POSGRASDO EN GESTIÓN Y AUDITORÍA DE LA SEGURIDAD

Nombre Estudiante: Marina Marrugat Soler

Programa: Proyecto Final de Posgrado en Seguridad en servicios y aplicaciones

Nombre Consultor: Arsenio Tortajada

Centro: <UOC>

Data Entrega: 7 de junio de 2017

FICHA DEL TRABAJO FINAL

Título del trabajo:	*Elaboración de un plan de seguridad de la información*
Nombre del autor:	*Marina Marrugat Soler*
Nombre del consultor:	**Arsenio Tortajada**
Fecha de presentacióno (mm/aaaa):	*07/06/2017*
Área del Trabajo Final:	
Titulación:	Proyecto Final de Posgrado en Seguridad en servicios y aplicaciones

Resumen del Trabajo (máximo 250 palabras):

El proyecto realizado forma parte de la evaluación final del postgrado en gestión y auditoria de la seguridad. Se ha realizado un plan de seguridad director, en el cual se toma de base una empresa con el fin de realizar mejora en la aplicación de la norma de la seguridad de la información. Se marcan unos objetivos, para poder responder al final del trabajo. Para la elaboración, se realizó en una primera entrega un resumen detallado, de las características de la empresa; además de una comparación de las normas ISO 27001 y 27002 indicando el nivel de cumplimiento donde, se determina el alcance del PSD (Plan de seguridad Director). Una segunda entrega, donde se presenta un esquema documental con todos los documentos que tiene la empresa, con las especificaciones necesarias. Una tercera entrega consistió, en el análisis de riesgos. Con la enumeración de los activos y su valoración mediante la metodología MARGERIT. Se recopilan los resultados en una tabla con los aspectos más críticos de cada activo. Además de define el nivel aceptable para la empresa. Se realiza, después, una propuesta de proyectos, donde se planificación en el tiempo, y se especifican los costes económicos, para mitigar el riesgo de la organización. Una quinta entrega, donde se realiza una auditoría de cumplimiento: con la ayuda del CMM (modelo de madurez de la capacidad). Los análisis se presentan con diagramas para la mejor lectura. Se finaliza con las principales conclusiones, y la respuesta a los objetivos planteados al principio del trabajo.

Abstract (in English, 250 words or less):

The present project is part of the postgraduate named "*en gestión y auditoria de la seguridad*". A master security plan has been done, in which a company is taken as a base in order to improve the application of the information security standard, always according to the standard ISO 27002. We set some goals, that we will try to answer at the end of the project. For the first delivery, we had to give a very concrete description of the organization we chose; with a comparison of the ISO 27001 and ISO 27002, so we could identify its lack of application, as well as the aim of the PSD was determined. Secondly, we presented a summary of the several documents that a company should have. On the third delivery, a risk analysis was made. We made a list of the assets and its value according to MARGERIT. The most important results, are exposed on a chart; and we define the acceptable risk for the organization. Then a proposal of projects is made: Where we had to elaborate a schedule of the procedure. Each one, must have its budget as well as the different people involved. One last delivery is made, with the Capability Maturity Model (CMM), where we present a compliance auditory. The results, once again are in a chart, to ease the reading. We finish with the conclusions and the answer to the goals set at the beginning.

Palabras clave (entre 4 y 8):

Seguridad informática, auditoria, PSD (Plan de Seguridad Director), ISO 27002, análisis, riesgos, amenazas.

Índice

I. Contextualización y objetivos de la empresa 5
B. Descripción de la empresa 5
C. Objetivos 9
D. Enfoque y método seguido 9
E. Planificación del Trabajo 10
II. Alcance y análisis diferencial (fase 1) 11
F. Alcance del PSD (Plan de Seguridad director) 11
G. Valoración inicial 12
III. Esquema documental (fase 2) 17
A. Política de Seguridad 17
B. Procedimiento de auditorías internas 17
H. Gestión de indicadores 18
I. Procedimiento de revisión por la dirección 18
J. Gestión de Roles y Responsabilidades 18
K. Metodología de análisis de riesgos 18
IV. Análisis de riesgos (fase 3) 18
V. Propuestas de proyectos (fase 4) 25
VII. Conclusiones y objetivos 39
VIII. Bibliografia 40
IX. Anexos 40
L. Anexo 1 40
M. Anexo 2 43
N. Anexo 5 53

I. Contextualización y objetivos de la empresa

B. Descripción de la empresa

Las características de la compañía son las siguientes:

1. Se trata de una multinacional que se dedica a distintos sectores. El que nos interesa es el económico. En nuestro caso se trata de una empresa contractada por una entidad bancaria, que le ha encargado la gestión de la morosidad de su empresa.
2. La empresa en cuestión, se ubica en Barcelona.
3. Tiene unos 1000 empleados en esta ubicación. Solo se contemplan los que trabajan directamente en esta empresa, sin tener en cuenta el soporte externo.
4. Se le domina "*cliente*" a la empresa que lo ha contratado.
5. La empresa es española, por tanto, se encarga de la morosidad a nivel nacional.
6. Se gestiona en las siguientes comunidades autónomas (el resto de CCAA son gestionadas por otra gestoría):
    a. Cataluña
    b. Murcia
    c. Andalucía
    d. Extremadura
    e. Navarra
    f. País vasco
7. En los últimos años sus ganancias son positivas, pero han disminuido en comparación con los años anteriores.
8. El espacio físico es el siguiente: está formado por dos edificios. Ambos conectados por unas escaleras, que solo puede acceder un determinado personal, mediante lectura de una tarjeta. Se separa en dos las instalaciones de tal manera que una se encarga de la logística y la otra de la morosidad, dividida en los

departamentos que son convenientes. Es decir, uno envía la documentación que debe llegar a su destina, la organizan. Se encargan de proporcionar material, de la misma manera que hacen llegar los paquetes y correspondencia que pertenece a cada departamento. En el otro edifico, organizan las demandas, se gestiona la documentación necesaria para la preparación de estas. También se encargan de hacer el seguimiento de estas demandas, y atender cualquier consulta que tengan las oficinas de la entidad bancaria. Además, de encargarse de contactar con los clientes si se da el caso, también se realiza *factoring a* nivel de los letrados y todos aquellos involucrados en la presentación de las demandas.

9. Más adelante se explica el alcance del SGSI, y esta descripción tendrá más sentido. El departamento en que enfocamos el plan director, utiliza 3 aplicativos. El acceso a dos de ellos es a través de motores de búsqueda, como *internet explorer* o google Chrome. El tercero, es un programa interno que necesita ser descargado en el ordenador, del cual no se introducirá en el plan director. Los dos aplicativos usados, se utilizan para llevar a cabo la preparación de la demanda. Ése, contiene las herramientas necesarias para recopilar los datos informativos de cada cliente que se encuentra en el programa de morosidad. Más adelante, en la descripción de los activos se definirá la función más detalladamente. Estos aplicativos fueron ideados por el gerente de la empresa para el uso exclusivo de la empresa. Hay que destacar que estos aplicativos son usados exclusivamente por el departamento que se elabora el SGSI.
10. La seguridad de los documentos que se usan es un documento de seguridad firmado por los empleados de confidencialidad, junto con el contrato. El acceso a cada aplicativo es con un usuario formado por dos letras y 7 números. Estos identifican, a los empleados con su nombre completo, este usuario se usa para la

entrada al pc y a los distintos aplicativos, además de los programas que puedan ser de utilidad. Este usuario, es generado por informáticos, ya que los empleados no tienen acceso a los ordenadores como administradores, ni pueden crear usuarios ni ampliar o disminuir los permisos. Cualquier modificación que se quiera hacer, o error, debe ser gestionado y arreglado por una empresa distinta que se dedica exclusivamente a estas gestiones. La creación de tales usuarios, es tardía y genera que un mismo usuario sea usado por distintas personas, sin dar pie a la identificación de cada una. Es por ello, y mucho más que un plan director debe ser elaborado.

11. El organigrama del departamento de seguridad es el siguiente:

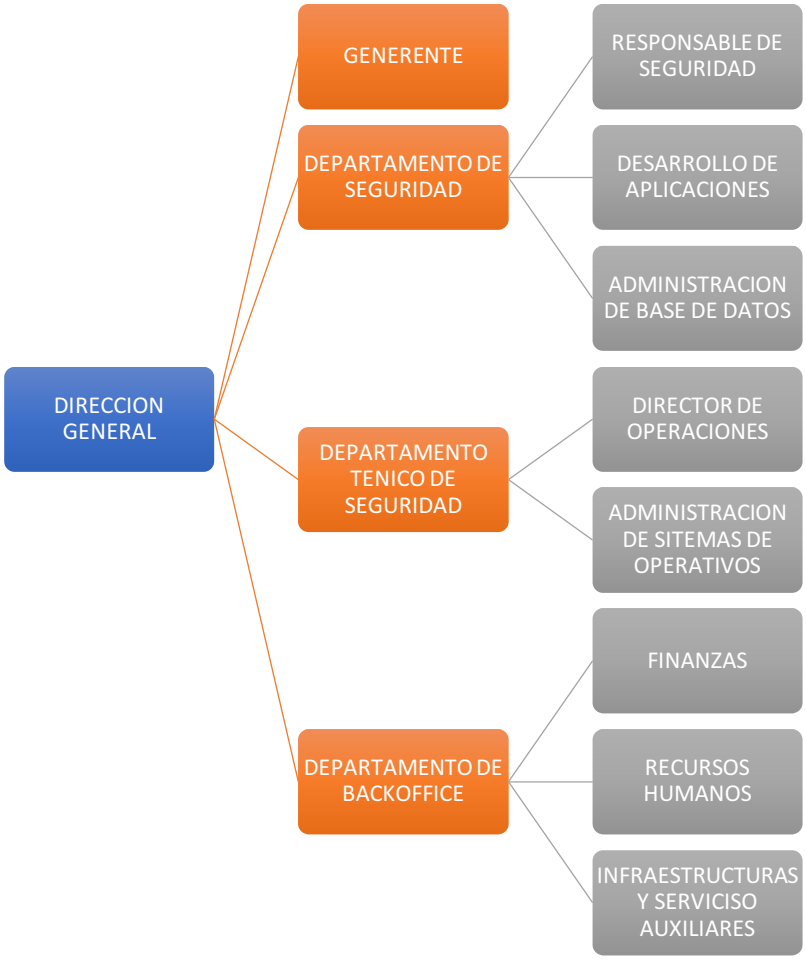


Ilustración 1: diagrma representactivo de direccion de la empresa.

Especificación de los Responsables de la gestión de los activos

a. Responsable de seguridad

Existen dos equipos de responsables. El primero es un departamento entero que se ubica en la misma planta que *Hallo* se ubica, solo que apartado para cuando se les requiere. Normalmente, siempre acude una misma persona física y por ello, ésa responde por todos. Es la que se encarga de solucionar los errores que pueden surgir a lo largo de la actividad diaria. Es decir, los aparatos como los ordenadores, impresoras. También realiza las tareas que requieran de algún conocimiento más informático, como la perdida de conexión de internet o conectar algún cable que no esté bien conectado. El segundo se trata de la plataforma que distribuye los ordenadores. Este también es un equipo formado por varias personas que actúan por igual, y tienen una estructura jerárquica. Donde Hallo solo se comunica con los que están a la atención de los empleados. Estos están administrados, como se ha dicho con anterioridad por una misma empresa llamada *Suave.* Esta tiene todos los permisos para realizar cualquier acción relacionada con los ordenadores y sus conexiones.

b. Responsable de información

Existe un sub-departamento dentro del de seguridad, muy reducido, pues al existir varios departamentos, cada departamento se encarga de su propia gestión en cuanto a la información que manejan. Del que nos ocupa, el que prepara las demandas, tiene un archivo físico dividido en armarios donde se almacena toda la información que se gestiona. Esta información también existe en formato electrónico, pues se escanea toda la información que se recibe y se archiva posteriormente en los armarios. Se encarga pues, de tener en mente toda la actividad que lleva a cabo al empres crédito ya y hallo. Una depende de a otra, y deben rendirse cuenta, es aquí donde el responsable de la información juega su papel.

c. Responsable de ámbito legal

Esta figura está encabezada por una sola persona, pues se centra en el departamento propio que nos ocupa. Esta esté especializada en derecho y tiene suficiente conocimiento de las normas y leyes que amparan aquellas clausulas relacionadas con los préstamos en general. Su función es aconsejar sobre las acciones que se llevan a cabo durante la tramitación de una demanda, además de los problemas que puedan surgir de temas legales.

C. Objetivos

- Mejorar la seguridad de la página web
- Adecuar los controles de acceso físico
- Hacer un control de usuarios
- Identificar las correcciones que sean convenientes para la seguridad de los documentos tratados
- Exponer el cumplimiento de las normas
- Demostrar a los clientes confianza
- Evaluar las posibles amenazas y sus soluciones (exhaustivamente)
- Describir las políticas de seguridad de la empresa

D. Enfoque y método seguido

Se trata de, en base al ISO/EIC 27001 y 27002, valorar si la empresa cumple con los requisitos. En el caso de no cumplirse, se realizarán observaciones para poder llegar a implementar aquellas partes en que la empresa no cumpla con los criterios de seguridad.

