoto a la red y a la infraestructura de procesamiento de información, siempre debe estar autenticado y sus conexiones deberán utilizar cifrado de datos.

***Gestión de contraseñas de usuario.***
Todos los recursos de información críticos tienen asignados los privilegios de acceso de usuarios con base a los roles y perfiles que cada usuario requiera para el desarrollo de sus funciones, definidos y aprobados por los departamentos y administrados por la Dirección TIC
.
Todo funcionario o tercero que requiera tener acceso a los sistemas de información debe estar debidamente autorizado y debe acceder a dichos sistemas haciendo uso de un usuario LDAP y contraseña asignado por la organización. El usuario debe ser responsable por el buen uso de las credenciales de acceso asignadas.

***Segregación de redes.***
La plataforma tecnológica que soporta los sistemas de Información debe estar separada en segmentos de red físicos y lógicos e independientes de los segmentos de red de usuarios externos (aulas formación), de conexiones con redes con terceros y del servicio de acceso a Internet. La división de estos segmentos debe ser realizada por medio de dispositivos perimetrales e internos de enrutamiento y de seguridad si así se requiere. La Dirección TIC es el área encargada de establecer el perímetro de seguridad necesario para proteger dichos segmentos, de acuerdo con el nivel de criticidad del flujo de la información transmitida.

Se establecen mecanismos de identificación automática de equipos en la red, como medio de autenticación de conexiones, desde segmentos de red específicos hacia las plataformas donde operan los sistemas de información de la Organización.

Es responsabilidad de los administradores de los recursos tecnológicos de la organización, garantizar que los puertos físicos y lógicos de diagnóstico y configuración de plataformas que soporten sistemas de información deban estar siempre restringidos y monitoreados con el fin de prevenir accesos no autorizados.

***Identificación de requerimientos de seguridad.***
La inclusión de un nuevo producto de hardware, software, aplicativo, cambios y/o actualizaciones a los sistemas existentes, deben estar acompañados de la identificación, análisis, documentación y aprobación de los requerimientos de seguridad de la información; labor que debe ser responsabilidad de la Dirección TIC y los departamentos propietarias del sistema en cuestión.

Los requerimientos de seguridad de la información identificados, obligaciones derivadas de las leyes de propiedad intelectual y derechos de autor deben ser establecidos en los acuerdos contractuales que se realicen entre la empresa y cualquier proveedor de productos y/o servicios asociados a la infraestructura de procesamiento de información. Es responsabilidad de la Dirección TIC garantizar la definición y cumplimiento de los requerimientos de seguridad de la Información y en conjunto con la Secretaria General establecer estos aspectos con las obligaciones contractuales especificas.

**ANEXO II**

**PLANIFICACION DE AUDITORIA INTERNA.**

| | |
|---|---|
| **Organización** | |
| **Documento** | **Planificación de Auditoría Interna.** |
| **Fecha documento** | **26 Marzo 2015** |

**Contenido.**

1. Introducción.
2. Objetivos.
3. Auditor/Auditores.
4. Metodología.
5. Cronograma.

## 1. Introducción.

Este procedimiento se aplica a todas las actividades realizadas dentro del Sistema de Gestión de Seguridad de la Información (SGSI)

## 2. Objetivos.

El objetivo de la auditoría interna es determinar si los procedimientos, controles, procesos, acuerdos y demás actividades dentro del SGSI concuerdan con las normas ISO 27001, con las regulaciones correspondientes y con la documentación interna de la organización; como también verificar si son implementados y sostenidos y si cumplen requisitos de políticas y establecen objetivos.

## 3. Auditor/Auditores.

Junto con la dirección, el responsable de seguridad en la empresa, tendrá la responsabilidad de determinar la composición del equipo en base a los objetivos de auditoría, el alcance, los criterios y la duración estimada de la auditoría. Debiendo de tener en cuenta la competencia general del auditor o equipo auditor necesaria para conseguir los objetivos de la auditoría y los requisitos necesarios de los organismos de acreditación/certificación, si es de aplicación.

Es necesario preservar la independencia del equipo auditor de las actividades a ser auditadas, y evitar conflictos de intereses, máxime como en el caso que nos ocupa, que el auditor en principio (aunque se contempla una auditoria por parte de empresa especializada también) es una persona de la empresa, del departamento TIC, con conocimientos suficientes e independencia.

Los conocimientos y habilidades del auditor en la empresa, deben contemplar:

- Estudios acordes a la labor recomendada, con una Ingeniería técnica como mínimo y deseable la titulación de Master en la materia.
- Capacidad de comunicación con el personal afectado.
- Capacidad de previsión y resolución de conflictos.
- Haber participado en auditorías como miembro de un equipo auditor.
- Conocimientos sobre los principios de auditoría, procedimientos y técnicas que le permitan asegurarse de que las auditorías se llevan a cabo de manera coherente y sistemática.
- Haber desarrollado los informes relativos a la auditoría en la que participó.

El plan de auditoría deberá estar aprobado tanto por el auditor como por parte de la dirección de la empresa. Una vez realizada, se confeccionará un informe lo más simple y directo posible facilitando la información relevante, así como los distintos hallazgos realizados. Al mismo tiempo, debe facilitar de manera sencilla la forma de resolver las deficiencias halladas.

El informe final de auditoría puede seguir cualquier esquema, pero el elegido debe incluir o tratar de un modo u otro los siguientes aspectos:

- Resumen ejecutivo.
- Metodología empleada.
- Listado detallado de los hallazgos.
- Anexos recopilando información que respalde los hallazgos descritos en el cuerpo del informe.

Las auditorías se realizarán una vez por año en el marco de la ISO 27001 y todos los años se realizarán los planes de auditoría y se emitirán los informes oportunos.

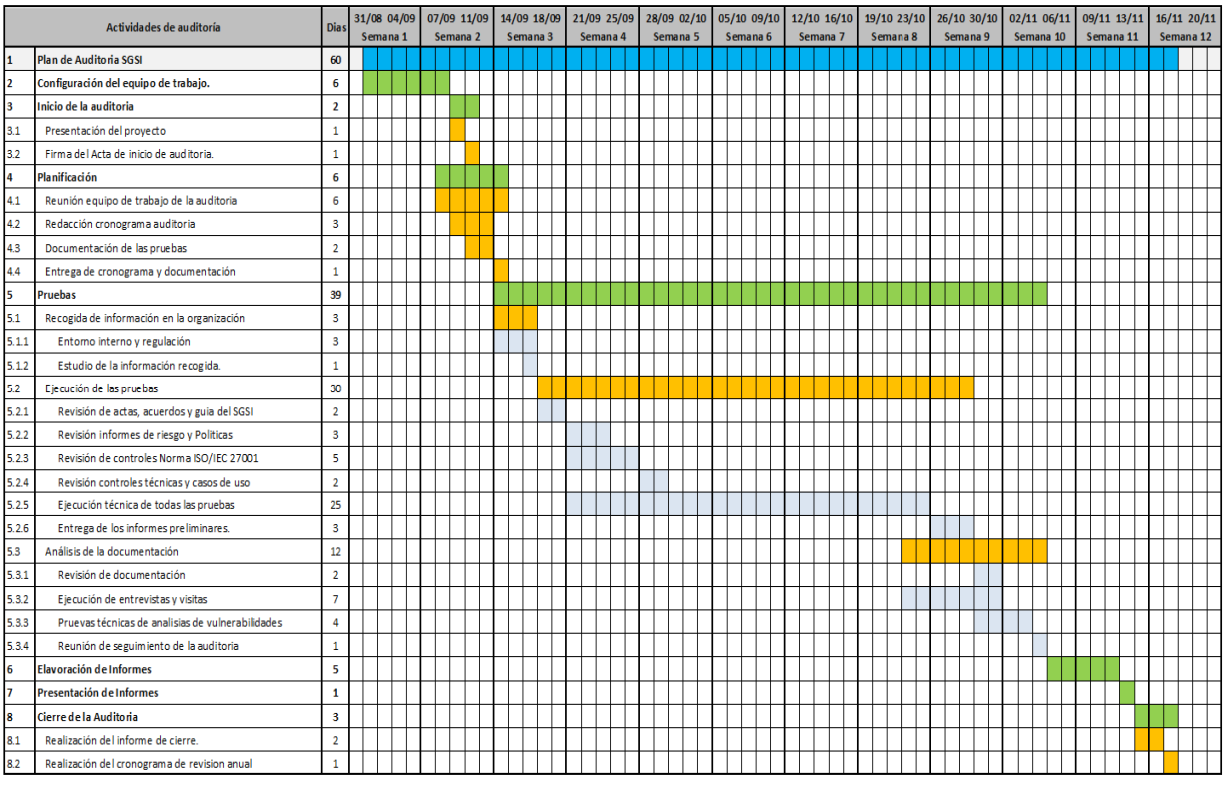
## 4. Metodología.

La presente figura representa de manera esquemática la metodología para llevar a cabo las auditorías internas:

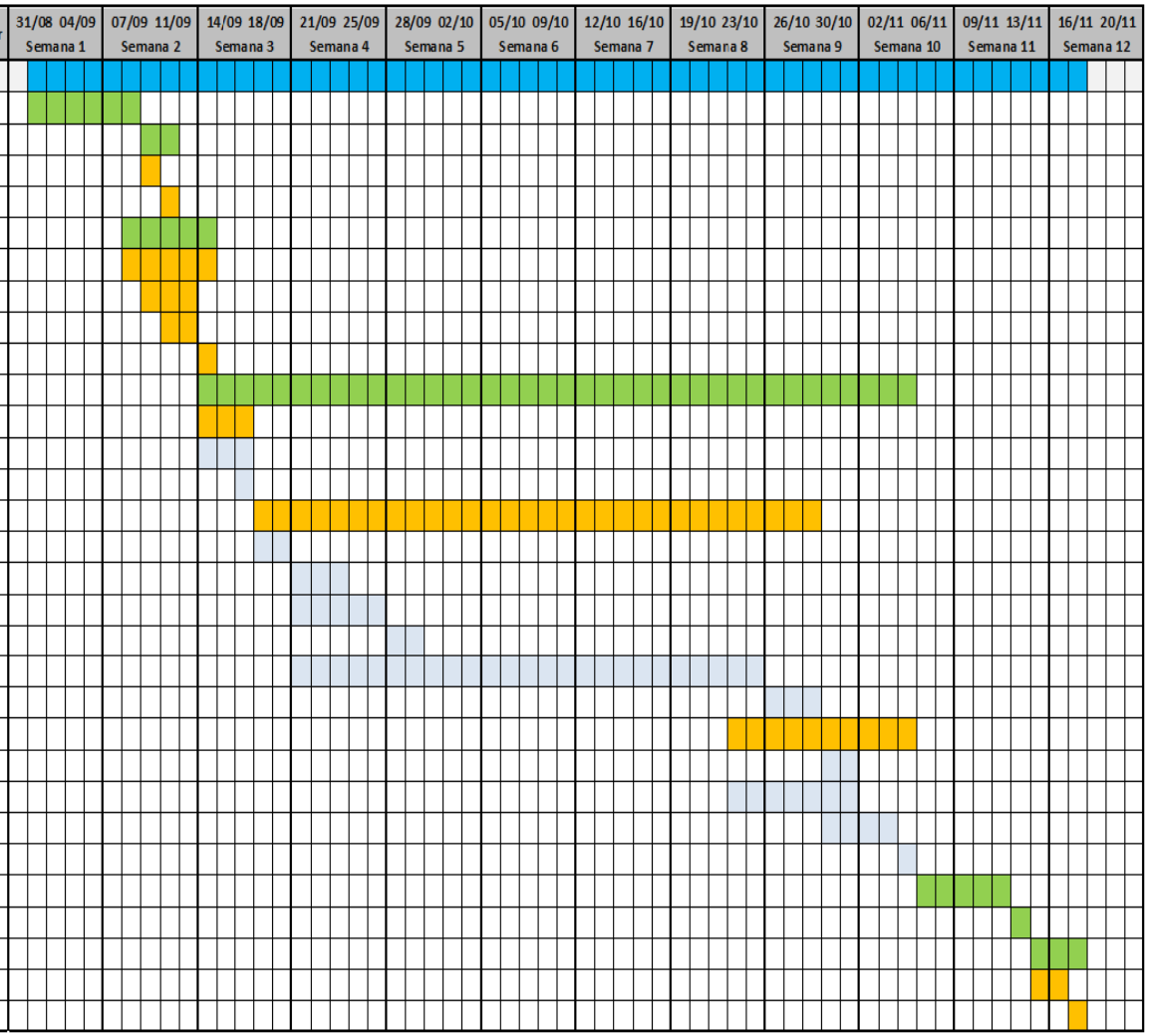

## 5. Cronograma.

| | Actividades de auditoría | Dias | Fecha de inicio | Fecha de fin | Predecesor |
|---|---|---|---|---|---|
| **1** | **Plan de Auditoria SGSI** | **60** | **01/09/2015** | **17/11/2015** | |
| **2** | **Configuración del equipo de trabajo.** | **6** | **01/09/2015** | **08/09/2015** | |
| **3** | **Inicio de la auditoria** | **2** | **09/09/2015** | **10/09/2015** | |
| 3.1 | Presentación del proyecto | 1 | 09/09/2015 | 10/10/2015 | 2 |
| 3.2 | Firma del Acta de inicio de auditoria. | 1 | 10/10/2015 | 10/09/2015 | 3.1 |
| **4** | **Planificación** | **6** | **08/09/2015** | **14/09/2015** | |
| 4.1 | Reunión equipo de trabajo de la auditoria | 6 | 08/09/2015 | 14/09/2015 | |
| 4.2 | Redacción cronograma auditoria | 3 | 08/09/2015 | 10/09/2015 | |
| 4.3 | Documentación de las pruebas | 2 | 10/09/2015 | 11/09/2015 | |
| 4.4 | Entrega de cronograma y documentación | 1 | 14/09/2015 | 14/09/2015 | 4.3 |