El trabajo se dividirá en las fases que comportan un plan de seguridad. Es decir, habrá tantos capítulos como fases tenga un plan.

Las dimensiones y su valoración criítica, se ha realizado únicamente para 3 parámetros: integridad, disponibilidad y confidencialidad. En el cuadro establecido aparecen como C, D, I.

E. Planificación del Trabajo

El proyecto se realiza mediante 6 entregas programas a lo largo del semestre. Cada una de ellas, pide unas tareas explícitas.

Se realiza una primera entrega en que se hace la presentación de la empresa con detalle. Además, se presentan los objetivos del plan, junto con la metodología que se sigue usa para la realización del plan. Así mismo, se realiza un análisis diferencial de las normas que sirven como estándares para la seguridad de la información.

La segunda entrega consiste en detallar los distintos documentos que toda empresa debe tener. Se hace la redacción de estos, indicando los roles y responsabilidades de quienes deben realizar y ejecutar el documento; además de indicar con que control de la norma se hace referencia para su aplicación.

La tercera entrega, consiste en el análisis de los riesgos. Este se realiza con el CMM y el MARGERIT (se desarrollan dentro de la fase en concreto). Se trata de valorar que activos son más susceptibles de padecer una amenaza. Se realiza identificando el nivel integridad la disponibilidad y la confidencialidad del que cada activo goza. Se elabora un cuadro exhaustivo, para su comprensión que se encuentran en los anexos, junto con unas tablas resumen.

Una cuarta entrega es realizada, donde se especifican los proyectos que debe realizar la empresa para la mejoría de la aplicación de la norma, a partir del análisis de riesgos realizado en la entrega anterior.

En quinto, y último lugar, se realiza el análisis de cumplimiento. Esto, se realiza mediante el CMM, y los controles aplicables de la norma ISO 27002. Para su

identificación, se realiza un cuadro donde se especifica el nivel de madurez que tiene cada control y lo que debería realizar la empresa en cada uno de ellos. La ilustración de lo comentado, se puede lograr mediante un gráfico en radar, donde se acentúan los puntos fuertes y débiles de la aplicación de la norma.

II. Alcance y análisis diferencial (fase 1)

F. Alcance del PSD (Plan de Seguridad director)

En el apartado de introducción se ha definido en rasgos generales la actividad de la empresa. Se ha enfocado de modo a su descripción. Ahora procedemos a la explicación del alcance, donde se define con detalle el departamento al cual se refiere el plan de seguridad director que se elaborará.

En primer lugar, se trata de una empresa que está dividida en departamentos que gestionan diferentes acciones para llevar a cabo una misma actividad. Se trata del departamento de morosidad de una gestoría del banco llamado *Crédito Ya*. La empresa contratada se llama *Hallo*, la cual se ha denominado con anterioridad al "cliente".

El PSD, tiene como objetivo, aparte de los mencionados anteriormente, de los aplicativos y los accesos a estos que se usan para llevar a cabo la actividad de la empresa.

Los aplicativos mencionados, son 4. Más concretamente son identificamos como activos sin los que la empresa no puede realizar su finalidad. Cada uno sirve para realizar tareas únicas. El primero se llama IDD (Información de Deudores), donde se encuentra toda la información relacionada con los préstamos que puede tener un titular. Es decir: fecha de la constitución de un préstamo o de una hipoteca. Además, de los datos personales, como su DNI, y si son solventes, o no, para poder iniciar un procedimiento y reclamar la cantidad que deben. También encontramos aquella información útil para llevar a cabo la demanda final. Es decir, ubicar todos los documentos y poder localizarlos fácilmente. La finalidad del PSD, no es la finalidad de este aplicativo ni conocer si es

seguro o no, sino que es más bien su acceso y el acceso al edificio. Es por eso que no nos extenderemos a la explicación exhaustiva de todas las posibilidades que permite el aplicativo.

Este mismo aplicativo, tiene un método de archivador. El cual solo tiene acceso una persona. Esta persona se encarga de gestionar la documentación de cada contrato que hay en la oficina. Del mismo modo, su utilidad, no es parte de PSD, no nos extenderemos.

Existe otro aplicativo que es usado por las oficinas de *Crédito Ya* en sus sucursales de España. Se trata de un aplicativo que las oficinas utilizan para controlar si un contrato esta moros o no. Permite acceder a todo lo que tiene un cliente contratado con una oficina. Esto goza a cada usuario conocer la ciudad y la provincia que se contrató cualquier movimiento.

Del mismo modo, existe un cuarto y último aplicativo del cual hay la misma información que el primero, pero es aún más detallado. Permite la gestión más precisa de copias, de las escrituras o prestamos en el caso de que estén extraviados. Cuando las copias llegan a la oficina se deben recepcionar y cada usuario lo recibe, y lo puede tramitar para llevar a cabo la preparación de la demanda. Hay que destacar, que no se realiza la redacción de la demanda. Esta la realizan letrados, a los que se les remite la documentación que se prepara. Se encargan de hacer llegar a los procuradores las demandas redactas, adjuntando y numerando los documentos que la empresa les proporciona.

G. Valoración inicial

La diferenciación de la ISO, se realiza en base a los puntos que esta tiene. Se hará una breve explicación de lo que la organización cumple y de lo que no cumple, además de proponer alguna mejoría si es oportuno.

<u>Políticas de seguridad</u>

La empresa realiza distintos manuales para la realización de las demandas. Los que tramitan estas, deben seguirlos para una gestión adecuada de la información. Se deben tener en cuenta, pues pueden afectar a los deudores negativamente si no se aplican como viene en el manual. Aun así, teniendo los manuales, esto cambian muy a menudo. Es por eso que las normas y las directrices no son concretas y suelen durar una semana como mínimo hasta que se vuelven a cambiar. Es un aspecto, que debería cambiarse si se quiere certificar. Esto suele suceder cuando, desde asesoría jurídica, aparecen nuevas leyes que obligan a cambiar los procedimientos establecidos, en estos momentos hablamos de las clausulas suelo y el vencimiento hipotecado, que ambas afectan las hipotecas de los considerados consumidores.

Aspectos organizativos de la seguridad de la información

La organización está divida en departamentos, que son proyectos. Cada uno de ellos tiene un responsable que es el portavoz y el que coordina el grupo. El responsable hace un balance del trabajo realizado semanalmente. Cada responsable tiene asignada su responsabilidad y la conoce, por el cual fueron formados para poder realizarla.

Se trata de distintos proyectos, por lo que las tareas que se realizan se segregan en esos. Además de los responsables mencionados, existen gerentes que están por encima de ésos, de modo que supervisan que los primeros realicen sus tareas adecuadamente.

Cada departamento tiene sus propias políticas de la gestión de seguridad, puesto que se realizan distintas actividades.

Seguridad ligada a los recursos humanos

Los empleados que son contratados pasan una entrevista, no es muy exhaustiva, puesto que no hay muchos requisitos. Según el departamento, se piden más o menos experiencia. Se firman contratos de los cuales existen dos tipos: de empres o empresa de trabajo temporal (ETT). Si este segundo se alarga, se pude ser de empresa.

Los empleados no reciben formación específica de la importancia de la seguridad, ni del trabajo que realizan. Es muy probable pues, que la información que se trate no sea con el debido cuidado.

Gestión de activos

Existe un inventario de los activos, pero se es muy indulgente a la hora de cambiarlos o repararlos, e incluso de pedir nuevos activos. La empresa no pasa por un buen momento económico, e intenta reducir gastos.

La mayoría de activos son gestionados por otra empresa, que el cliente tiene para centralizar cualquier problema que los empleados tengan.

Los ordenadores, tienen usuario que no permite cambiar ninguna configuración del mismo. Es decir, no se puede obrar como administrador, se debe acudir a la misma plataforma mencionada anteriormente para solucionarlo.

Control de accesos y seguridad física y ambiental

El acceso al edifico es con una tarjeta magnética, que identifica al empleado con una foto acompañada del número de empleado, si se trata de empresa, o bien con el DNI, si se trata de ETT. Hay una banda magnética por la cual se debe pasar la tarjeta. Si un empleado se olvida la tarjeta, se debe acudir a recepción para pedir una provisional que debe ser devuelta al final del día, sino se desactiva y no se puede volver a utilizar. Las tarjetas pueden ser verdes, si es de ETT, y caducan cada dos meses, los responsables deben renovarlas periódicamente para que el empleado pueda entrar. Si es blanca, es de empresa y no necesita renovación.

El acceso al pc, es mediante usuario. Cada uno, goza de unos permisos de utilización y de acceso a los aplicativos. Según su función en el departamento, se tendrán los necesarios para realizar su actividad. El usuario es el mismo para el resto de aplicativos.

Un nuevo empleado usara el usuario de un compañero puesto que aún no se le ha dotado de su propio. Del mismo modo, que cuando un empleado se va de la organización sus usuarios aún siguen vigentes y se tarda meses en darlos de baja. La rapidez en la gestión de usuarios debería mejorarse.

Las contraseñas, se repiten entre empleados o son muy simples. Entre ellos, los empleados se prestan los usuarios lo que crea conflicto de seguridad.

Seguridad en la operativa

Este apartado no ha sido aplicado con exceso cuidado por parte dela empresa, por lo que no se hace un análisis.

Seguridad de las telecomunicaciones

No hay intercambio con información externa, por lo que no se contempla esta parte. El trato de la información es interno, pues se mueve de oficina a oficina, o hacia los letrados/procuradores. No se trata de ninguna empresa que tenga la misma actividad, sino de personas físicas contratadas. El cliente, es el mismo para la empresa que lleva el resto de España, que no ha sido mencionado en la parte introductoria.

La mensajería electrónica, es a través de un mail del cliente que es exclusivo para el uso de la actividad. No tiene una finalidad personal, ni para tratar con los empleados.

Adquisición, desarrollo y mantenimiento de los sistemas de información

Se realizan todos los requisitos que dice la norma, puesto que los procedimientos se hacen tal como se pide. Además, se realizan las pruebas que se requiere. También, se revisan las aplicaciones que se usan con periodicidad, para controlar que cumplen con la función.

Gestión de incidentes en la seguridad de la información

Un error tiene lugar, este tiene unos responsables que responde por el e intentar solucionarlo. Este error, debe ser comunicado, mediante una petición a un informático.

La petición se realiza vía mail, o vía telefónica. La respuesta a estos es inmediata en la mayoría de los casos, aunque la solución es lenta. Aun así, no se consigue solventar el incidente y se queda sin resolver. A consecuencia, no se aprende ni se mitiga.

Continuidad del negocio

Existe una planificación de la continuidad de la seguridad, pero esta no es mejorada, sino que es la misma que hay implementada. Aun así, se verifican y se revisan la seguridad de la información para intentar mejorarla.

Cumplimiento

El cuadro ilustrativo se encuentra en el apartado de anexos: anexo 5

A continuación, se presenta una tabla con algunos ejemplos más específicos:

Ilustracion 2: esquema general de los aspectos tratados en las normas y su aplicabilidad

ASPECTOS A EVALUAR	RESPUESTA
¿la organización ha definido un documento con la política de seguridad de la información?	Si, se ha redactado tal documento y toda la empresa que esta en relación ha firmado un contrato de confidencialidad.
¿La política de seguridad de la información se revisa periódicamente?	Se hace una revisión cada 2 meses.
¿Se han definido las responsabilidades en materia de seguridad de la información?	Si, estos están definidos y cada uno tiene sus responsabilidades establecidas.
¿Se han implantado perímetros de seguridad (paredes, puestos de recepción, entradas controladas por tarjeta) para proteger las áreas de acceso restringido?	Si: todas las entradas estan controladas por puestos de recepción y controles con tarjeta.
¿Se registran las actividades de los administradores y operadores de sistema?	No. Estos no se realizan con regularidad, aunque se hace un control de un usuario cada día.
¿Se registran las actividades de los administradores y operadores de sistema?	No. La contraseña cada uno escoge la que le es más cómoda para recordarla.

¿Los usuarios se aseguran de proteger los equipos desatendidos? (Ej. bloqueando o cerrando la sesión?	No: cada usuario actúa como más cómodo le es, a la hora de abandonar su puesto de trabajo.

III. Esquema documental (fase 2)

En la norma ISO, los documentos requeridos se dividen en dos partes: los que son requisitos obligatorios aquellos que la empresa debe cumplir, y aquellos que son complementarios y según la organización consideran si se aplican o no.

De acuerdo con lo anterior, se describen, a continuación, el listado de documentos que harán de base del SGSI de la empresa objeto de estudio. En los anexos se añaden los cuadros de los respectivos procesos.

A. Política de Seguridad

La Política de Seguridad de la Información del SGSI se ha desarrollado para garantizar la confidencialidad, integridad y disponibilidad de la información y de los de los procesos. Al implementar esta política las personas involucradas, tanto empleados como proveedores, deben garantizar la protección de los procesos, la reputación y la mejora continua.

B. Procedimiento de auditorías internas

Se elabora un registro de las auditorias que se llevarán a cabo en la organización cuando se haya obtenido la certificación. Se detalla todo aquello que sea necesario para los auditores internos. Además de un esquema básico de cómo deben estar presentados los resultados de las auditorias.