| | | | | | |
|---|---|---|---|---|---|
| **5** | **Pruebas** | **39** | **14/09/2015** | **04/11/2015** | |
| 5.1 | Recogida de información en la organización | 3 | 14/09/2015 | 16/09/2015 | |
| 5.1.1 | Entorno interno y regulación | 3 | 14/09/2015 | 16/09/2015 | |
| 5.1.2 | Estudio de la información recogida. | 1 | 16/09/2015 | 16/09/2014 | |
| 5.2 | Ejecución de las pruebas | 30 | 17/09/2015 | 28/10/2015 | |
| 5.2.1 | Revisión de actas, acuerdos y guia del SGSI | 2 | 17/09/2015 | 18/09/2015 | |
| 5.2.2 | Revisión informes de riesgo y Politicas | 3 | 21/09/2015 | 23/09/2015 | |
| 5.2.3 | Revisión de controles Norma ISO/IEC 27001 | 5 | 21/09/2015 | 25/09/2015 | |
| 5.2.4 | Revisión controles técnicas y casos de uso | 2 | 28/09/2015 | 29/09/2015 | |
| 5.2.5 | Ejecución técnica de todas las pruebas | 25 | 21/09/2015 | 23/10/2015 | |
| 5.2.6 | Entrega de los informes preliminares. | 3 | 26/10/2015 | 28/10/2015 | 5.2.5 |
| 5.3 | Análisis de la documentación | 12 | 22/10/2015 | 04/11/2015 | |
| 5.3.1 | Revisión de documentación | 2 | 29/10/2015 | 30/10/2015 | 5.2.6 |
| 5.3.2 | Ejecución de entrevistas y visitas | 7 | 22/10/2015 | 30/10/2014 | |
| 5.3.3 | Pruevas técnicas de analisias de vulnerabilidades | 4 | 29/10/2015 | 03/11/2015 | 5.2.6 |
| 5.3.4 | Reunión de seguimiento de la auditoria | 1 | 04/11/2015 | 04/11/2015 | 5.3.3 |
| **6** | **Elavoración de Informes** | **5** | 05/11/2015 | 11/11/2015 | 5.3.4 |
| **7** | **Presentación de Informes** | **1** | 12/11/2015 | 12/11/2015 | 6 |
| **8** | **Cierre de la Auditoria** | **3** | 13/11/2015 | 17/11/2015 | |
| 8.1 | Realización del informe de cierre. | 2 | 13/11/2015 | 16/11/2015 | 7 |
| 8.2 | Realización del cronograma de revision anual | 1 | 17/11/2015 | 17/11/2015 | 8.1 |



| | Actividades de auditoría | Dias | Fecha de inicio | Fecha de fin | Predecesor |
|---|---|---|---|---|---|
| 1 | **Plan de Auditoria SGSI** | **60** | **01/09/2015** | **17/11/2015** | |
| 2 | **Configuración del equipo de trabajo.** | **6** | **01/09/2015** | **08/09/2015** | |
| 3 | **Inicio de la auditoria** | **2** | **09/09/2015** | **10/09/2015** | |
| 3.1 | Presentación del proyecto | 1 | 09/09/2015 | 10/10/2015 | 2 |
| 3.2 | Firma del Acta de inicio de auditoria. | 1 | 10/10/2015 | 10/09/2015 | 3.1 |
| 4 | **Planificación** | **6** | **08/09/2015** | **14/09/2015** | |
| 4.1 | Reunión equipo de trabajo de la auditoria | 6 | 08/09/2015 | 14/09/2015 | |
| 4.2 | Redacción cronograma auditoria | 3 | 08/09/2015 | 10/09/2015 | |
| 4.3 | Documentación de las pruebas | 2 | 10/09/2015 | 11/09/2015 | |
| 4.4 | Entrega de cronograma y documentación | 1 | 14/09/2015 | 14/09/2015 | 4.3 |
| 5 | **Pruebas** | **39** | **14/09/2015** | **04/11/2015** | |
| 5.1 | Recogida de información en la organización | 3 | 14/09/2015 | 16/09/2015 | |
| 5.1.1 | Entorno interno y regulación | 3 | 14/09/2015 | 16/09/2015 | |
| 5.1.2 | Estudio de la información recogida. | 1 | 16/09/2015 | 16/09/2014 | |
| 5.2 | Ejecución de las pruebas | 30 | 17/09/2015 | 28/10/2015 | |
| 5.2.1 | Revisión de actas, acuerdos y guia del SGSI | 2 | 17/09/2015 | 18/09/2015 | |
| 5.2.2 | Revisión informes de riesgo y Politicas | 3 | 21/09/2015 | 23/09/2015 | |
| 5.2.3 | Revisión de controles Norma ISO/IEC 27001 | 5 | 21/09/2015 | 25/09/2015 | |
| 5.2.4 | Revisión controles técnicas y casos de uso | 2 | 28/09/2015 | 29/09/2015 | |
| 5.2.5 | Ejecución técnica de todas las pruebas | 25 | 21/09/2015 | 23/10/2015 | |
| 5.2.6 | Entrega de los informes preliminares. | 3 | 26/10/2015 | 28/10/2015 | 5.2.5 |
| 5.3 | Análisis de la documentación | 12 | 22/10/2015 | 04/11/2015 | |
| 5.3.1 | Revisión de documentación | 2 | 29/10/2015 | 30/10/2015 | 5.2.6 |
| 5.3.2 | Ejecución de entrevistas y visitas | 7 | 22/10/2015 | 30/10/2014 | |
| 5.3.3 | Pruevas técnicas de analisias de vulnerabilidades | 4 | 29/10/2015 | 03/11/2015 | 5.2.6 |
| 5.3.4 | Reunión de seguimiento de la auditoria | 1 | 04/11/2015 | 04/11/2015 | 5.3.3 |
| 6 | **Elavoración de Informes** | **5** | **05/11/2015** | **11/11/2015** | 5.3.4 |
| 7 | **Presentación de Informes** | **1** | **12/11/2015** | **12/11/2015** | 6 |
| 8 | **Cierre de la Auditoria** | **3** | **13/11/2015** | **17/11/2015** | |
| 8.1 | Realización del informe de cierre. | 2 | 13/11/2015 | 16/11/2015 | 7 |
| 8.2 | Realización del cronograma de revision anual | 1 | 17/11/2015 | 17/11/2015 | 8.1 |



**ANEXO III**

**GESTIÓN DE INDICADORES.**

| | |
|---|---|
| **Organización** | |
| **Documento** | **Gestión de Indicadores** |
| **Fecha documento** | **26 Marzo 2015** |

**Contenido.**

1. Introducción.
2. Tabla de Indicadores.

## 1. Introducción.

Para que el sistema se encuentre entre los márgenes deseables, es preciso que se pueda evaluar la eficiencia del mismo de forma constante, estableciéndose una serie de indicadores con los que se pueda cuantificar el correcto funcionamiento de las medidas de seguridad planificadas, su eficiencia y actualizaciones de estas necesarias.

Para cada indicador se establecen una serie de identificadores con que calificarle, tales como el nombre del indicador, la descripción del mismo, cuál es el valor correcto y cuál es el valor por debajo del que hay que levantar una alarma y en quién recae la responsabilidad de medir el indicador.

## 2. Tabla de Indicadores.

| Nombre del Indicador | Medida del número de revisiones de la Política de Seguridad por parte de la dirección. |
|---|---|
| Descripción | Número de revisiones realizadas |
| Frecuencia | 2 veces por año |
| Valor objetivo | 2 |
| Valor limite | 1 |
| Responsable de la medida | Responsable de seguridad |

| Nombre del Indicador | Identificación y actualización de activos |
|---|---|
| Descripción | Identificación y clasificación de nuevos activos a fin de establecer los mecanismos de protección mas adecuados |
| Frecuencia | 1 vez al año |
| Valor objetivo | 2 |
| Valor limite | 1 |
| Responsable de la medida | Responsable de seguridad |

| Nombre del Indicador | Medida de verificación realizadas para proteger la información contra violaciones de seguridad |
|---|---|
| Descripción | Número de actuaciones en verificar los controles para protección contra accesos no deseados. |
| Frecuencia | 1 vez al año |
| Valor objetivo | 1 |
| Valor limite | 1 |
| Responsable de la medida | Responsable de seguridad |

| Nombre del Indicador | Medida de incidentes en seguridad informática |
|---|---|
| Descripción | Número de incidentes en seguridad de las TIC |
| Frecuencia | Bimestral |
| Valor objetivo | 0 |
| Valor limite | 2 |
| Responsable de la medida | Responsable de seguridad |

| Nombre del Indicador | Medida de fallos en seguridad en puestos de usuario |
|---|---|
| Descripción | Número de incidentes en los equipos informáticos de usuario relativos a fallos de seguridad (virus/datos) |
| Frecuencia | Mensual |
| Valor objetivo | 0 |
| Valor limite | 2 |
| Responsable de la medida | Responsable de seguridad |

| Nombre del Indicador | Medida del número de auditorías. |
|---|---|
| Descripción | Número de auditorías internas realizadas y externas si estuviera programado. |
| Formula de calculo | Número de auditorías realizadas |
| Frecuencia | 1 vez al año |
| Valor objetivo | 1 |
| Valor limite | 1 |
| Responsable de la medida | Responsable de seguridad |

| Nombre del Indicador | Medida de software no autorizado detectado en los equipos de la empresa. |
|---|---|
| Descripción | Número de programas detectado en los PCs de la organización |
| Formula de calculo | % de programas localizados del total de PCs en planta |
| Frecuencia | Trimestral |
| Valor objetivo | Menor al 20% |
| Valor limite | 25% |
| Responsable de la medida | Responsable de seguridad |

| Nombre del Indicador | Medida de programas maliciosos detectados en los equipos y servidores |
|---|---|
| Descripción | Número de programas maliciosos detectados en los equipos |
| Formula de calculo | % de programas localizados del total de PCs en planta |
| Frecuencia | Trimestral |
| Valor objetivo | Menor al 20% |
| Valor limite | 25% |
| Responsable de la medida | Responsable de seguridad |