A tal resultado, se realizará 1 auditoria cada 3 meses. Cada una de ellas se centrará en un departamento. Aleatoriamente, pues hay dos departamentos que se auditan. La ultima auditoria a realizar, se realizará en un conjunto de las dos, de este modo se obtiene una auditoria más amplia y más concreta en cada departamento.

H. Gestión de indicadores

Se remite al cuadro realizado en la fase I.

I. Procedimiento de revisión por la dirección

Los objetivos que deben ser tratados en cada reunión, se realizaran cuando se haya determinado el resto del proyecto.

J. 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 Dirección.

El comité de seguridad, está compuesto por el director, los representantes de cada departamento que dé servicios de seguridad de la organización, un secretario, el responsable de seguridad de la organización. Si se considera oportuno podrán participar aquellas personas, que ostenten una posición que pueda ser útil según la auditoria que se vaya a realizar.

K. Metodología de análisis de riesgos

Se remite al cuadro que se ha realizado en el apartado anterior.

El detalle de cada uno de los documentos se encuentra en el documento adjuntado nominado “anexo 2: esquema documental”.

IV. Análisis de riesgos (fase 3)

El uso de la tecnología dentro de las organizaciones está en auge. Es por es que Margerit es una metodología perfecta para el análisis de riesgos de una organización. Tienen el objetivo de sistematizar el análisis, que pueden presentar los activos de la empresa. Hay

que minimizar los riesgos asociados, garantizando la integridad la disponibilidad y la confidencialidad de los mismos (Abril, Pulido y Bohada, 2014).

Se presentan, a continuación, el resultado de los aspectos críticos según Nivel de Riesgo Aceptable. Este, de previo acuerdo con la dirección, se han establecido los controles que deben ser aplicados: deben quedar entre medio o bajo. Tal como se refleja en el cuadro de la definición de la metodología de Análisis de Riesgos:

Impacto / Pérdidas

	Leves	Moderadas	Graves
Alta	**Medio**	**Alto**	**Alto**
Moderada	**Bajo**	**Medio**	**Alto**
Baja	**Bajo**	**Bajo**	**Medio**

Ilustración 3: cuadro de los análisis de riesgo según Margerit

Detalle del análisis de riesgos

Identificación de los activos

Se definirán los activos que existen y que se usan en la empresa, con el fin de poder llevar a cabo un correcto análisis de los mismos:

- Personal: toda aquella persona que se dedica a llevar a cabo acciones que tienen como resultado su trabajo.
- Aplicativos: 3 tipos de aplicativos, los cuales se acceden teniendo una conexión a internet, desde los cuales se tiene un control de la información de la goza la empresa.
- Unidades: es el instrumento con el cual se llevan a cabo las acciones.

- Impresoras: estas sirven para el resultado final y la recolección de la información.
- Muebles: son el apoyo para cualquier actividad, ya sea la mesa para disponer los ordenadores, ya sea las sillas para que el personal se pueda sentar.
- Archivo: se trata de un espacio de almacenaje de toda la documentación relativa a las personas que se están estudiando, los deudores, para reclamar la deuda.
- Conexión a internet: esta permite la realización de la actividad a través de los ordenadores.

Fuentes y características de las amenazas

Existe una clasificación de las amenazas, según donde provengan y las características que pueden afectar si se materializan.

Las características usadas en nuestro caso son las que se detallan a continuación:

- Disponibilidad: El acceso a la información no es posible.
- Confidencialidad: La información se revela a personas no autorizadas
- Integridad: La información es modificada o manipulada por personas o procesos no autorizados

Las fuentes que se utilizan son:

- Natural: Fenómenos naturales (ej: rayo, inundación, incendio).
- Humana: Actos malintencionados, incumplimientos de las normativas de seguridad, negligencias, o falta de controles adecuados.
- Entorno: Averías o defectos en dispositivos, redes o software

Identificación de los activos

En el presente análisis de riesgo se han identificado 32 activos de la empresa clasificados en seis tipos correspondientes a los subtipos.

- Físicos: activos de hardware

    - Equipos de personal
    - Equipos de comunicación
    - Servidores
- Lógicos:
    - Software de desarrollo
    - Documentación y datos
- Personal
    - Directivos y responsables
    - Personal
    - Personal externo
- Entorno e infraestructura
    - Seguridad física
    - Suministros
    - Comunicaciones

<u>Valoración de los riesgos (impacto y perdidas)</u>

Para valorar los riesgos se han establecidos unas escalas, para al probabilidad/frecuencia y la evaluación de impacto/perdidas (ya especificadas en la evaluación de riesgos). Lo que se presenta a continuación, son posibles escenarios que podrían darse si se materializan loas diferentes amenazas. Se han clasificado de forma que sea fácil su lectura.

Probabilidad/Frecuencia

- Alta: Existe la probabilidad de que se materialice el riesgo cuatro o más veces durante un año.
- Moderada: Existe la probabilidad de que se materialice el riesgo de dos a tres veces durante un año.
- Baja: Existe la probabilidad de se materialice el riesgo una vez al año o menos

Evaluación

- Graves:

- Quizás cause un grave daño pues los documentos deben ser digitalizados para proseguir con la demanda
- Causaran un grave daño que impedirá utilizar los ordenadores (entre otro)
- Se envía documentación original a los letrados: el servicio de mensajería debería ser efectivo
- Los 3 aplicativos muy importantes, y un daño sobre estos paraliza toda la actividad. Lo que retrasaría esta y nos e cumpliría con los plazos.
- Los navegadores son necesarios para realizar la actividad, pues se opera a través de ellos. Si estos no funcionan, la actividad se paraliza de nuevo
- El teléfono, Es un método de comunicación primordial para la empresa, ya que comunica con demás oficinas a nivel nacional.
- El teléfono, Causaría desatención a las oficinas, sin poder llevar a cabo la actividad.
- Un error, en los letrados causaría que no llegaran las demandas a tiempo de ser presentadas, pues se perdería dinero en la preparación
- Los ordenadores no gozan de poder ser administradores del mismo, sino que s externo. Si el daño lo tienen los externos, no se podría solventar de ninguna manera.
- Se usa primordial la electricidad, hay un sistema de alimentación que permite la actividad a un número reducido de ordenadores por los que se sigue la actividad sin necesidad de perder tiempo. Si sufriera algún daño, la actividad sería de ninguna

- Moderadas:
  - Si un ordenador no tuviera un antivirus, mucha información podría verse afectada.
  - El correo no resultaría un problema, puesto que no es la vía principal de comunicación
  - La coordinación es importante, puesto que el trabajo no sería realizado dentro de los plazos.
  - Se usa primordial la electricidad, hay un sistema de alimentación que permite la actividad a un número reducido de ordenadores por los que se sigue la actividad sin necesidad de perder tiempo. Si sufriera algún daño, la actividad sería de ninguna.
  - Los usuarios externos podrían ser necesitados para reparar por ejemplo una máquina que se usa constantemente: causaría un cumulo de trabajo si la maquina no funciona que los empleados no podrían asumir
- Leves:
  - Las sillas pueden ser substituidas por otras, y podrían haber de sobra

- El lenguaje es irrelevante pues no influye en la actividad. Dependen de la zona de España en que se envíen las demandas.

Se presenta en detalle lo explicado en el anexo 1. De forma más general se expresa de la siguiente manera. Cabe destacar que, se realiza un único gráfico para detallar las posibles amenazas que tienen un alto riesgo de materializarse.

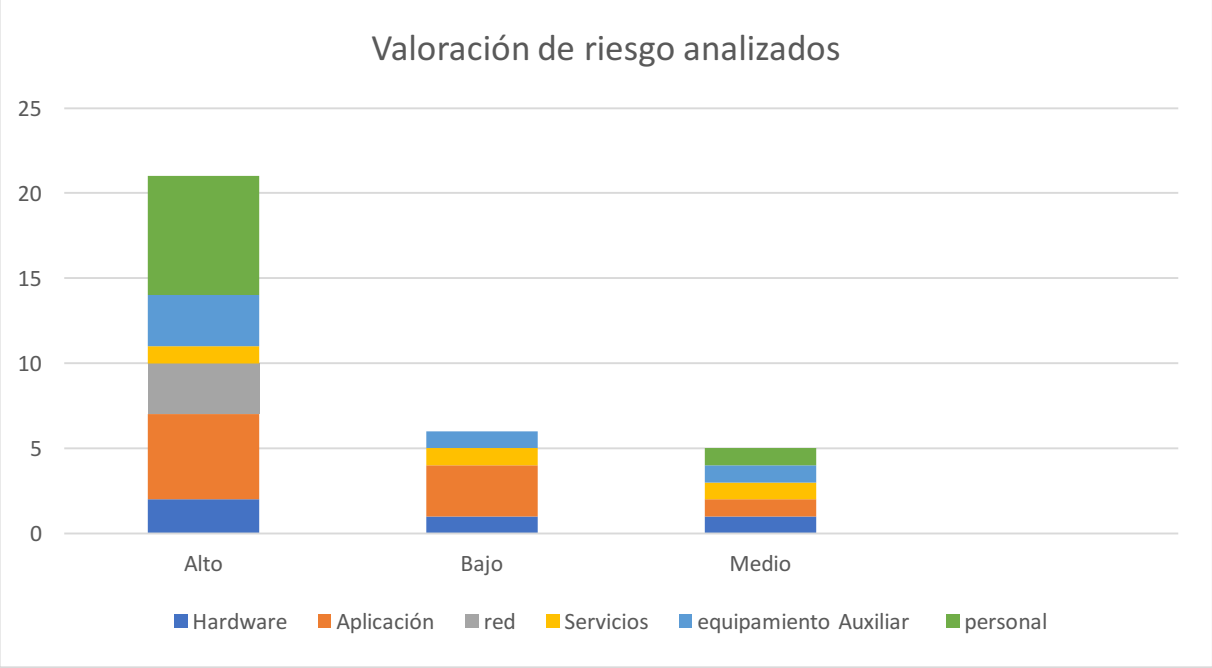


Ilustración 4 : diagrama de la valoración de riesgos analizados

De forma general, dentro de la gestoría, lo que más amenaza parece tener son los aplicativos y el personal. En una nota más específica, podemos observar que la empresa tiene muchos activos que tienen una valoración y criticidad muy alta. Esto es debido, a que el plan director y el análisis que se está realizando se centra en un único departamento y no en la totalidad de la empresa.

A continuación, se presentan los diferentes activos según la criticidad, la disponibilidad y la integridad de los mismos:

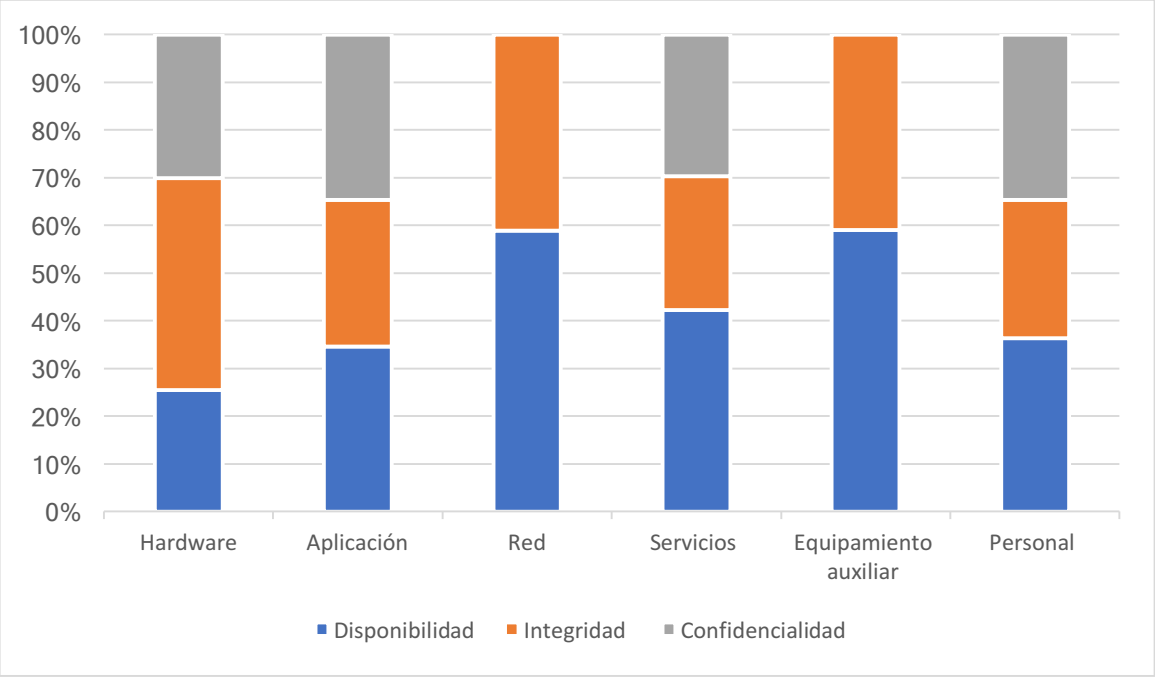


Ilustración 5: diagrama de la valoración de los activos

Observamos, qué en el activo de aplicación, los tres aspectos críticos tienen un valor similar, si no es considerado igual. Lo que corrobora lo anteriormente mencionado, el aplicativo es uno de los activos más relevantes para la organización. Del mismo modo sucede, con el personal. Se considera de vital importancia cubrir a los empleados de modo que la organización pueda seguir ofreciendo un servicio de calidad.