| Nombre del Indicador | Medida Accesos no autorizados a la red de la organización |
|---|---|
| Descripción | Número de Accesos no autorizados a la red de la organización |
| Formula de calculo | % de accesos no autorizados del total de accesos realizados |
| Frecuencia | Mensual |
| Valor objetivo | 10% |
| Valor limite | 25 % |
| Responsable de la medida | Responsable de seguridad |

| Nombre del Indicador | Medida de incidentes respecto a los acuerdos confidenciabilidad |
|---|---|
| Descripción | Número de incidentes por falta de confidenciabilidad |
| Frecuencia | Semestral |
| Valor objetivo | 0 |
| Valor limite | 2 |
| Responsable de la medida | Responsable Recursos Humanos |

| Nombre del Indicador | Medida de incumplimientos nomas acceso a internet en la empresa |
|---|---|
| Descripción | Número de violaciones en las normas de acceso a Internet |
| Formula de calculo | % de accesos no autorizados o incumpliendo las normas sobre el total de los accesos (sesiones) a Internet |
| Frecuencia | Mensual |
| Valor objetivo | 10% |
| Valor limite | 20% |
| Responsable de la medida | Responsable de seguridad |

| Nombre del Indicador | Medida de incumplimientos nomas correo electrónico corporativo |
|---|---|
| Descripción | Número de violaciones en las normas de uso del correo de la empresa |
| Formula de calculo | % de incumpliendo de las normas sobre el total de los usuarios de correo |
| Frecuencia | Mensual |
| Valor objetivo | 10% |
| Valor limite | 20% |
| Responsable de la medida | Responsable de seguridad |

| Nombre del Indicador | Medida de incumplimiento del uso de redes Wiffi |
|---|---|
| Descripción | Incumplimiento de las normas de accesos a redes inalámbricas tanto de la organización como externas |
| Formula de calculo | % de incumpliendo de la norma sobre el total de los accesos |
| Frecuencia | Mensual |
| Valor objetivo | 20% |
| Valor limite | 30% |
| Responsable de la medida | Responsable de seguridad |

| Nombre del Indicador | Medida de violaciones de los accesos físicos dentro de la empresa a zonas no autorizadas |
|---|---|
| Descripción | Intentos de acceso o incumplimiento de acceso a zonas de seguridad restringidas o fuera de horario autorizado |
| Formula de calculo | % de incumpliendo de la norma sobre el total de los accesos |
| Frecuencia | Trimestral |
| Valor objetivo | 5% |
| Valor limite | 10% |
| Responsable de la medida | Responsable de seguridad |

| Nombre del Indicador | Medida de dispositivos sin software antivirus y software mailiciso |
|---|---|
| Descripción | Número de equipos sin el software de seguridad instalado |
| Formula de calculo | % equipos son software de protección sobre el total de equipos |
| Frecuencia | Semestral |
| Valor objetivo | 5% |
| Valor limite | 15% |
| Responsable de la medida | Responsable de seguridad |

**ANEXO VI**

**REVISIÓN POR LA DIRECCIÓN.**

| | |
|---|---|
| **Organización** | |
| **Documento** | **Informe de revisión por la Dirección.** |
| **Fecha documento** | **26 Marzo 2015** |

| **FORMATO ACTA DE REUNION**<br><br>Informe de revisión por la Dirección | |
|---|---|

| OBJETO: Realizar la Revisión por la Dirección del sistema de mejora continua del Sistema de Gestión de la Información de la empresa.<br><br>LUGAR:<br><br>FECHA: | PARTICIPANTES: |
|---|---|

**TEMAS A TRATAR:**

1. Revisión de la Política de seguridad y objetivos de calidad.
2. Revisión de los indicadores de nivel de eficacia establecidos.
3. Revisión Resultados de auditorías internas.
4. Revisión de Acciones correctivas y preventivas.
5. Revisión de Acciones de seguimiento de revisiones previas.
6. Revisión de Cambios que puedan afectar el sistema
7. Recomendaciones para la mejora.

**DESARRROLLO:**

El día de fue enviado a través del correo electrónico la programación para la revisión por la dirección a todos los responsables líderes de proceso:

| Proceso | Desarrollado por: | Lugar y Hora | Responsable |
|---|---|---|---|
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |

| **FORMATO ACTA DE REUNION**<br><br>Informe de revisión por la Dirección | |
|---|---|

| | |
|---|---|
| **1.** Revisión de Política y Objetivos de Calidad. | |
| Política y objetivos de calidad | La política de calidad es establecida directamente desde la … |
| **2.** Revisión de los indicadores de nivel de eficacia establecidos. | |
| Revisión de los indicadores de nivel de eficacia establecidos | |
| **3.** Revisión de Resultados de Auditorías Internas. | |
| Revisión Resultados de auditorías internas | |
| **4.** Revisión de Acciones Correctivas y preventivas. | |
| Revisión de Acciones correctivas y preventivas | |
| **5.** Revisión de Acciones de seguimiento de revisiones previas. | |
| Revisión de Acciones de seguimiento de revisiones previas. | |
| **6.** Revisión de Cambios que puedan afectar el sistema. | |
| Revisión de Cambios que puedan afectar el sistema. | |
| **7.** Recomendaciones para la mejora. | |
| Recomendaciones para la mejora | |

**FORMATO ACTA DE REUNION**

Informe de revisión por la Dirección

**CONCLUSIONES GENERALES**

Podemos concluir que ...