Tal como se ha dicho al inicio de este apartado, el nivel de riesgo aceptable es de "medio" y "bajo". Como se puede comprobar, la gran mayoría de los riesgos están en el novel "alto". Esto nos indica que se debe insistir en aquellos que están en esa situación y deben ser priorizados. Tales activos son el personal y los aplicativos. Para ambos, hay que definir los controles que se encuentran en el anexo 1, detalladamente.

b) Impacto potencial

Hemos analizado diferentes situaciones en las cuales muchos activos están en peligro. Si hacemos un balance, vemos que aquello que pude tener más riesgo son los aplicativos.

Estos son la base del trabajo que realiza la empresa. Es por eso que las posibles amenazas, como el fallo de la luz, el tener ordenadores viejos, la falta de conexión inalámbrica a internet, que los navegadores no funcionen, pueden causar una bajada de la productividad de la empresa.

Al mismo tiempo existe una amenaza sobre los armarios. Estos están cerrados con llaves, pero durante el día todo el mundo tiene acceso puesto, que están abiertos. Aun así, a la hora de comer en el departamento no hay nadie para vigilar y se tienen las tarjetas de identificación para entrar en la planta (no para entrar al edifico).

Se puede añadir, que los usuarios no son usados por una sola persona. El método de crear los usuarios es muy lento, lo que provoca el uso múltiple de un mismo. Es desconcertante, pues cada día se pide un usuario para hacer una revisión de los mismos. Debería agilizarse la creación de los usuarios, de manera que se tenga que usar el de otro empleado por el menor tiempo posible. Del mismo modo, que se tendría que ser más riguroso a la hora de crear las contraseñas. Están deberían ser únicas y no deberían repetirse, igual que debería evitarse el usar el número de usuario como contraseña, que viene por defecto. Debería ser más fácil cambiar la contraseña, pues solo se puede hacer cuando se está a punto de caducar.

V. Propuestas de proyectos (fase 4)

A continuación, se detallan las amenazas que se destacaron en el apartado anterior. Del mismo modo, se da respuestas a estas posibles amenazas.

ID 01	**Documento para la revisión de las impresoras.**
Descripción: Se trata de evitar que las impresoras dejen de funcionar en momentos en la que su funcionamiento es fundamental. Se pide a los empleados que lo notifiquen cuando haya errores.	

Objetivos: Se conseguirá agilizando el proceso de revisión de las máquinas. Estas serán controladas, y al mínimo detalle que no funcione se debe comunicar a los responsables, para que estos llamen al técnico. Intentar que sea el técnico directo de la marca, en lugar del informático de la empresa.	
AFECTACION	
Activos: Todas las impresoras de la planta	**Dominios ISO/IEC 27003:2013** **8.Gestión de activos**
Riesgos mitigados: La impresora funcione todo el tiempo.	
Durada: durante 1 año cada 3 semanas	**Periodo de consecución**: alto
Recursos necesarios	
Personal - Departamento informático - Responsables de departamento - Técnicos de impresoras - Empleados	Económicos Se estima un coste interno de 1000€ en función de las veces que deba venir el técnico fuera de las visitas convenidas.

ID 02	**Aplicativos en uso**
Descripción Los aplicativos son la base del servicio de la empresa. Se trata de evitar que estos dejen de dar a error ante los cambios que han sufrido.	
Objetivos: Se hará una revisión semanal con los empleados de los fallos que han tenido los aplicativos. Estos son los que los usan, y podrán dar un f*eedback* más realista.	
AFECTACION:	
Activos Aplicaciones: GID, terminal financiero y GDS *users*	**Dominios ISO/IEC 27003:2013** **Seguridad en la operativa**
Riesgos mitigados: Se reduce los errores de la aplicación delante de los cambios que sufre a causa de las nuevas leyes que están en vigor desde hace poco, y obligan a cambiar los procedimientos para llevar a cabo las demandas**.**	
Durada: 6 meses, con revisión cada semana	**Periodo de consecución**: alto
Recursos necesarios:	

Personal: - Empleados - Técnicos - Informáticos - Responsables	Económicos: Se van a necesitar 900€ para llevar a cabo lo que se ha determinada, dado que es un producto interno y creado internamente.

ID 03	**Ordenadores**
Descripción Los ordenadores son la herramienta básica. En los últimos meses han dado muchos fallos, y el funcionamiento es lento.	
Objetivos: Se debe comprobar que los ordenadores estén funcionando correctamente y que están actualizados con las ultimas condiciones.	
AFECTACION	
Activos Ordenadores	**Dominios ISO/IEC 27003:2013** Seguridad física y ambiental
Riesgos mitigados: Los PC estarán en buen estado para poder dar un uso diario.	
Durada: 5meses	Periodo de consecución: medio
Recursos necesarios	
Personal: - Técnico - Responsable de material	Económicos: Se destinarán unos 1500€ para la consecución de los objetivos.

ID 04	**Red**
Descripción Todo tipo de red, ya sea telefónica o inalámbrica, debe funcionar de manera permanente. Se trata de tener la mayor cobertura posible en cuanto a redes, para poder garantizar un uso óptimo. De modo que no se retrase la actividad.	
Objetivos: Conseguir las redes más potentes que haya en el mercado. Se intenta evitar perder el contacto con el resto de oficinas.	
AFECTACION	
Activos - Routers - Teléfonos - Cableado - Ordenadores	**Dominios ISO/IEC 27003:2013** 13.controles de red

- Wi-fi	
Riesgos mitigados: Se da un acceso ininterrumpido a internet las 24 horas del día los 7 días de la semana. Se trata de poder proporcionar el servicio constantemente.	
Durada: 1 mes	Periodo de consecución: alto
Recursos necesarios	
Personal - Técnicos de la compañía telefónica contratada - Informáticos - Recursos humanos	Económicos Se destinarán 500€.

ID 05	**Coordinación de grupos**
Descripción: Cada grupo tiene un responsable. Estos se encargan de coordinar la actividad que debe llevar a cabo el departamento. Es por eso que una buena comunicación con los empleados seria primordial. Además de una buena formación de los ésos para la consecución de los objetivos.	
Objetivos: Formar a los responsables para liderar el grupo y realizar las observaciones que sean necesarias. Del mismo modo que se proporciona una formación intergrupal entre los empleados y con los responsables.	
AFECTACION	
Activos: - Personal - Responsables - Departamentos	**Dominios ISO/IEC 27003:2013** 6.aspectos organizativos de la seguridad de la información
Riesgos mitigados: Evitar que el trabajo no sea autónomo y existe cohesión de equipo. Considerar el compañerismo como primera vía para la consecución de los objetivos del grupo.	
Durada: 1 año	Periodo de consecución: alta
Recursos necesarios	
Personal - Personal - Responsable - Profesionales en ámbito	Económicos 700€

- Psicólogos	

ID 06	Servicios internos
Descripción El departamento en cuestión gestiona las demandas de varis CCAA. Estas tienen oficinas de Crédito ya y deben ponerse en contacto las unas con las otras para poder obtener toda la información posible sobre los deudores.	
Objetivos: Facilitar el acceso a los datos de los clientes por parte de las oficinas y dar informaciones claras. Estas deben ser útiles, para la consecución del procedimiento judicial. Disponibilidad de los que se encargan de la información requerida.	
AFECTACION	
Activos: - Empleados - Empleados de las oficinas	**Dominios ISO/IEC 27003:2013** 15.relaciones con suministradores
Riesgos mitigados: Las personas que intervienen en el proceso de preparación de la demanda, tienen la información suficiente para el inicio del procedimiento judicial. Se evita errores y la consecución de deudores que no deben ser demandados.	
Durada: 6 meses	Periodo de consecución: medio
Recursos necesarios	
Personal - Empleados de las oficinas y del departamento - Responsables de morosidad/ directores de la sucursal	Económicos 300€

ID 07	Armarios
Descripción: Los armarios son el sitio donde se almacena toda la documentación necesaria para mandar a los letrados y que estos puedan redactar la demanda. Esta documentación es primordial que esté bien archivada, pues si se pierda la documentación, no se podrá presentar la demanda ni se reclamaran las deudas. Cada armario tiene llaves para cerrar por la noche los armarios.	
Objetivos: Conseguir que los armarios estén al día y la documentación que este físicamente en ellos sea la necesaria para la actividad. Evitando acumulación de expedientes	

y evitando un mal archivo de los mismos. Usar las llaves para cerrar los armarios con seguridad.	
AFECTACION	
Activos - Escrituras - Pólizas - Armarios - Llaves	**Dominios ISO/IEC 27003:2013 11. seguridad física y ambiental**
Riesgos mitigados: **Se contrata una sola persona para que archive y para que coja la documentación de los armarios. Se evita la perdida de la documentación y el extravío de las demandas.**	
Durada: 1,5 año	**Periodo de consecución: alto**
Recursos necesarios	
Personal: - Empleados	Económicos Se destinan 1000€

ID 08	**Usuarios**
Descripción: Cada empleado tiene un usuario que le sirve para entrar en los pc y en los aplicativos. Es individual y cada uno escoge su propia contraseña, a menos que se deba restaurar, que en este caso se activa una al azar. Los empleados se prestan los usuarios entre sí, los primeros días que hay un empleado nuevo. Los usuarios de los responsables, tienen más permisos y se pueden realizar más acciones.	
Objetivos: Prever los usuarios para los nuevos empleados sin necesidad de duplicar la actividad de un mismo usuario. Recomendar contraseñas que sean difíciles de encontrar. Evitar que los administradores sean utilizados por el personal.	
AFECTACION	
Activos - Usuarios - Empleados - Ordenadores - Contraseñas fuertes - Administradores	**Dominios ISO/IEC 27003:2013:** **c) Gestión de accesos: gestión de acceso de usuarios 9.22**

Riesgos mitigados: Más seguridad a la hora de saber quién ha realizado que acción y saber identificar a la persona.	
Durada: 1,5 año	**Período de consecución: alto**
Recursos necesarios	
Personal: - Empleados - Técnicos - Informáticos	Económicos Se destinan 1000€

A continuación, determinaremos los proyectos y su orden de prioridad, para finamente realizar un plan de proyecto completo.

A continuación, se realiza una lista en orden de prioridad que se ha considerado para la empresa. El primero siendo el que tiene más prioridad y el ultimo el que tiene menos. Aun así, hay que recordar que todos los activos que resultan de una alta criticidad. Es por eso que son los únicos que se han considerado en esta fase, para la creación de proyectos.

1. *Red.* Se hará una prueba de calidad para la señal de la red y comprobar que esta funciona. Los empleados jugaran un gran papel, pues también son los que hacen uso de esta red constantemente.
2. *Aplicaciones.* Existen tres aplicativos y cada uno tiene una función asignada que le es única. Aún, así se trata de proteger estos frente a una misma amenaza, pues el tipo de información que contienen y almacenan tiene el mismo riesgo si se perpetuara alguna de las amenazas. Cada día, se pedida el usuario a un empleado. Se hará un estudio de los errores que probablemente haya. Además, se entrevistará al usuario para que facilite, en el caso de que los hubiera, los fallos que haya encontrado. De este modo se crean actividades desde un punto de vista técnico y otro más práctico.

3. *Servicios internos*. Se realizará un test de calidad. Esto consistirá en recopilar la información que un empleado pide a la oficina, y recoger aquello que la oficina contesta. El riesgo que se corre, es que la información puede ser sugestiva y no ser completa. Al mismo tiempo, las preguntas pueden no estar formuladas correctamente y la respuesta puede no ser clara.
4. *Ordenadores.* Los ordenadores son la herramienta básica del trabajador. Estas deben tener un rendimiento adecuado al nivel de trabajo que se realiza a lo largo del día. Es por eso que al mismo tiempo que se pide un usuario para hacer el seguimiento, también se realiza del PC. Cada una tiene un número, y estos están apuntados junto con la persona y usuario que lo utiliza. Cualquier tipo de incidencia que suceda, se debe abrir una incidencia, con el personal de mantenimiento. Los empleados no deben tocar nada: ni los cables, ni las torres. Tampoco pueden mover las torres si se cambian de sitio, puesto que debe hacerlo un informático.
5. *Armarios.* En ellos se almacena toda la documentación relacionada con la morosidad. Es todo aquel documento que se firmó en su momento para el préstamo, además de la fe notarial que lo que se está argumentado, es la suma correcta de lo que se debe. Es por eso, que se escogen 40 contratos de los cuales se hace el seguimiento. Se les llama, el TOP 40. Estos son seguidos por el equipo de responsables y se debe conocer su situación en todo momento.
6. *Usuarios*. El problema radica en el uso múltiple de un mismo usuario. Un empleado nuevo no tiene usuario el primer día, puesto que aún no se han pedido los permisos. Es por eso que se usa el usuario de otro empleado mientras el suyo es creado. El control de estos usuarios, es una vez más con control diario de uno. Se quiere intentar

7. *Impresoras.* Los departamentos disponen de un código de acceso a las impresoras. Se contabilizarán los errores, desde la sala en que los encargados de mantenimiento de las maquinas podrán verlos al momento. Se hará el seguimiento de ellos, para poder llamar al técnico que corresponda en tiempo. La reparación no se hace de manera interna. Esto retrasa la actividad, por lo que se instalan varias de ellas en la planta de trabajo.
8. *Coordinación de equipos*. Un grupo es liderado por su responsable, el cual debe estar disponible en todo momento durante su horario laboral. Se harán cursillos, para que los responsables comuniquen con los empleados y sepan transmitir con claridad las ordenes. Además, deben saber afrontar las situaciones en que deban tomar decisiones que pueden traer consecuencias para el equipo.