**PLAN DE ACCIÓN**

*Para: mejoras en el sistema – mejoras en los procesos – Recursos destinados para la actividad.*

| ACTIVIDAD (MEJORA) | RESPONSABLE | FECHA EJECUCION | RECURSOS DESTINADOS |
|---|---|---|---|
| | | | |
| | | | |
| | | | |

Para constancia se firma por los que en ella intervinieron

_____ _____

Nombre Nombre
Cargo: Cargo:

_____ _____

Nombre Nombre
Cargo: Cargo:

_____ _____

Nombre Nombre
Cargo: Cargo:

**ANEXO VI**

**AUDITORÍA DEL CUMPLIMIENTO.**

| | |
|---|---|
| **Organización** | |
| **Documento** | **Informe de auditoría (1ª auditoria de seguimiento)** |
| **Fecha documento** | **10 Junio 2015** |

**INFORME DE AUDITORIA**
Nº Expediente: XXX-0001-ISO/IEC 27001:2013
Fecha de realización: 05-06-2015 / 10-06-2015

| **Información General** | | |
|---|---|---|
| *Organización* | Centro Especial Empleo XXXX | |
| *Localización* | Avda. Madrid, 104 45005 Toledo | |
| *Representante empresarial* | *Nombre* | |
| | *Cargo* | |
| | *Teléfono Contacto* | |
| *Tipo de Auditoria:* | Auditoria de complimiento (1ª) | |

| **Planificación de la Auditoría** | | | |
|---|---|---|---|
| *Fecha de inicio* | 05/06/2015 | *Fecha fin* | 10/06/2015 |
| *Auditor Jefe* | Juan González Martínez | | |
| *Auditor* | Juan González Martínez | | |
| *Técnico experto* | N/C | | |
| *Objetivo de la auditoria* | | | |
| Determinación de la conformidad de los sistemas de gestión de la organización auditada, siguiendo los criterios fijados por la certificación UNE-ISO/IEC 27001:2013, a fin de evaluar la capacidad de esta del cumplimiento de los requisitos técnicos, legales, reglamentarios y de seguridad aplicables, así como identificar las posibles aéreas de mejora en la organización. | | | |

**Resumen ejecutivo:**

Se ha realizado auditoria de cumplimiento sobre la norma ISO/IEC 27001:2013, en sus 114 controles o medidas preventivas sobre las buenas prácticas para la Gestión de la Seguridad de la Información; primera de las auditorias de seguimiento planteadas sobre lo sistemas de gestión de la organización.

Para evaluar la madurez de la seguridad de la organización, se han analizado los siguientes dominios de la ISO/IEC 27002: 2013:

- Política de seguridad
- Organización de la seguridad de la información
- Gestión de activos
- Seguridad a los recursos humanos
- Seguridad física y ambiental
- Gestión de comunicaciones y operaciones
- Control de acceso
- Adquisición, desarrollo y mantenimiento de Sistemas de Información
- Gestión de incidentes
- Gestión de continuidad de negocio
- Cumplimiento

Durante el estudio se realizó la revisión de los 114 controles planteados por la norma a cumplir, con los diferentes objetivos de control, siguiendo la tabla indicada en la memoria basada en el Modelo de Madurez de la Capacidad (CMM), Evaluándose el cumplimiento de los diferentes sub-apartados a raíz de los cuales se realizará el cálculo de nivel de cumplimiento del objeto a estudio, bloque a bloque, según la descripción de los controles que se expone en el proyecto y cuya verificación también se muestra en su tabla de cumplimiento.

De forma general, podemos indicar, que el Sistema de Gestión de Seguridad de la Información se encuentra correctamente implantado, es coherente con la Política y Objetivos de Seguridad, se adapta a la situación actual de la organización y permite la identificación de oportunidades de mejora, concluyéndose que el Sistema responde de forma satisfactoria a los requisitos de certificación.

Se verifica la existencia de un plan anual de auditorías internas en el que se recogen tanto auditorías a los procesos del sistema como auditorías a los controles. Una vez revisados programa y sistemas de información se presenta un informe de las no conformidades y se indican las acciones correctivas asociadas.