VI. FASE V: AUDITORIA DE CUMPLIMIENTO

Se han definido y evaluado las amenazas posibles que se pueden dar en la empresa. Llegados a este punto, hay que verificar si los 114, puntos que define la ISO a la cual se quiere verificar, se cumplen. De este modo, enfocaran las siguientes acciones a mejorar esta relación y lo que falta para llegar a los niveles óptimos de la ISO.

Se ha hecho una relación con todos los controles que hay definidos y deben aplicarse, según la tabla que se basa en el Modelo de Madurez de la Capacidad (CMM). Este fue diseñado por el SEI (Instituto de Ingeniería del Software) en 1991 en EEUU (Aguirre y Córdoba, 2008); para dar respuesta a "los problemas de mal funcionamiento y cumplimiento de expectativas de los programas informáticos". El CMM, se desarrolla a partir de 5 niveles:

Efectividad	CMM	SIGNIFICADO	DESCRIPCION
0%	L0	INEXISTINTE	Carencia completa de cualquier proceso reconocido

10%	L1	INICIAL /AD HOC	El ÉXITO DE LOS PROCESOS SE BASA EN LA MAYOR PARTE DEL ESFUERZO DEL PERSONAL. LOS PROCEDIMEINTOS SON INEXISTENTES O LOCALIZADOS EN AREAS MUY CONCRETAS. No existen plantillas
50%	L2	REPRODUCIBLE PERO INTUITIVO	Los procesos similares se llevan a cabo de manera similar por diferentes personas con la misma tasca. Se normalizan las buenas prácticas en base a la experiencia y el método.
90%	L3	PROCESO DEFINIDO	La organización en su conjunto participa en el proceso. Los procesos están implantados, documentados y comunicados.
95%	L4	GESTIONADO Y MEDIBLE	Se puede seguir la evolución de los procesos mediante indicadores numéricos y estadísticos. Hay herramientas para mejorar la calidad y la eficiencia
100%	L5	OPTIMIZADO	Los procesos están bajo constante mejora. En base a criterios cuantitativos se determinan las desviaciones

Ilustración 6 : CMM

La aplicación de tal sistema a la empresa de estudio es la siguiente: se ha realizado el análisis del CMM, completo tal como queda reflejado en la tabla del anexo 5. Se puede encontrar por cada control, la descripción del mismo en aquellos que se consideran relevantes para el análisis de la realización del presente trabajo. A fin, de evitar una tarea extensa y una lectura complicada. Se han juntado las descripciones y el grado de

cumplimiento de cada uno de ellos. Se han anotado según el cuadro anteriormente presentado.

De forma general, los controles de madurez del CMM quedaría de la siguiente manera:

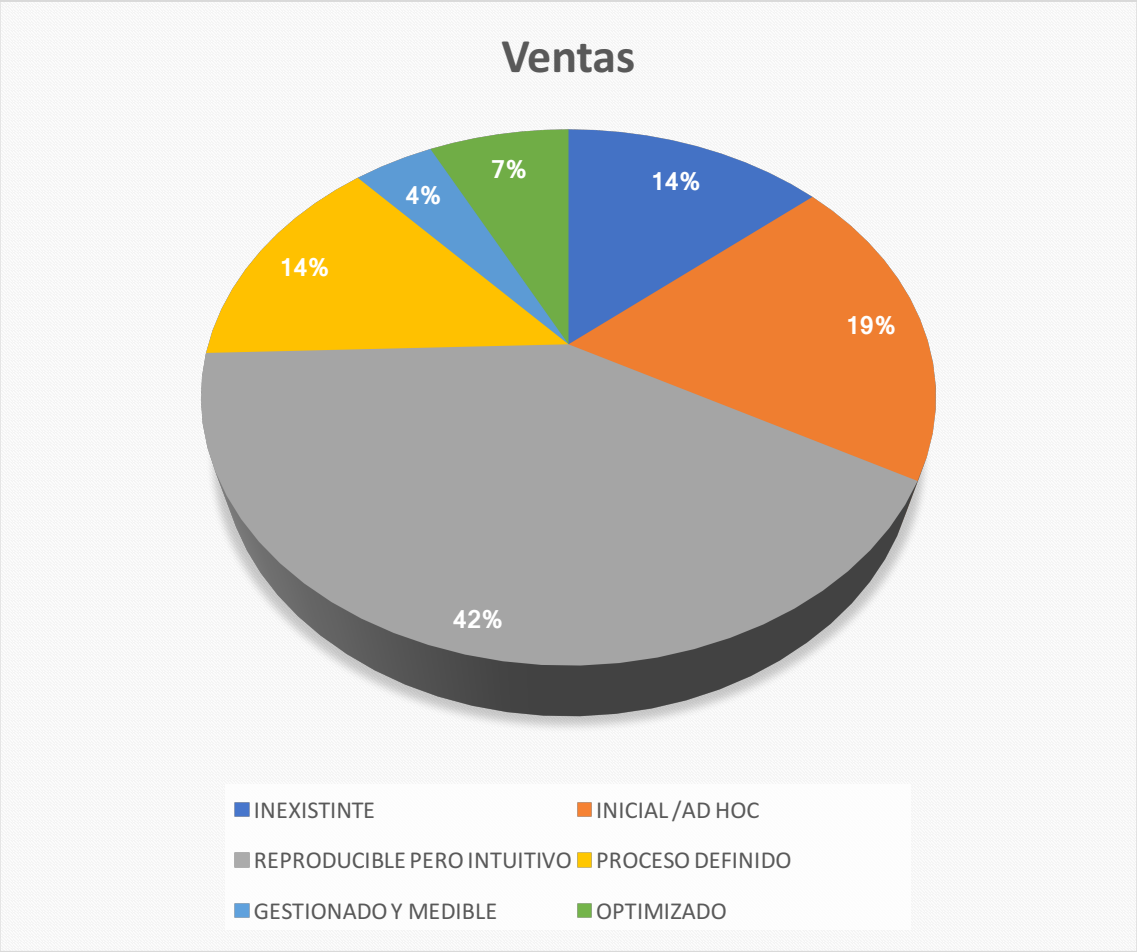


Ilustración 7: madurez CMM de los controles ISO

Del anterior gráfico, cabe comentar que el cumplimiento que más se da para los controles es el de "reproductible, pero intuitivo". Las normas establecidas no están bien repartidas: una misma tarea la realizan distintas personas. Es una repetición del trabajo, que ocupa tiempo y no es eficiente. La comunicación entre las distintas personas que realizan la tarea, es inexistente, y no hay formación al respecto. Es por eso que se debe, trabajar en esas áreas en donde las tareas no son claras, y podrían mostrar una amenaza

muy alta. En concreto, como se ha comentado, los dos activos que están con un riesgo notablemente alto son el personal y los aplicativos. Esto nos hace deducir, que el personal no está bien formado para su tarea y lo aplicativos carecen de seguridad.

Madurez de los controles definidos en ISO 27002

Los cuadros que se relacionan con el apartado son añadidos en los anexos 5. A continuación, se presenta un cuadro representativo de forma general del cumplimiento actual del ISO 27002, además de las no conformidades. Se han podido extraer desde los cumplimientos que han dado resultado del análisis comparativo de la ISO 27001 y 27002.

Dominio	**% de efectividad**	**NC mayores**	**NC Menores**
5. política de seguridad	30	0	2
6. aspectos organizativos de SI	50	2	5
8. gestión de activos	25	0	6
7. seguridad ligada a los recursos humanos	40	0	6
8.gestion de activos	25	6	4
9. control de accesos	40	4	9
11. seguridad física y ambiental	40	6	9
12. seguridad en la operativa	80	3	11
13. seguridad en las telecomunicaciones	60	1	5

14. Adquisición, desarrollo y mantenimiento de los sistemas de información.	40	2	9
16. gestión de incidentes en la seguridad de la información	20	6	0
17. aspectos de seguridad de la información en la gestión de la continuidad del negocio	20	1	3
18. cumplimiento	65	0	4

Ilustración 8: cuadro resumen de los niveles de cumplimiento del Iso 27002 y las no conformidades

Tal como se observa, el dominio que claramente tiene el grado de más avanzado es el "12. Seguridad en la operativa". Por lo contrario, los que necesitan más trabajo son el 16 y 17.

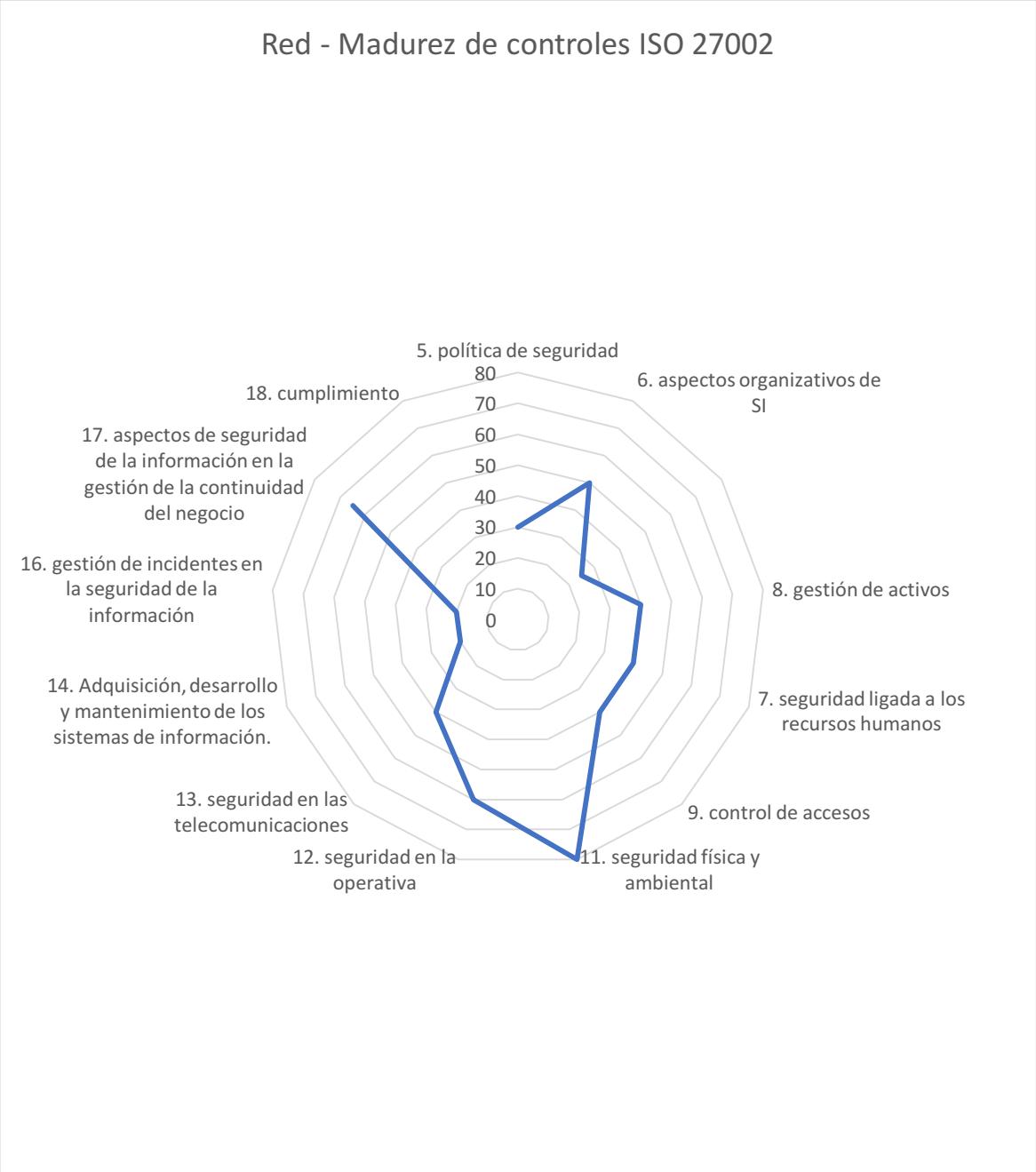


Ilustración 7: red de madurez del CMM

Así mismo, se debe trabajar en la gestión de los incidentes y en los aspectos de la seguridad continuidad del negocio. Se deduce, que los "planes de futuro", de la empresa no están bien definidos. La normativa no está aplicada con rigurosidad y debe ser actualizada con los últimos protocolos existentes.

VII. Conclusiones y objetivos

Se presentan los objetivos que se indicaron al principio, a modo de recordatorio:

- Mejorar la seguridad de la página web
- Adecuar los controles de acceso físico
- Hacer un control de usuarios
- Identificar las correcciones que sean convenientes para la seguridad de los documentos tratados
- Exponer el cumplimiento de las normas
- Evaluar las posibles amenazas y sus soluciones (exhaustivamente)
- Describir las políticas de seguridad de la empresa

Veamos a continuación si, tras el análisis se pueden o se podrán completar y conseguir los objetivos que se propusieron. Se hará de forma, que la respuesta que se dé, serán las conclusiones del trabajo.