Ejecutados los proyectos detallados en la memoria del proyecto, se ha observado en esta auditoría cambios significativos con respecto al análisis de riesgos realizado a la organización:

- Se ha desarrollado e implantado un plan director de políticas de seguridad, verificado por la dirección, nombrándose un responsables de seguridad e inculcando el modelo en el tejido organizativo.
- Se ha realizado una correcta identificación y definición de todos los activos empresariales, identificando responsables, propietarios y usuarios, dando así seguridad a su acceso y modificación.
- Se ha procedido a clasificar la información que maneja la organización atendiendo a su valor, seguridad y requisitos legales.
- Se han implementado mejoras en el acceso a zonas seguras y restringidas, especialmente donde se encuentran los sistemas de gestión, con controles técnicos y físicos de entrada tanto al CPD como a dependencias susceptibles de tener información sensible.
- Se han implantado y desarrollado las acciones formativas iniciales para la adecuación del personal de la organización al uso de los sistemas de información y a la misma información en sí, con los requisitos que se establecen en el propio plan de seguridad establecido. Igualmente, están planteadas las actualizaciones de formación en eta materia para las novedades o vacios que puedan ir surgiendo.
- Se ha reestructurado todo el acceso a la información y los controles oportunos, para adaptar la organización a la LODP y normas UNE en las que la organización se ve afectada, poniendo en valor la modificación de las normas internas, tan pronto exista alguna normativa que hubiera que aplicar.

**Nivel de implementación basado en CMM:**

La siguiente tabla muestra el nivel de implementación de los controles.

| | | Nivel de cumplimiento |
|---|---|---|
| 5. | Polîtica de Seguridad | 50% |
| 6. | Organización de la Seguridad de Información | 13% |
| 7. | Seguridad de Recursos Humanos | 52% |
| 8. | Gestión de Activos | 62% |
| 9. | Control de Acceso | 79% |
| 11. | Seguridad fisica y ambiental | 76% |
| 12. | Operaciones de Seguridad | 76% |
| 13. | Seguridad de las comunicaciones | 73% |
| 14. | Sistema de adquisición, desarrollo y mantenimiento | 77% |
| 15. | Cumplimiento | 37% |
| 16. | Información de gestión de incidentes de seguridad | 76% |
| 17. | Aspectos de seguridad de información de la gestión de | 83% |
| 18. | Conformidad | 90% |

Podemos observar que todos los controles excepto el de la organización de la seguridad de la información, están por encima del 50%, con muy buenos resultados en los dos últimos dominios, los cuales, se evidencia un trabajo importante.

Teniendo en cuenta la situación de partida con respecto a la actual (CMM), tras aplicación de los proyectos indicados, podemos observar de una forma positiva como ha mejorado la implementación de los controles de la norma, teniendo en cuenta muchas acciones de mejora de desarrollar.

Es importante trabajar sobre las no conformidades que se reconocen y las acciones de mejora planteables.

**Cuadro de NO CONFORMIDADES observadas:**

| Ref. | Descripción de la NO CONFORMIDAD | Apartado ISO | Categoria |
|---|---|---|---|
| NC-01 | A pesar de tener implementado un plan director de seguridad, este esta definido de forma bastrante general en el nucleo de la organización, faltando detalles concretos que delimiten las actuaciónes inadecuadas. | 5 | Observación |
| NC-02 | Falta definir un reglamento de regimen interior, donde se detallen las responsabilidades personales de la reguridad de la información, codigo de onductas y en especial un regimen disciplinario detallado para el personal. | 6-7 | Menor |
| NC-03 | A pesar de implementarse la identificación y definición de todos los activos empresariales, se observa la falta de una correcta guia de identificación disponible para todos los miembros de la empresa, donde conste el modelo de etiquitado de seguridad que se establece. | 8 | Menor |

| | | | |
|---|---|---|---|
| NC-04 | Se observa una brecha de seguridad en el intercambio de información (sensible o no) existente entre los servicios de gestión en la sede principal y el tayer/almacen, donde la información viaja en memoprias USB trasnportadas por el personal; esto carece de seguridad ante perdida, destrucción o uso por personas no autorizadas. | 9 | Mayor |
| NC-05 | El uso de información confidencial, o activos sensibles, no esta encriptado o con verificación de autentificación; los accesos a los archivos de los servidores, se realizan mediante la identificación en el LDAP de la organicación, medida de seguridad medio-baja si no se suplementa con algun tivo de verificación alternativa. | 9 | Menor |
| NC-6 | El sistema de mensajeria electronica no es propio de la organización, estando alojado el servidor de correo en servidores ajenos a esta; igualmente no existe dominio propietario para salvaguardar el correo, dependiendo de los servicios de otra entidad, a quien se confia la información sensible que se envie por esta via | 13 | Menor |

Para todas las NC de la tabla anterior, será necesario que la Organización establezca y documente las acciones correctivas pertinentes.

**Observaciones finales:**

Se solicita a la dirección de la Organización, el calendario con las fechas para la realización de la próxima auditoría.

Una vez tenidas en cuenta las no conformidades que se indican, si la dirección precisa la presentación del Plan de Acciones Correctivas, esta enviarlo al departamento de auditorías en 30 días naturales a partir de la fecha de emisión del informe de auditoría.

En Toledo, a 25 de junio de 2.014

El Representante de la Organización

El Equipo Auditor