Todas las posibles amenazas y sus soluciones han sido evaluadas y han sido identificadas con un riguroso detalle.

La página web, es decir, los aplicativos, han mostrado ser seguros. Lo que no es seguro, es la forma de trabajar con ellos por parte de los empleados.

Al realizar el análisis de riesgos, los resultados indican que aquellos que tienen más peligro son las aplicaciones y los empleados. Más concretamente, las aplicaciones son débiles por el mal uso de los usuarios por parte de los empleados. No se lleva a cabo un registro riguroso de estos y tampoco se dan de baja cuando uno de los empleados abandona la empresa. Esto conduce a un descontrol de privacidad y de identificación dentro del sistema de los aplicativos.

Los empleados, no tienen la suficiente formación para gestionar la información con la que se trabaja, ni conocen las tareas de seguridad que deben llevar a cabo para mantener la confidencialidad.

Los accesos físicos, han demostrado ser parte de las "no conformidades", pero de las menores. Es decir, que deben ser ajustados, pero no de inmediato, por lo que hay otras no conformidades que son prioritarias.

VIII. Bibliografia

Aguirre Mayorga, H., & Córdoba Pinzón, N. (2010). Diagnóstico de la madurez de los procesos en empresas medianas colombianas. *Ingenieria Y Universidad: Engineering For Development, 12*(2). Retrieved from http://revistas.javeriana.edu.co/index.php/iyu/article/view/944/541

Abril, A., Pulido, J., & Bohada, J. A. (2014). Análisis de Riesgos en Seguridad de la Información. *Ciencia, Innovación y Tecnología*, *1*, 39-53.

Standard ISO 27002 y 27001.

IX. Anexos

L. Anexo 1

AMBITO	ACTIVO	VALORACION/ CRITICIDAD	ASPECTOS CRITICOS		
			c	i	d
HARDWARE	1. Scanner 2. Servidores	1. Alto 2. Alto 3. Bajo 4. Medio	3 4 5 7	8 9 6 5	9 9 5 6

	3. Mobiliario (armarios, sillas, mesas…) 4. Medios de impresión				
APLICACIÓN	Desarrollo propio: 1. Aplicativo IDD 2. GDS USERS Desarrollo a medida: 1. TERMINAL FINANCIERO Estándar: 2. Antivirus 3. Lenguaje 4. Navegador web 5. Servicios correo 6. Sistemas operativos	1. Muy Alto 2. Muy Alto 3. muy alto 4. alto 5. despreciable 6. alto 7. medio 8. medio	9 9 9 7 5 7 8 9	8 8 8 6 5 7 6 8	10 10 10 8 4 7 6 8
RED	1. Red telefónica 2. Red inalámbrica 3. Red	1. Muy Alto 2. Alto 3. Muy alto	7 5 5	7 7 7	10 10 10
SERVICIOS	Servicios internos: 1. Atención a las oficinas, letrados y cualquier que relacionado con demandas 2. Coordinación de los equipos 3. Asignación de letrados y procuradores	1. Alto 2. medio 3. bajo	7 4 8	8 4 6	9 9 9
EQUIPAMIENTO AUXILIAR	1. Sistemas de alimentación ininterrumpida 2. Generadores eléctricos 3. Equipos de climatización 4. Cableado 5. Armarios del archivo	1. Alto 2. Muy alto 3. Medio 4. Bajo 5. Muy alto	4 4 3 5 9	7 8 8 7 10	8 7 4 7 10

PERSONAL	Usuarios internos: 1. Administradores de sistemas 2. Desarrolladores 3. Administradores de los aplicativos 4. Talento humano 5. Coordinadores	1. Muy alto 2. Muy alto 3. Muy alto 4. Muy alto 5. Medio	8 8 8 9 6	7 6 9 6 7	9 6 9 9 9
	Usuarios externos 1. Los técnicos de las maquinas 2. Trabajadores de empresas que colaboran 3. Transportistas 4. Mensajeros	1. Alto 2. Bajo 3. Alto 4. Alto	7 6 7 8	5 6 5 5	7 6 7 8

DIMENSIONES DE SEGURIDAD

ACTIVO	FRECUENCIA	[C]
[HARD] hardware [HARD] Scanner no funciona [HARD] perdida llaves armarios [HARD] impresoras no tienen tinta	100 20 1 0	100% 50% 30% 20%
[APP] aplicación [*APP] Desarrollo propio* [APP] no se guardan las acciones que se realizan [APP] no deja asignar el letrado [APP*] Desarrollo a medida:* [APP] da error cuando se quiere buscar un cliente por el DNI [*APP] Estándar* [APP] no es potente [APP] al estar en Cataluña, algunas CCAA no entienden los mails [APP] dejan de funcionar los navegadores [APP] falla la conexión a los mails [APP] el sistema es muy lento	 100 20 50 30 20 50 20 0 0 0 0	100% 40% 20% 20% 30% 30% 30% 5% 5% 5% 5% 10%
[*RED] RED* [RED] ha habido una tormenta que ha cortado la luz [RED] la conexión a internet es débil y lenta	60 20 40 0	100% 30% 40%

[RED] la red se cuelga repetidamente		30%
[SERV]Servicios internos [SERV] las oficinas no sabrían resolver dudas sobre las demandas [SERV] los empleados no saben cual es su trabajo [SERV] los letrados no saben los contra los cuales deben presentar una demanda	100 60 20 10	100% 30% 50%
[EQUIP]equipamiento auxiliar [EQUIP]si hay un apagón, algunos ordenadores aun funcionaran y permitirán guardar lo último que se ha hecho [EQUIP]Generadores eléctricos [EQUIP] si hiciera frío, conectaría para estar en un ambiente más cálido [EQUIP]los aparatos funcionan con ellos para conectarse a la corriente o entre si [EQUIP]los armarios podrían desaparecer, o su información si no se cierra con llave	100 30 20 1 0 1	100% 30% 10% 10% 20% 30%
[PERS] **PERSONAL** [*PERS] Usuarios internos* [PERS]un usuario necesita ser restaurado [PERS]los permisos de cada empleado están muy limitados a su función en el trabajo y se usaría el usuario de otro [PERS] los profesionales no están bien formados [PERS] estos están enfermos y nadie está allí para coordinar al equipo	 50 40 50 20 1	100% 50% 15% 20% 10% 5%
[P*ERS] Usuarios externos* [PERS] la colaboración entre empresas sería una pérdida de tiempo [PERS] las acciones no estarían al día [PERS] las demandas no llegarían a tiempo para ser presentadas	50 20 0 1	50% 10% 10% 15% 15%

M. Anexo 2

ESQUEMA DOCUMENTAL

A continuación, se desarrolla el esquema documental. Se ha realizado de tal manera, que se trata cada uno de manera individual. La apariencia de cada uno va acorde con los procesos establecidos.

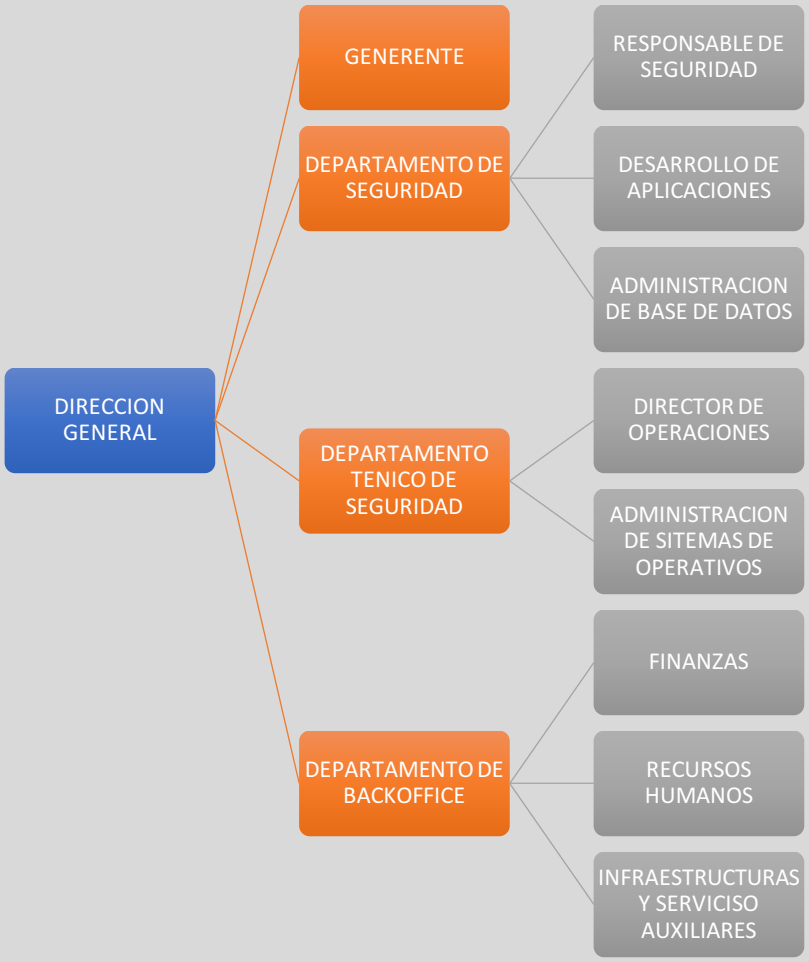
POLITICA DE SEGURIDAD	P PS- 01 PAGINA 1
VERSIÓN. 1.0 Fecha de implementación 2/05/2017	

PRINCIPIOS GENERALES: Los principios generales de la política del Sistema de Gestión de Seguridad de la Información (SGSI) son los siguientes:

- El Sistema de Gestión de Seguridad de la Información debe velar esencialmente por la preservación de la confidencialidad, integridad y disponibilidad, de todos los activos de información físicos y electrónicos propiedad de ***Dinero ya SL***, de sus clientes, empleados, asociados de negocio y partes interesadas.
- Los Objetivos en Seguridad de la Información deben estar de acuerdo a las obligaciones contractuales y legales, la rentabilidad de los activos, el estado de la tecnología y los criterios organizativos vigentes.
- Se debe aplicar una Gestión de los Riesgos con un criterio de evaluación del riesgo alineado con la estrategia de la organización y aprobado por la Dirección
- Se deben aplicar los principios de mejora continua en la reducción del riesgo, los procesos y la implementación de controles, anteponiendo la prevención a la corrección.
- La política debe ser conocida y cumplida por todo el personal que trabaja en y para la organización, así como las partes interesadas (terceros o clientes) que puedan tener afectación en la seguridad de la información, independiente de su nivel jerárquico u organizativo.
- Quien con conocimiento manifiesto de la presente política de seguridad omita su cumplimiento o actúe de manera negligente contra cualquiera de sus preceptos podrá quedar sujeto a acciones disciplinarias, llegando si procede al despido y al emprendimiento de las acciones legales contra él que la compañía considere oportunas.
- La compañía proporcionará todos los medios humanos y recursos económicos y técnicos a su alcance para establecer, adecuar y mejorar de manera permanente un plan de Continuidad del Negocio que tenga como objetivo asegurar la operatividad de las actividades productiva en caso de producirse un desastre con posibles consecuencias mayores

Responsabilidades: Definiremos en este apartado las responsabilidades especificas respecto de la gestión de la seguridad de la información.

Tal como se ha indicado al principio de la memoria, las responsabilidades son las



siguientes:

Ilustración XX: diagrama organizativo

El gerente se encargará de la ejecución de las funciones de los departamentos encargados de la seguridad da la información.

El departamento de seguridad, tendrá como competencias dirección, formación, análisis del desempeño y establecimiento de procedimientos y procesos relacionados con la seguridad de la información. Esta dará, así mismo los permisos al departamento técnico, para desarrollar lo que considere, permisos de accesos a los programas y aplicativos, la entrada a los edificios, etc.

Cualquier tipo de intromisión será competencia del departamento de *backoffice*, su investigación y/o posible resolución.

Gestión de indicadores	P - GESTIND- 02 PAGINA 1 DE 1
VERSIÓN. 1.0 Fecha de implementación 2/05/2017	

Para la evaluación de los indicadores, definiremos los indicadores. Junto a ello, constará su valor y su funcionamiento. El caso ideal sería, el detalle de cada uno de los indicadores que figuran en la norma. Por razones de lectura más amena, hemos seleccionado aquellos que son más relevantes para el estudio y su aplicación dentro de la norma.

NOMBRE DEL INDICADOR	Gestion de la segurida de las redes
DESCRIPCION	Integridad de la red
CONTROL DE SEGURIDAD	10.6
FORMULA DE MEDIMIENTO	Numero de errores
UNIDAD DE MEDIDA	
FRECUENCIA	1 vez por mes
RESPONSABLE DE LA MEDIDA	Responsable técnico de la seguridad de la información

NOMBRE DEL INDICADOR	Adquisición, desarrollo y mantenimiento de sistemas de información
DESCRIPCION	Funcionamiento permanente de los aplicativos
CONTROL DE SEGURIDAD	12.2, 12.1, 12.3, 12.5.2, 12.4, 12.6, 10.8, 11.6
FORMULA DE MEDIMIENTO	
UNIDAD DE MEDIDA	Días que falla/momento del día en que falla
FRECUENCIA	1 vez por semana

RESPONSABLE DE LA MEDIDA	Responsable técnico de la seguridad de la información

NOMBRE DEL INDICADOR	Control de los ordenadores
DESCRIPCION	Controlar el buen funcionamiento de lso ordendores
ONTROL DE SEGURIDAD	11, 11.7, 9.2
FORMULA DE MEDIMIENTO	
UNIDAD DE MEDIDA	Frecuencia con la que fallan
FRECUENCIA	Una vez al mes
RESPONSABLE DE LA MEDIDA	Informáticos

NOMBRE DEL INDICADOR	Buen estado del material e infraestructuras
DESCRIPCION	Los armarios están cerrados correctamente
ONTROL DE SEGURIDAD	9.1 y 9.2
FORMULA DE MEDIMIENTO	Comprobaciones
UNIDAD DE MEDIDA	
FRECUENCIA	Cada día
RESPONSABLE DE LA MEDIDA	Responsable del departamento

NOMBRE DEL INDICADOR	Control de usuarios
DESCRIPCION	Cada empleado debe tener su propio usuario, para no llevar a confusiones de acciones. Del mismo modo que cuando dejan de trabajar para la empresa, darlo de baja.
ONTROL DE SEGURIDAD	11.3, 11.6, 11.7, 12.5.2
FORMULA DE MEDIMIENTO	
UNIDAD DE MEDIDA	Comprobaciones
FRECUENCIA	1 vez al mes/si el empleado ya no trabaja
RESPONSABLE DE LA MEDIDA	Responsable del departamento/responsable de la seguridad de la información

NOMBRE DEL INDICADOR	Control de la infraestructura para la realización del trabajo
DESCRIPCION	Las funciones de impresión y escaneo de las impresoras deben estar siempre a punto
ONTROL DE SEGURIDAD	7.1 y 9.2
FORMULA DE MEDIMIENTO	
UNIDAD DE MEDIDA	Comprobaciones recurrentes/según la demanda de los empleados
FRECUENCIA	Cada día
RESPONSABLE DE LA MEDIDA	Responsable de las impresoras

NOMBRE DEL INDICADOR	Seguridad ligada a los recursos humanos
DESCRIPCION	La coordinación de los equipos
ONTROL DE SEGURIDAD	8.1-2-3
FORMULA DE MEDIMIENTO	
UNIDAD DE MEDIDA	Reuniones
FRECUENCIA	Trimestralmente
RESPONSABLE DE LA MEDIDA	Gerente

<table>
<tr><td colspan="2">Procedimiento de auditorísas internas</td><td>P dr- 02
PAGINA 1 DE 1</td></tr>
<tr><td colspan="3">VERSIÓN. 1.0
Fecha de implementación 2/05/2017</td></tr>
<tr><td colspan="3">Objetivo:
Elaborar un registro de las auditorias que se realizaran a cabo y el formato que deben tener.</td></tr>
<tr><td colspan="2">Alcance: será entorno a los dos departamentos que se auditan.</td><td>Responsabilidades: el comité de seguridad debe procurarse que el registro se realice y que se cumplan.</td></tr>
<tr><td>Revisiones:
Sin revisiones.</td><td colspan="2">Desarrollo: se realizará 1 auditoria cada 3 meses. Cada una de ellas se centrará en un departamento. Aleatoriamente, pues hay dos departamentos que se auditan. La ultima auditoria a realizar, se realizará en un conjunto de las dos, de este modo se obtiene una auditoria más amplia y más concreta en cada departamento.
El contenido de las auditorias será el siguiente:
- Data
- Nombre de los auditores
- Alcance
- Controles auditados
- Conformidad del SGSI con la norma
- No-conformidades detectadas
- Recomendaciones de mejora
- Resumen comparativo de la última auditoria</td></tr>
</table>

<table>
<tr><td colspan="2">Procedimiento de revisión por la dirección</td><td>P dr- 04
PAGINA 1 DE 1</td></tr>
<tr><td colspan="3">VERSIÓN. 1.0
Fecha de implementación 2/05/2017</td></tr>
<tr><td colspan="3">Objetivo:
Establecer las reuniones que llevará a cabo la dirección, para la revisión interna de los procesos.</td></tr>
<tr><td colspan="2">Alcance: los responsables que estarán presentes en las reuniones. Son los responsables de cada departamento, y aquellos que ostenten un cargo de relevancia en la empresa.</td><td>Responsabilidades: el director general es quien se encargará de organizar las reuniones. Su función es hacer que los asistentes estén en las reuniones.</td></tr>
<tr><td>Revisiones:
Sin revisiones.</td><td colspan="2">Desarrollo: el director general deberá establecer el orden día (aquello que se hablará en la reunión); deberá enviar vía mail una convocación a los asistentes. Asimismo, debe establer cuales son las prioridades de la reunión.</td></tr>
</table>

<table>
<tr><td colspan="2">Gestión de roles y responsabilidades</td><td>P RR- 05
PAGINA 1 DE 1</td></tr>
<tr><td colspan="3">VERSIÓN. 1.0
Fecha de implementación 2/05/2017</td></tr>
<tr><td colspan="3">Objetivo:
Identificar los roles que debe llevar a cabo cada responsable.</td></tr>
<tr><td colspan="2">Alcance: los responsables del departamento al que se realiza la auditoria; el comité de seguridad.</td><td>Responsabilidades: el gerente de la oficina es quien se encarga de que los responsables, realicen su trabajo. Una persona de la dirección que forma parte del comité de seguridad. Nos remitimos al diagrama que, de forma clara, identifica los diferentes roles que existen.</td></tr>
<tr><td>Revisiones: Sin revisiones.</td><td colspan="2">Desarrollo: los responsables deben dirigir las actividades que llevan a cabo los empleados; deben al mismo tiempo reunirlos si hay algún acontecimiento que sea de interés para todos. El comité de seguridad, debe crear, mantener, supervisar y mejorar el Sistema.</td></tr>
</table>

<table>
<tr><td colspan="2">ANALISIS
DE
RIESGO</td><td>P AR- 06
PAGINA 1 DE 1</td></tr>
<tr><td colspan="3">VERSIÓN. 1.0
Fecha de implementación 2/05/2017</td></tr>
<tr><td colspan="3">Objetivo:
Establecer aquellos riesgos que pueden llegar a perpetuarse.</td></tr>
<tr><td colspan="2">Alcance: está diseñado para los aplicativos, los armarios, y las impresoras.</td><td>Responsabilidades: el responsable de seguridad es quien se encargará de vigilar los aspectos que puedan derivarse.</td></tr>
<tr><td>Revisiones:</td><td colspan="2">Desarrollo: cada día, los empleados deben desconectar el usuario con el que han entrado en el aplicativo; deben desconectar las impresoras y cerrar los armarios al finalizar el día. Por la mañana, se hace lo contrario para poder usarlo.</td></tr>
</table>

N. Anexo 5

[5]POLÍTICAS DE SEGURIDAD	**30%**	**Control**	
[5.1] Directrices de la Dirección en seguridad de la información.	30%		
[5.1.1] Conjunto de políticas para la seguridad de la información.	30%	La dirección debería aprobar un documento de política de Seguridad de la información, publicarlo y distribuirlo a todos los afectados	L2
5.1.2] Revisión de las políticas para la seguridad de la información	30%	La política de seguridad de la información debería revisarse a intervalos planificados o siempre que se produzcan cambios significativos, a fin de asegurar que se mantenga su idoneidad, adecuación y eficacia.	L2

[6] ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMACION	50%		
[6.1] Organización interna.	50%	La Dirección debe mostrar un apoyo a la seguridad dentro de la organización a través de directrices claras, compromiso, asignaciones explícitas y el reconocimiento de las responsabilidades de seguridad de la información.	
[6.1.1] Asignación de responsabilidades para la seguridad de la información	90%	Las tareas relacionadas con seguridad de la información deben estar repartidas con precisión según el departamento.	L3
[6.1.2] Segregación de tareas.	50%	Para cada nuevo recurso de tratamiento de la información, debería definirse e implantarse un proceso de autorización por parte de la Dirección.	L2

[6.1.3] Contacto con las autoridades.	20%		L2
[6.1.4] Contacto con grupos de interés especial.	40%	Cada nuevo compromiso debe acompañarse de los espcialistas adecuados.	L2
[6.1.5] Seguridad de la información en la gestión de proyectos.	50%	Debería determinarse y revisarse periódicamente la necesidad de establecer acuerdos de confidencialidad o no revelación, que reflejen las necesidades de la organización para la protección de la información.	L2
[6.2] Dispositivos para movilidad y teletrabajo.	0%	0%	
[6.2.1] Política de uso de dispositivos para movilidad.	0%	debe existir una politaca explicita sobre el uso de los dispositivos, indicando quien y donde se pueden usar.	L0
[6.2.2] Teletrabajo	0%	Debe existir un cierto margen para pode trabajar a distancia: como distintas formas de comunicación.	L0

[7] SEGURIDAD LIGADA A LOS RECURSOS HUMANOS.	40%	CONTROL	CUMPLIMIENTO
[7.1] Antes de la contratación.	90%		
[7.1.1] Investigación de antecedentes.	90%	La comprobación de los antecedentes de todos los candidatos a un puesto de trabajo, de los contratistas o de los terceros, se debería llevar a cabo de acuerdo con las legislaciones, normativas y códigos éticos que sean de aplicación y de una manera proporcionada a los requisitos del negocio, la clasificación de la información a la que se accede y a los riesgos considerados.	L3
[7.1.2] Términos y condiciones de contratación.	90%	Como parte de sus obligaciones contractuales, los empleados, los contratistas y los terceros deberían aceptar y firmar los términos y condiciones de su contrato de trabajo, que debería establecer sus responsabilidades y las de la organización en lo relativo a seguridad de la información.	L3
[7.2 Durante la contratación.	20%		

[7.2.1] Responsabilidades de gestión.	30%	La Dirección debería exigir a los empleados, contratistas y terceros, que apliquen la seguridad de acuerdo con las políticas y procedimientos establecidos en la organización.	L2
[7.2.2] Concienciación, educación y capacitación en segur. de la información	20%	Todos los empleados de la organización y, cuando corresponda, los contratistas y terceros, deberían recibir una adecuada concienciación y formación, con actualizaciones periódicas, sobre las políticas y procedimientos de la organización, según corresponda con su puesto de trabajo.	L2
[7.2.3] Proceso disciplinario.	20%	Debería existir un proceso disciplinario formal para los empleados que hayan provocado alguna violación de la seguridad	L2
[7.3] Cese o cambio de puesto de trabajo.	20%		
[7.3.1] Cese o cambio de puesto de trabajo	20%	Las responsabilidades para proceder al cese en el empleo o al cambio de puesto de trabajo deberían estar claramente definidas y asignadas.	L2

[8] GESTIÓN DE ACTIVOS	**25%**	CONTROL	CUMPLIMIENTO
[8.1] Responsabilidad sobre los activos	25%		
[8.1.1] Inventario de activos	50%	Todos los activos deberían estar claramente identificados y debería elaborarse y mantenerse un inventario de todos los activos importantes.	L2
[8.1.2] Propiedad de los activos	10%	Toda la información y activos asociados con los recursos para el tratamiento de la información deberían tener un propietario que forme parte de la organización y haya sido designado como propietario.	L1
[8.1.3] Uso aceptable de los activos	30%	Se deberían identificar, documentar e implantar las reglas para el uso aceptable de la información y de los activos asociados con los recursos para el tratamiento de la información.	L2
[8.1.4] Devolución de activos	10%	los activos, deben serdevueltos una ve cesa el empleo	L1
[8.2] Clasificación de la información.	20%		

[8.2.1] Directrices de clasificación.	30%	La información debería ser clasificada según su valor, los requisitos legales, su sensibilidad y criticidad para la organización	L0
[8.2.2] Etiquetado y manipulado de la información.	10%	Se debería desarrollar e implantar un conjunto adecuado de procedimientos para etiquetar y manejar la información, de acuerdo con el esquema de clasificación adoptado por la organización	L0
[8.2.3] Manipulación de activos.	20%		L2
[8.3] Manejo de los soportes de almacenamiento.	30%		
[8.3.1] Gestión de soportes extraíbles.	0%	La información debería ser clasificada según su valor, los requisitos legales, su sensibilidad y criticidad para la organización	L0
[8.3.2] Eliminación de soportes.	30%	Se debería desarrollar e implantar un conjunto adecuado de procedimientos para etiquetar y manejar la información, de acuerdo con el esquema de clasificación adoptado por la organización	L2
[8.3.3] Soportes físicos en tránsito.	0%	los soportes deben ser tal como manda la organización de la seguridad de la información	L0

[9] CONTROL DE ACCESOS		CONTROL	CUMPLIMIENTO
[9.1] Requisitos de negocio para el control de accesos.	70%		
[9.1.1] Política de control de accesos.	95%	Habria que establecer una política de control de acceso basada en los requisitos del negocio y de seguridad para el acceso.	L4
[9.1.2] Control de acceso a las redes y servicios asociados.	40%		L2
[9.2] Gestión de acceso de usuario.	10%		

[9.2.1] Gestión de altas/bajas en el registro de usuarios.	10%	Debria exitir un riguroso seguimiento de las bajas en el personal, paa a simismo dar de baja esos usuarios.	L1
[9.2.2] Gestión de los derechos de acceso asignados a usuarios.	10%	Se debería regular los permisos que cada empleado tiene con su usuario y llevar un recuento.	L1
[9.2.3] Gestión de los derechos de acceso con privilegios especiales.	20%	Del mismo, modo, se beria elaborar un control con los permisos especiales de cada empleado que lo tenga.	L2
[9.2.4]Gestión de información confidencial de autenticación de usuarios.	10%	La dirección, debe revisar la información confidencial, como las contraseñas de usuarios: estas deberían ser únicas, sin repeticiones	L1
[9.2.5] Revisión de los derechos de acceso de los usuarios.	30%	La Dirección debería revisar los derechos de acceso de usuario a intervalos regulares y utilizando un proceso formal.	L2
[9.2.6] Retirada o adaptación de los derechos de acceso	30%	Si hay ascensos dentro de la empresa, habría que revisar los controles de accesl que tiene cada uno.	L2
[9.3] Responsabilidades del usuario.	20%		
[9.3.1] Uso de información confidencial para la autenticación.	20%	Cada usuario, debe establecer su contraseña, segura y única.	L2
[9.4] Control de acceso a sistemas y aplicaciones.	56%		
[9.4.1] Restricción del acceso a la información.	50%	Se debería restringir el acceso a la información y a las aplicaciones a los usuarios y al personal de soporte, de acuerdo con la política de control de acceso definida.	L2
[9.4.2] Procedimientos seguros de inicio de sesión.	40%	El acceso a los sistemas operativos se debería controlar por medio de un procedimiento seguro de inicio de sesión.	L2

[9.4.3] Gestión de contraseñas de usuario.	90%	Se debería llevar un riguroso control de las contraseñas.	L4
[9.4.4] Uso de herramientas de administración de sistemas.	0%	Se debería restringir y controlar de una manera rigurosa el uso de programas y utilidades que puedan ser capaces de invalidar los controles del sistema y de la aplicación.	L1
[9.4.5] Control de acceso al código fuente de los programas	100%		L5

[11]SEGURIDAD FÍSICA Y AMBIENTAL.	**40%**	**CONTROL**	**40%**
[11.1] Áreas seguras.	60%		
[11.1.1] Perímetro de seguridad física.	30%	Se deberían utilizar perímetros de seguridad (barreras, muros, puertas de entrada con control de acceso a través de tarjeta, o puestos de control) para proteger las áreas que contienen la información y los recursos de tratamiento de la información.	L2
[11.1.2 Controles físicos de entrada.	30%	Las áreas seguras deberían estar protegidas por controles de entrada adecuados, para asegurar que únicamente se permite el acceso al personal autorizado.	L2
[11.1.3 Seguridad de oficinas, despachos y recursos.	40%	Se deberían diseñar y aplicar las medidas de seguridad física para las oficinas, despachos e instalaciones	L2
[11.1.4 Protección contra las amenazas externas y ambientales.	50%	Se debería diseñar y aplicar una protección física contra el daño causado por los desastres naturales o provocados por el hombre.	L2
[11.1.5 El trabajo en áreas seguras.	100%	Hay que diseñar una protección física.	L2
[11.1.6 Áreas de acceso público, carga y descarga.	90%	Deberían controlarse de las áreas de carga y descarga y otros puntos, donde el personal	L2

		no autorizado pueda acceder a las instalaciones,	
[11.2] Seguridad de los equipos.	20%		
{[11.2.1] Emplazamiento y protección de equipos.	10%	Los equipos deberían situarse o protegerse de forma que se reduzcan los riesgos derivados de las amenazas y peligros de origen ambiental así como las ocasiones de que se produzcan accesos no autorizados.	L4
[11.2.2] Instalaciones de suministro.	20%	Los equipos deberían estar protegidos contra fallos de alimentación y otras anomalías causadas por fallos en las instalaciones de suministro.	L1
[11.2.3] Seguridad del cableado.	20%	El cableado eléctrico y de telecomunicaciones que transmite datos o que da soporte a los servicios de información debería estar protegido frente a interceptaciones o daños.	L1
[11.2.4] Mantenimiento de los equipos.	20%	Los equipos deberían recibir un mantenimiento correcto que asegure su disponibilidad y su integridad	L1
[11.2.5] Salida de activos fuera de las dependencias de la empresa.	20%	Hay que aplicar medidas para los activos que estén fuera de las instalaciones	L0
[11.2.6] Seguridad de los equipos y activos fuera de las instalaciones.	20%	Hay que aplicar medidas para los activos que estén fuera de las instalaciones	L0
[11.2.7] Reutilización o retirada segura de dispositivos de almacenamiento.	20%	Los equipos que sean cambiados o trasladados, también deben ser retirados con seguridad	L0
[11.2.8] Equipo informático de usuario desatendido.	20%	Al abandonar el puesto de trabajo, se debe tomar las precauciones debidas sobre los equipos.	L2
[11.2.9] Política de puesto de trabajo despejado y bloqueo de pantalla.	20%	Durante los descansos, hay que promover una política de apagado de las pantallas.	L2

[12] SEGURIDAD EN LA OPERATIVA.	**80%**	CONTROL	CUMPLIMIENTO
[12.1] Responsabilidades y procedimientos de operación.	20%		

12.1.1 Documentación de procedimientos de operación.	50%	Deberia documentarse.	L2
12.1.2 Gestión de cambios.	10%	Debería controlar los cambios en los recursos y sistemas de tratamiento de información.	L1
12.1.3 Gestión de capacidades.	10%	Hay que controlar las responsabilidades son llevadas a cabo, y si los que están a cargo son capaces de realizarlo.	L1
12.1.4 Separación de entornos de desarrollo, prueba y producción.	10%	La separación es clave para reducir riesgos en entradas no autorizadas.	L1
[12.2] Protección contra código malicioso.	90%		
12.2.1 Controles contra el código malicioso.	90%	Implementar controles de detección, prevención y recuperación.	L4
[12.3] Copias de seguridad.	90%		
12.3.1 Copias de seguridad de la información.	90%	Realizar copias periódicamente.	L4
[12.4] Registro de actividad y supervisión.	100%		
12.4.1 Registro y gestión de eventos de actividad.	100%		L5
12.4.2 Protección de los registros de información.	100%		L5
[12.4.3] Registros de actividad del administrador y operador del sistema.	100%		L5
[12.4.4] Sincronización de relojes.	100%		L5
[12.5] Control del software en explotación.	95%		

[12.5.1] Instalación del software en sistemas en producción.	95%		L4
[12.6] Gestión de la vulnerabilidad técnica.	95%		
[12.6.1] Gestión de las vulnerabilidades técnicas.	95%		L4
[12.6.2] Restricciones en la instalación de software.	95%		L4
[12.7] Consideraciones de las auditorías de los sistemas de información.	50%		
[12.7.1] Controles de auditoría de los sistemas de información.	50%		L2

[13]SEGURIDAD EN LAS TELECOMUNICACIONES	60%	CONTROL	CUMPLIMIENTO
[13.1] Gestión de la seguridad en las redes.	60%		
[13.1.1] Controles de red.	90%	Se deben gestionar correctamente, para evitar intrusiones.	L3
[13.1.2] Mecanismos de seguridad asociados a servicios en red.	50%		L2.
[13.1.3] Segregación de redes.	50%	Se deben segregar las redes para evitar que se infecten todas las redes.	L2
[13.2] Intercambio de información con partes externas.	60%		
[13.2.1] Políticas y procedimientos de intercambio de información.	10%	Todo aquello que tenga que ver con información de terceros, debe estar regulado entre ambas partes.	L1
[13.2.2] Acuerdos de intercambio.	40%	Los acuerdos de intercambio	L2

		deben estar regularizados.	
[13.2.3] Mensajería electrónica.	80%	Toda la información que circule debe estar protegida.	L2
[13.2.4] Acuerdos de confidencialidad y secreto.	100%	Los acuerdos deben ser de confidencialidad para aquello que trte datos confidenciales.	L5

[14] ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN.	40%	CONTROL	CUMPLIMIENTO
[14.1] Requisitos de seguridad de los sistemas de información.	20%		
[14.1.1] Análisis y especificación de los requisitos de seguridad.	30%		L2
[14.1.2] Seguridad de las comunicaciones en servicios accesibles por redes públicas.	0%		L0.
[14.1.3] Protección de las transacciones por redes telemáticas.	30%	Debería existir una política sobre la protección de los datos que se transmiten telemáticamente.	L2
[14.2] Seguridad en los procesos de desarrollo y soporte.			
[14.2.1] Política de desarrollo seguro de software.	90%		L4
[14.2.2] Procedimientos de control de cambios en los sistemas.	40%		L2
[14.2.3] Revisión técnica de las aplicaciones tras	50%	Se debería llevar una revisión periódica de los	L2

efectuar cambios en el sistema operativo.		aplicativos tras los cambios.	
[14.2.4] Restricciones a los cambios en los paquetes de software.	0%		L0
[14.2.5] Uso de principios de ingeniería en protección de sistemas.	100%	Debería usarse los principios de ingeniería para la protección de los sitemas.	L5
[14.2.6] Seguridad en entornos de desarrollo.	30%		L2
[14.2.7] Externalización del desarrollo de software.	30%		L2
[14.2.8] Pruebas de funcionalidad durante el desarrollo de los sistemas.	30%		L2
[14.2.9] Pruebas de aceptación.	30%		L2
[14.3] Datos de prueba.	30%		
[14.3.1] Protección de los datos utilizados en pruebas	30%	Debe protegerse los datos que se manipulan cuando se trata de una prueba, pues es más débil.	L2

[16] GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN.	20%	CONTROL	CUMPLIMIENTO
[16.1] Gestión de incidentes de seguridad de la información y mejoras.	20%		
[16.1.1] Responsabilidades y procedimientos.	70%	Debería existir un protocolo donde figuren los responsables y las tareas en	L3

		caso de incidentes.	
[16.1.2] Notificación de los eventos de seguridad de la información.	10%	Debería existir una guía donde informe los nuevos incidentes para toda la plantilla.	. L1
[16.1.3] Notificación de puntos débiles de la seguridad.	10%	Se debería crear un informe donde se explica los puntos débiles de la empresa.	L1
[16.1.4] Valoración de eventos de seguridad de la información y toma de decisiones.	10%		L1
[16.1.5] Respuesta a los incidentes de seguridad.	10%	Debería existir un protocolo de respuesta en caso de incidentes.	L1
[16.1.6] Aprendizaje de los incidentes de seguridad de la información.	10%	Tendría que existir un registro de los incidentes que han ocurrido, de modo a cuantificarlos y conocerlos.	L1
[16.1.7] Recopilación de evidencias.	10%		L1

[17] ASPECTOS DE SEGURIDAD DE LA INFORMACION EN LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO``.	20%	CONTROL	CUMPLIMIENTO
[17.1] Continuidad de la seguridad de la información.	30%		
[17.1.1] Planificación de la continuidad de la seguridad de la información.	40%	Debería existir un plan futuro para el manejo de la información.	L2

[17.1.2] Implantación de la continuidad de la seguridad de la información.	20%	La implantación del plan, debería estar redactado, al igual que el plan en sí.	L2.
[17.1.3] Verificación, revisión y evaluación de la continuidad de la seguridad de la información	30%	Se debería crear un mecanismo para la revisión del plan de continuidad.	L2
[17.2] Redundancias.	10%		
[17.2.1] Disponibilidad de instalaciones para el procesamiento de la información	10%		L1

[18] CUMPLIMIENTO	**65%**	CONTROL	CUMPLIMIENTO
[18.1] Cumplimiento de los requisitos legales y contractuales.	80%		
[18.1.1] Identificación de la legislación aplicable.	50%	Debería existir un texto donde se identifican las diferentes leyes que se aplican.	L2
[18.1.2] Derechos de propiedad intelectual (DPI).	90%	Deberían implantarse procedimientos adecuados para garantizar la correcta aplicación de las normas de DPI.	L3
[18.1.3] Protección de los registros de la organización.	90%	Los documentos considerados importantes deben estar protegidos en caso de pérdida, o robo.	L3
[18.1.4] Protección de datos y privacidad de la	90%	Debe garantizarse la protección de datos.	L3

información personal.			
[18.1.5] Regulación de los controles criptográficos.	90%	Los controles criptográficos se deberían utilizar de acuerdo con todos los contratos, leyes y reglamentaciones pertinentes	L3
[18.2] Revisiones de la seguridad de la información.	50%		
[18.2.1] Revisión independiente de la seguridad de la información.	50%	Debe revisarse aleatoriamente la seguridad de la información, por parte de la dirección.	L2
[18.2.2] Cumplimiento de las políticas y normas de seguridad.	50%	Debe comprobarse regularmente, que se cumplen las normas, y adecuarse a los cambios en las legislaciones vigentes.	L2
[18.2.3] Comprobación del cumplimiento.	50%	Debe comprobarse que efectivamente se cumplen las nuevas leyes aprobadas.	L2